Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.6, Dec. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.6.1463

국내 무기체계에 대한 RMF 적용 실 사례 연구*

조 현 석,† 차 성 용, 김 승 주‡
고려대학교 정보보호대학원

A Case Study on the Application of RMF to Domestic Weapon System*

Hyun-suk Cho,† Sung-yong Cha, Seung-joo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

현대의 첨단 무기 체계는 과거와 달리 복잡하고 많은 구성품들이 결합되어 하나의 무기체계를 형성한다. 또한, 하드웨어가 주 구성이었던 과거와 달리 소프트웨어 비중이 매년 증가하고 있어 무기체계의 보안 보증 활동이 과거보다 더 어려워지고 있다. 미국은 1960년대부터 자신들이 개발하는 무기체계의 보안을 보증하기 위해 연구를 진행해왔다. 이 연구 결과는 미국 내부 표준으로 만들어졌고 정기적으로 업데이트 되었으며 현재는 RMF로 적용되고 있다. 국내에서는 미국의 RMF를 기반으로 2010년경부터 연구 활동을 해왔다. 그러나 미국 내 RMF 적용 실 사례는 기밀로 분류해 얻을 수 없고, 국내에서도 공식적인 적용사례는 없다. 본 논문에서는 지금까지 연구된 한국형 RMF 연구를 활용하여 최근 개발된 실제 무기체계에 적용해 본다. 그리하여 RMF를 적용할 수 있는 상세 가이드라인을 제시한다.

ABSTRACT

Unlike the past, modern high-tech weapons systems are complex and many components are combined to form a weapons system. In addition, unlike the past, where hardware was the main component, the proportion of software is increasing every year, making the security assurance activities of weapon systems more difficult than in the past. The United States has been working to ensure the security of the weapons systems they develop since the 1960s. The findings were made to US internal standards, updated regularly, and are now being applied as RMF. In Korea, research activities have been conducted since 2010 based on the RMF of the United States. However, actual RMF application cases in the United States cannot be classified and obtained, and there are no official cases in Korea. In this paper, we apply Korean RMF research that has been studied so far to apply to the recently developed real weapon system. Thus, detailed guidelines for applying the RMF are presented.

Keywords: RMF(Risk Management Framework), Weapon System, Secure SDLC

I. 서 론

현대 사회에서 정보 보호 활동은 자산과 직접적으로 관련이 있으며 그 중요성은 날로 증가하고 있다. 특히 국방 관련 정보는 국가 안보와 관련돼 있어 무엇보다 중요하다. 2011년 이란군의 미국 스텔스 드론 RQ-170 해킹은 개발 비용을 휴지조각으로 바꾼 대형 사건이다[1]. 우리나라도 2016년 북한의 소행

Received(10. 24. 2019), Modified(11. 14. 2019), Accepted(12. 03. 2019)
* 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2019-2015-0-00403)
† 주저자, ambitihyun@naver.com
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

으로 추정되는 국방 전산망 해킹 사례가 있다[2]. 국방 네트워크를 일반 외부 네트워크와 분리하여 해킹 위협으로부터 안전하다는 국방부의 주장과 달리, 국방 네트워크 및 일반 외부 네트워크 컴퓨터 모두에서 동일한 백신 프로그램을 운영하여 취약점이 발생하였다. 이 취약점을 이용한 해커들에게 군사 작전과 관련된 고등급 보안 자료들이 유출되었다.

첨단 무기체계는 과거 재래식 무기체계와 달리 대형 장비와 복잡한 부품으로 구성되어 있다. 소프트웨어가 진보함에 따라 무기체계를 구성하는 부품에 소프트웨어 비율이 높아지고 있으며, 정보의 형태도 디지털화 되어 과거보다 더 많은 정보가 자산으로 식별되고 있다. 국내 무기체계는 대부분 서버와 클라이언트 형태로 네트워크에 연결되어 있다. 클라이언트 무기체계나 그 구성요소를 도난당하면 서버까지 악성 공격자의 위협에 노출될 수 있다. 실제로 군사안보지원사령부(구 국군기무사령부) 정보보호인증센터에서 국내 무인항공기 무기체계의 보안 검증을 실시한 결과, 관리자의 계정 정보가 소프트웨어 소스 코드와 주석, 설정 파일 등에 그대로 노출되어 있었다[3]. 즉, 보안 취약점을 가진 국산 무인기가 악의적인 공격자에게 넘어가면 국가안보를 위협할 정도로 그 여파가 크다.

많은 국가에서는 무기체계의 SDLC(System Development Life-Cycle)에서 보안 위험을 초래할 수 있는 요소를 개발단계에서 제거함으로써 사후 유지보수의 시간과 비용을 줄이려고 노력하고 있다. 이를 Secure SDLC라고 하며, 미국과 다른 강대국들은 이미 각자의 국가를 위해 Secure SDLC를 구축해 왔다. 이 가운데 미국은 수십 년간 Secure SDLC를 구축하고 절차를 강화해 왔다. 미 국방부는 C&A(Certification and Accreditation)라는 시스템을 의무화함으로써 납품되는 모든 시스템을 적용하고 있다. C&A의 시작은 1983년 일명 오렌지북이라 불리는 TCSEC(Trusted Computer System Evaluation Criteria)이다. 이후 DITSCAP(DoD Information Technology Security Certification and Accreditation Process), DIACAP(Defense Information Assurance Certification and Accreditation Process) 순으로 업데이트 되었으며 현재는 미국표준기술연구소(National Institute of Standard and Technology, 이하 NIST)에서 정의한 RMF(Risk Management Framework)를 도입하여 Secure SDLC에 적용하고 있다. 이렇게 미국의 Secure SDLC는 연구에 투자한 기간이 길기 때문에 다른 나라에 비해 선진화 되어 있다.

국내에서도 몇 년 전부터 무기체계의 보안을 확보하기 위한 정책이 수립되어 왔지만, 몇 가지 문제가 있다. 첫째, 현재의 정책은 SDLC의 모든 단계에서 보안을 고려한 활동이 아니라 구현 단계에서 시큐어 코딩 또는 모의해킹을 적용하는 데만 초점을 맞추고 있다. 반면에 요구사항 분석 및 설계 단계에서의 보안 보증 활동은 등한시 되고 있다. 이로 인해 요구사항 분석 및 설계 중에 식별해야 하는 보안 기능이 누락될 수 있다. 둘째로, 무기체계가 갖춰야 할 보안 기능들이 운영 환경을 고려하지 않는다. 마지막으로, 개발이 완료된 무기체계의 정비 대책에서는 보안이 고려되지 않는다.

제시된 세 가지 문제를 해결하기 위해, Secure SDLC는 무기체계의 수명 주기 전체에 걸쳐 보안을 고려하도록 구축되어야 한다. 국내 무기체계의 SDLC는 미국 표준을 인용하여 구축되었기 때문에, 각 단계에서 수행되는 활동과 문서 산출물이 유사하다. 이 때문에 미국에서 보안 보증 활동으로 적용하고 있는 표준을 국내 환경에 맞게 수정하면 한국형 Secure SDLC를 효과적으로 구축할 수 있게 되고 앞서 언급한 세 가지 문제점을 해결할 수 있게 된다. 국내 무기체계에 RMF를 적용한 최초의 연구결과는 [4]에서 확인할 수 있다. 그러나 미국 무기체계에 적용하는 RMF의 실제 사례는 대외비로 분류되기 때문에 관련 자료를 얻을 수 없다. 이 때문에 국내 무기체계 SDLC에 RMF를 적용한 연구에서도 단계적으로 실시해야 할 활동은 언급하고 있지만 실제 무기체계에 적용된 공식적인 사례는 아직 없다.

본 논문에서는 현재 국내에서 개발 중인 잠수함 무기체계를 대상으로 RMF 프로세스를 실제 적용해 본다. 이 과정에서 기존 SDLC의 문서 산출물을 활용하여 RMF를 효과적으로 적용할 수 있는 방법을 제안한다. 또한 본 논문에서 RMF를 적용한 결과를 기존 보안 정책과 비교하여 그 효과를 확인한다.

본 논문은 서론에 이어, 2장에서는 Secure SDLC에 대한 관련 연구를 제시한다. 3장에서는 RMF를 적용하는 방안을 제시하고, 4장에서는 최근 개발이 완료된 잠수함 무기체계에 적용해보고 그 결과를 분석한다. 이후 5장에서 추후 연구 활동을 기술한 다음 마무리 한다.

II. 관련 연구

2.1 美 무기체계의 Secure SDLC 연구와 정책 동향

미국 무기체계의 Secure SDLC는 C&A 체계를 의무화하고 이를 바탕으로 발전해왔다. C&A 체계는 보안 기능이 있는 정보시스템의 보안 요건이 충족되는지 여부를 인증하고 운용모드에서의 보안 위험에 대한 대책을 인가하는 정부의 활동을 말한다.

C&A 체계에 기반을 둔 Secure SDLC의 시작은 1983년도에 발표되어 일명 오렌지북으로 불리는 TCSEC이다. TCSEC은 이미 1960년대부터 20년간 연구되었다. TCSEC은 보안의 3요소인 기밀성, 무결성, 가용성 중 기밀성에 초점을 맞춰 개발과 평가를 위해 만들어졌다. 이후 유럽의 보안 인증 평가인 ITSEC(Information Technology Security Evaluation Criteria)과 결합되어 1999년 국제 표준인 CC(Common Criteria) 인증이 되었다.

1997년, 미국은 무기체계 개발부터 운용단계까지 모든 개발 프로세스에 보안성 평가를 수행하는 DITSCAP을 정책으로 만들어 Secure SDLC를 업데이트 하였다. 이 Secure SDLC는 표준 보안통제항목이 없어 개발되는 각각의 무기체계마다 새롭게 정의한 보안통제항목을 사용해야 했다.

이후 2007년 연방정보보호관리법(Federal Information Security Management Act, 이하 FISMA)를 충족하기 위해 미 국방부는 DIACAP 모델을 만들었다. 미 정부에 납품되는 모든 소프트웨어는 FISMA를 준수하도록 되어 있었기 때문에 미 국방부의 무기체계도 예외사항은 아니었다.

DIACAP은 과도한 문서 산출물과 평가 시간으로 비용대비 효과가 저조했다. 또한 무기체계 SDLC와 연계성이 부족하여 보안과 개발이 별도 프로세스로 진행되는 단점이 있었다. 이를 보완하기 위해 2013년도 RMF(Risk Management Framework)가 탄생하였고 현재까지 적용되고 있다. RMF는 미 국방부지침(Department of Defense Instruction, 이하 DoDI) 8510.01 "Risk Management Framework(RMF) for DoD Information Technology(IT)"[5]에 그대로 반영되어 무기체계 개발 시 필수적으로 준수하도록 되어있다.

RMF는 제품 개발부터 평가 및 유지관리에 이르기까지 제품 라이프사이클 전반에 걸쳐 보안 보증 활동을 고려한 모델이다. Fig. 1.은 RMF의 6단계 과정이다. 각 단계의 세부적인 활동은 NIST가 배포한 특별 간행물(Special Publication, 이하 SP)에 설명되어 있으나, 앞서 언급했듯이 미국의 모든 국방 관련 자료는 비공개로 되어 있다.

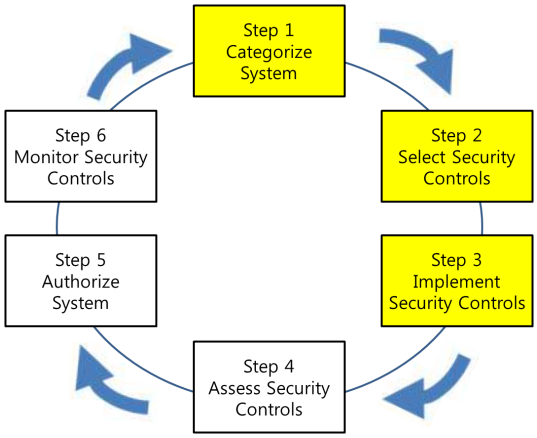

Fig. 1. RMF Process[6]

NIST SP 문서 중 800-37[6]은 RMF를 적용하기 위한 지침을 제공하여 본 논문에서 메인으로 참조한다. 해당 문서는 최근 2018년 12월에 Revision 2로 개정됐지만 본 논문은 해당 버전을 참고하지 않았다. 그 이유는 구버전인 Revision 1을 활용하여 이미 연구진행이 상당히 진행된 상태에서 Revision 2로 개정되었기 때문이다. 또한 Revision 2에서는 준비 단계를 추가하여 인가를 위한 범위를 조직 및 시스템 수준에서 설정하고, 필요에 따라 각 RMF 단계에 선행 가능하도록 개선하였다. 하지만, 본 연구에서는 RMF 중 1,2,3단계의 개념을 차용하므로, Revision 1의 해당 개념을 참고하여도 무방하다 판단하였다. 게다가 미 국방부 지침문서인 [5]에서도 신규 개정된 Revision 2를 아직 반영하지 않은 상태이다.

2.2 국내 무기체계의 Secure SDLC 연구와 정책 동향

국내 무기체계의 보안 보증 정책은 2016년에 개정된 '무기체계 개발 및 관리 매뉴얼'[7]에서 시작됐다. 이 정책에서는 전장관리체계를 대상으로 *시큐어코딩 가이드를 준수하도록 되어 있다. 이에 따라 국내 연구에서는 자동화 도구를 이용한 소스코드 보안 취약

* 행정안전부에서 발간한 'SW 개발보안가이드(2017.1)' 내부에 '4장 구현 단계 시큐어코딩 가이드'

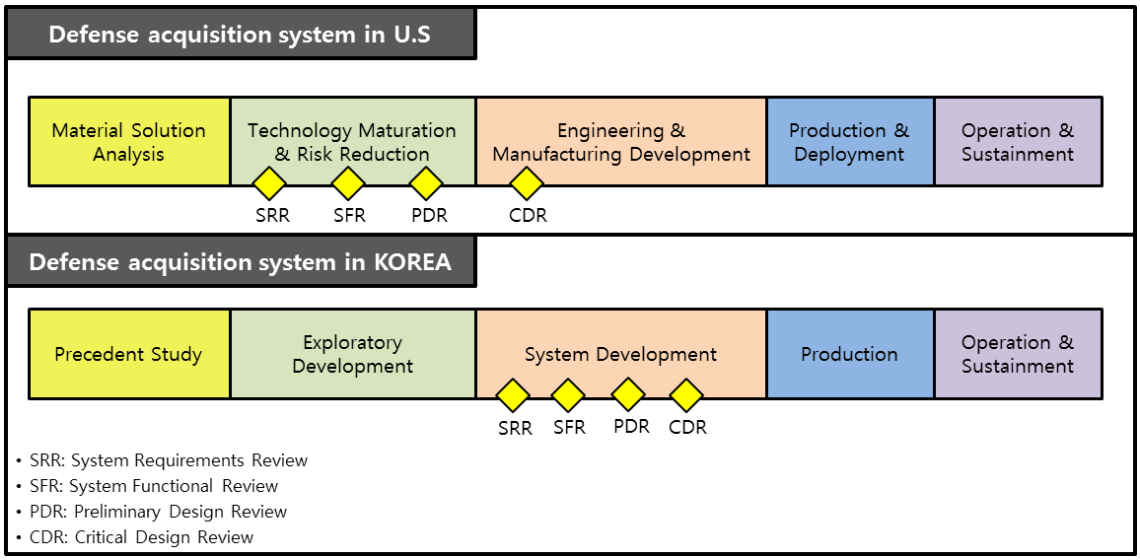

Fig. 2. Comparison of Defense acquisition system between U.S. and Korea[14]

성 분석에 주로 초점을 맞췄다[8][9]. 하지만 이 보안 보증 활동은 전체 개발 단계가 아닌 소스 코드 구현 단계로만 한정되기 때문에 요구사항 분석 단계나 설계 단계 등 다른 개발 단계에서 발생하는 보안 취약성은 놓칠 수밖에 없다.

2017년 우리 국방부에서는 무기체계 개발 시 필수로 준수해야하는 '국방전력발전업무훈령'[10]에 신규 정책인 '국방사이버안보훈령'[11]을 포함시켰다. [11]은 무기체계의 기능에 적합한 보안통제항목을 선정하고, 보안통제항목을 [11]의 부록인 '국방정보시스템 보호대책서'에 반영하도록 규정하고 있다. 그러나 [11]의 보안 보증 활동은 무기체계 개발 단계 초기에만 실시되며, 개발 라이프사이클인 SDLC와 유기적으로 구성되어있지 않다. 또 보안 요구사항 분석 활동이 없어 필요한 보안 요구사항이 모두 파악됐는지 알 수 없다.

최근 현 정책의 약점을 보완하기 위해서 국내 무기체계에 잘 갖춰진 해외 Secure SDLC을 적용하자는 제안이 나오고 있다. 그 중 [12]는 기존 SDLC에 Microsoft사의 Secure SDLC인 MS-SDL (Microsoft Secure Development Life-cycle)을 적용하자고 제안하였다. [13]도 마찬가지로 MS-SDL을 인용하여 국내 무기체계 Secure SDLC 제정을 주장하였다. MS-SDL은 대표적인 Secure SDLC 모델 중 하나지만 보안 보증 대상이 소프트웨어에 집중되어 있다. 하드웨어와 소프트웨어의 보안성을 모두 고려해야하는 무기체계와는 맞지 않다. 또한 국내 무기체계에는 구성품의 상세 구조를 파악하기 어려운 상용 제품이 다량 포함되기 때문에 MS-SDL에서 가이드하고 있는 보안성 분석 및 보증 활동은 적용하기 어려울 수 있다.

한국의 국방획득체계의 프로세스는 미국의 표준을 도입하여 구축했기 때문에 미국 국방획득체계 프로세스와 매우 유사하다. Fig. 2.를 보면 한국과 미국의 국방획득체계 프로세스 유사성을 확인할 수 있다. 미국의 RMF 도입 방법은 기존 국방획득체계 프로세스를 변경하지 않은 상태에서 RMF의 세부 활동을 추가하여 구축하였다. 그 내용은 [5]에서 확인할 수 있다. 따라서 미국 국방획득체계에 적용된 RMF를 국내 환경에 맞게 수정하여 국내 국방획득체계 프로세스에 적용하면 한국형 Secure SDLC를 가장 효율적으로 구축할 수 있다.

[4]는 RMF와 CC 인증을 이용하여 국가 간 무기체계를 거래할 때 구매국의 관점에서 보안평가 모델을 제시하였다. [4]에서 제안된 프로세스 중 개발 단계에서는 미국의 RMF를 적용하여 보안통제항목을 식별하였다. 국내 국방획득체계의 프로세스에 RMF를 적용한 최초의 연구 결과지만 실제 적용 사례는 없다.

국내 무기체계는 정부의 요구사항에 따라 기업이 개발하고, 개발된 무기 체계에 대한 시험과 평가는 정부에서 주관한다. 즉, RMF의 Step 1,2,3은 기업

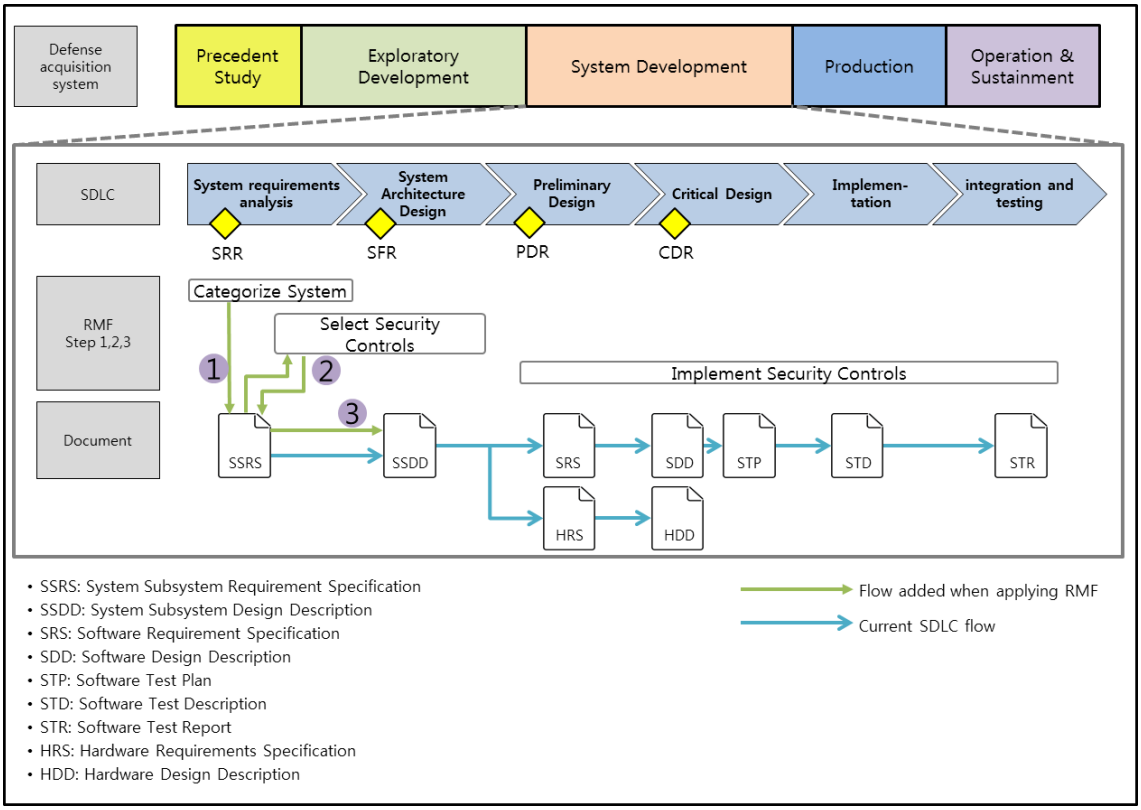

Fig. 3. Proposal of the relationship between documents and SDLC when applying RMF

과 정부가 공동 작업을 하고, Step 4,5,6은 정부에서 주관하는 활동이 된다. RMF의 각 Step별 활동은 NIST에서 발행한 SP 문서에서 상세히 가이드되고 있다. 하지만 Step 1,2,3 적용을 위한 NIST SP 문서에서는 국방 및 국가 안보와 관련된 시스템에 적용되는 가이드 내용이 모두 비공개로 되어있다. 따라서 본 논문에서는 RMF의 전체 프로세스 중 개발단계에 적용해 볼 수 있는 RMF Step 1,2,3을 실제 무기체계에 적용해 본다.

III. 제안 RMF 적용 방안

이 장에서는 기존 무기체계 개발단계에서 산출되는 문서들을 사용하여 현재 무기체계 SDLC에 RMF를 적용하는 방법을 제안한다. 이 과정에서 기존 산출되는 문서를 사용할 수 있는 부분과 보강해야 할 부분을 확인한다.

Fig. 3.은 RMF를 국내 무기체계 SDLC에 적용할 때 세부 단계와 산출 문서간의 관계를 제시했다. 전체 국방획득체계 프로세스에서 개발 단계 SDLC에만 RMF를 적용해본 제안이다. 이는 정부 요구사항에 맞춰 무기체계 개발 주관 기업이 적용할 수 있는 그림이다. 제시한 바와 같이 요구사항 분석과 설계 단계에서 RMF의 Step 1인 'Categorize System'과 Step 2인 'Select Security Controls'를 적용하였다. 요구사항 분석과 설계 단계에서 보안통제항목을 잘 식별하여 기존 산출 문서에 반영하면 RMF를 개발단계에 자연스럽게 적용할 수 있다.

적용한 세부 사항은 다음 절부터 개발 단계별로 제시한다.

3.1 요구사항 분석 단계

무기체계 개발 주관 업체는 정부로부터 받은 운용요구서(Operational Requirements Document, 이하 ORD)와 작전운용성능(Required Operational Capability, 이하 ROC)을 확인하고 사용자의 요구사항을 분석하여 체계요구사항명세서(System

Table 1. SSRS Contents

1. Scope
1.1 Identification
1.2 System Overview
1.3 Document overview
2. Reference Documents
2.1 Government Documents
2.2 Other Documents
3. Requirement
3.1 Required States and Modes
3.2 System Capability Requirements
3.2.X System capability (by subsystem)
3.3 System External Interface Requirements
3.3.1 Interface Identification and Diagram
3.3.X Interface Identification
3.4 System Internal Interface Requirements
3.4.1 Interface Identification and Diagram
3.4.X interface Identification
3.5 System internal data requirements
3.6 Adaptation Requirements
3.7 Safety Requirements
★3.8 Security and Privacy Protection Requirements
3.9 System Environment Requirements
3.10 Computer Resource Requirements
3.10.1 Computer Hardware Requirements
3.10.2 Computer Hardware Resource Utilization Requirements
3.10.3 Computer Software Requirements
3.10.4 Computer Communication Requirements
3.11 Factors
3.12 Design and Construction Constraints
3.13 Support Element
3.13.1 Personnel-related
3.13.2 Training-related
3.13.3 Logistics-related
3.14 Precedence and Criticality of requirements
3.15 Packaging Requirements
3.16 Other requirements
4. Qualification Provisions
Methods for determining satisfaction of "Chapter 3 Requirements" (demo, test, analysis, inspection, etc.) during test evaluation
5. Requirements traceability
Tracking from user requirements to system requirements
6. Notes/Appendix (if required)

Subsystem Requirement Specification, 이하 SSRS)를 작성한다. 이 과정에서 보안 요구사항은 SSRS의 3.8장 '보안 및 프라이버시 보호 요구사항(Security and privacy protection requirements)'에 작성하도록 되어있다. SSRS은 Table 1.과 같이 구성되어 있다.

문제는 현행 규정에는 ORD와 ROC를 분석할 때 보안을 고려한 요구사항 분석 지침이 없다는 점이다. 따라서 무기체계 개발에 필요한 충분한 보안 요구사항이 파악됐는지 알 길이 없다.

이러한 문제를 해결하기 위해 우리는 RMF의 Step 1인 'Categorize System'을 사용하여 보안 요구사항을 식별할 수 있다. Fig. 3.에서 ①로 표시해놓은 과정이다. RMF의 Step 1 적용 방법은 NIST SP 800-60[15] 문서에 안내되어 있다. [15]에서는 정보시스템별로 기밀성, 무결성, 가용성에 대한 잠재적 영향도(Potential Impact)에 따라 보안등급을 세 가지(High, Moderate, Low)로 분류하고 있는데 국방 및 국가 안보와 관련된 정보시스템은 비공개로 되어있다. 또한 [15]에서 식별되지 않은 정보시스템이나 비공개 되어있는 정보시스템의 보안등급을 산출하는 방법도 제시하고 있다. 그 방법은 Fig. 4.를 참고한다. 국내 무기체계도 마찬가지로 Fig. 4.를 참고하여 보안등급을 산출해야 한다.

Step 1에서 가장 중요한 것은 무기체계를 구성하는 모든 유형의 정보를 파악하는 것이다. 그래야 무기체계를 구성하는 모든 정보에 대한 보안 요구사항이 확인되었음을 보장할 수 있다. 정보 유형을 파악

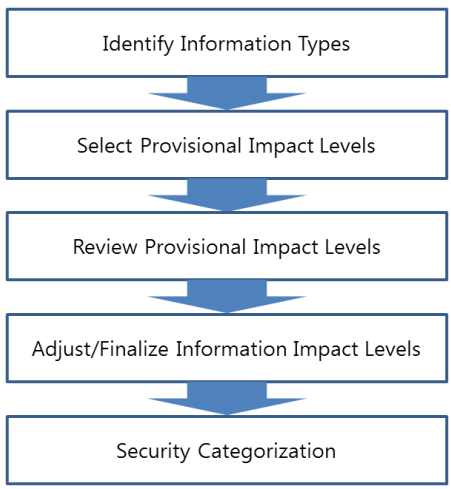

Fig. 4. RMF Step 1 Flow[15]

하기 위해서는 SSRS 문서의 3.3장인 System External Interface Requirements와 3.8장인 Security and privacy protection requirements를 참고한다. 이 두 개의 장절을 이용하면 미리 식별한 보안 요구사항에서 정보를 추출할 수 있고, 인터페이스 자료에서 데이터의 흐름을 보고 미식별한 정보를 찾아낼 수 있다.

그런 다음 각 정보 유형에 대한 임시 영향 값을 부여한다. 이해관계자와 전문가의 검토과정을 통해 각 정보 유형의 영향 값을 확정짓고 최종 무기체계의 보안 분류를 High, Moderate, Low 중 선택한다. 여기서 임시 영향 값이란 식별한 정보가 무기체계를 운용할 때 기밀성, 무결성 및 가용성을 고려하여 영향을 측정하는 값이다. 임시 영향 값은 측정 시 주관적인 판단보다는 최대한 많은 근거자료를 제시하여 그 근거를 뒷받침 할 수 있어야 한다. 무기체계 특성상 유사 근거자료를 찾기 어려울 때에는 보안 전문가를 포함한 모든 이해관계자들의 합의가 이루어진 임시 영향 값을 선택해야만 한다. 이렇게 정해진 보안등급은 추후 동일 무기체계의 성능개량 프로젝트 또는 유사 프로젝트 개발 진행 시 참고자료로 활용될 수 있기 때문에 정부는 무기체계에서 식별한 모든 정보와 임시 영향 값, 최종 보안 분류를 데이터베이스화할 필요가 있다.

RMF는 Step 1의 결과로 나오는 보안 분류를 보안 계획(Security Plan)문서에 반영하도록 가이드하고 있다. 우리나라 무기체계 산출 문서는 미국과 달리 모든 비기능 요소를 기능 요소와 함께 단일 문서로 관리하고 있다. 그렇기 때문에 별도의 문서를 만드는 것보다는 기존 SSRS의 3.8장을 세분화 하여 RMF Step 1의 적용 결과를 반영할 필요가 있다. 또한 SSRS 문서에 보안 요구사항을 반영한다는 것은 식별자를 가지고 SDLC 모든 단계에 반영된다는 것이다. 그렇기 때문에 SSRS에 Table 2.과 같이 모든 정보 유형(All Information Types), 보안 분류(Security Classifications), 보안 요구사항(Security Requirements) 내용이 추가되어야 한다.

Table 2. Proposal contents of SSRS

3.8 Security and Privacy Protection Requirements
3.8.1 All Information Types
3.8.2 Security Classifications
3.8.3 Security Requirements
3.8.4 Privacy Protection Requirements
3.8.5 Minimum Assurance Requirements
3.8.6 Security Controls in Security Requirements

RMF의 Step 1에서 보안 분류를 하는 이유는 정보 유형별 보안 요구사항을 확인하는 의미도 있지만 최소 보안통제항목(Minimum Assurance Requirements)을 도출하기 위한 객관적인 근거로 사용하기 위함이다. NIST SP 800-53[16]에서는 앞서 Step 1에서 분류한 보안 등급에 따라 기본적으로 적용해야하는 최소 보안통제항목을 제시하고 있다. 이 최소 보안통제항목 또한 Table 2.에서 3.8.5 항목과 같이 SSRS에 반영되어야 한다.

현재 국내 정책은 [11]에서 제시하는 보안통제항목과 SDLC의 연관성이 없어 요구사항 대비 보안통제항목 반영 여부가 불투명했다. 이를 해결하기 위해 우리는 RMF Step 2인 'Select Security Controls'를 적용함으로써 보안 요구사항에 맞는 보안통제항목을 선택하고 이를 다음 단계인 설계에 반영시킬 수 있다. Fig. 3.에서 ②로 표시해놓은 과정이다. SSRS에 식별해 놓은 보안 요구사항에서 보안통제항목을 선택하고 선택된 보안통제항목은 다시 SSRS에 기록해 놔야 한다. RMF의 보안통제항목 관련 내용은 [16]에서 가이드 되고 있고, 국가 보안시스템(National Security Systems)에 속한 시스템은 CNSSI 1253(Committee on National Security Systems Instruction 1253)[17]에서 제시하는 보안통제항목을 추가적으로 적용하도록 되어 있다. 최소 보안통제항목과 보안 요구사항으로부터 선택된 보안통제항목의 합은 최종 무기체계의 보안통제항목이 된다. [16]과 [17]에서 선택한 보안통제항목 또한 Table 2.에서 3.8.6 항목과 같이 SSRS에 반영되어야 한다.

요약하자면 요구사항 분석 단계에는 RMF Step 1,2 단계를 이용하여 개발하는 무기체계의 보안 등급을 분류하고 보안통제항목까지 도출해 내야 한다.

3.2 설계 단계

설계단계는 Fig. 3.의 SDLC에서 System Architecture Design, Preliminary Design, Critical Design에 해당된다. 현재 우리 군에서 사용하고 있는 체계설계기술서(System Subsystem Design Description, 이하 SSDD)는 개발 대상 무기체계의 구조 설계 내용과 설계 시 고려사항을 작성하기 위한 문서이고 Table 3.와 같이 구성되어 있다.

Table 3. SSDD Content

1. Scope
1.1 Identification
1.2 System Overview
1.3 Document Overview
2. Reference Documents
2.1 Government Documents
2.2 Other Documents
3. System-wide Design Decisions
3.1 Design Principles and Policies
3.2 Major Design Decisions
3.2.x ooo Function
3.2.x.1 Outline
3.2.x.2 Requirement Analysis Result
3.2.x.3 Design Alternatives and Design Proposal
3.2.x.4 Design Decisions
3.2.x.5 Assumption and Constraints
★4. System Structural Design
4.1 Outline
4.2 System Component
4.2.1 Software Component
4.2.2 Hardware Component
4.3 System Composition
4.3.1 Hardware Structural Design
4.3.2 Network Structural Design
4.3.3 Software Structural Design
4.4 Concept of Execution
4.4.1 Outline
4.4.2 Identify Business Use Cases
4.4.3 Executive Concepts by Business Case
4.5 Interface Design
4.5.1 System Internal Interface
4.5.2 System External Interface
★5. Requirement Traceability
Traceability from System Requirements to System Components
6. Notes/Appendix (if required)

SSRS의 모든 요구사항들은 각각 식별자를 가지고 SSDD 4장인 체계 구조설계(System Structural Design) 내용과 맵핑된다. 보안통제항목도 각 항목별로 식별자를 부여하고 SSDD 4장인 체계 구조설계 내용에 반영되었는지 여부를 확인해야 한다. 그리고 5장 추적성(Requirement Traceability) 부분에 설계 내용과 보안통제항목 내용의 맵핑 자료를 넣어 모든 보안통제항목 적용 여부를 체크할 수 있도록 해야 한다.

요구사항 분석 단계에서 식별된 전체 보안통제항목은 설계단계에서 구체화되어야 하며, 그 결과는 SSDD 문서에 기록되어야 한다. Fig. 3.에서 ③로 표시해놓은 과정이다. [16]과 [17]에서 제시하는 보안통제항목은 일반화 되어있기 때문에 적용하는 무기체계에 맞게 구체화하는 설계 과정이 필요하다. 예를 들어 보안통제항목에는 입력되는 데이터에 대한 유효성 검사를 수행해야 된다는 일반적인 내용만 식별됐다면 설계 단계에서는 입력되는 데이터의 자료형태도 제시되어야 하고, 유효성 검사를 수행하는 알고리즘도 제시되어야 한다. 일반화 되어있는 보안통제항목을 구체화 한다는 것은 관련 지식이 없으면 쉽지 않을 뿐더러 잘못된 설계는 후에 더 많은 비용을 초래할 수 있다. 따라서 SSDD에서 보안통제항목을 구체화한 설계 자료는 보안 전문가의 검토가 꼭 필요하기 때문에 SSDD의 작성 책임자는 보안 전문가의 검토가 반영되었는지 확인해야 한다.

SSDD에 반영된 보안통제항목은 기본설계 단계(Preliminary Design)에서 하드웨어요구사항명세서(Hardware Requirements Specification, 이하 HRS)와 소프트웨어요구사항명세서(Software Requirements Specification, 이하 SRS)로 나눠져 개발 완료까지 관리되기 때문에 기존 국내 국방획득체계 프로세스는 유지한 상태로 자연스럽게 RMF를 적용할 수 있게 된다.

3.3 구현/테스트 단계

SSDD에서 설계된 항목을 하드웨어와 소프트웨어로 구분하면 HRS와 SRS로 나눌 수 있다. 이는 구현 시 각각 HDD(Hardware Design Description)와 SDD(Software Design Description)로 나눠지고 구현된다. 소프트웨어는 식별자를 가지고 소프트웨어통합시험계획서(Software Test Plan, STP)와 소프트웨어통합시험절차서(Software Test Description, STD), 소프트웨어통합시험결과서(Software Test Report)로 이어지는 테스트 프로세스가 진행된다. 이후에 하드웨어와 소프트웨어를 연동하여 SSRS의 요구사항을 이용한 체계통합시험을 수행하고 개발을 완료한다.

추가적으로 기능 요구사항이 아닌 품질요소로 식별한 비기능 요구사항을 만족하기 위해 설계과정에서 위협 분석을 수행할 수 있다. 또한 소프트웨어 구현 과정에서는 자동화도구를 이용하여 소스코드의 정적 분석과 동적 분석 등 각종 테스트 활동을 동반할 수 있다. 이런 활동을 수행하는데 미국 무기체계의 시험평가 프로세스는 SDLC에 맞춰 RMF와 유기적으로

이뤄져 있다. 미국 DoD(Department of Defense)에서 발간한 [18]문서를 참고하면 무기체계 연구개발에 RMF를 인용한 시험평가 프로세스를 확인할 수 있다.

IV. 적용 결과

RMF를 적용할 무기체계는 잠수함 무기체계로 최근 개발이 완료되었다. 개발 시에는 보안 요구사항에 따라 [11]에서 제시된 보안통제항목을 적용했다. 이 장에서는 본 논문 3장에서 제시한 Fig. 3. 내용 중 ①, ②, ③을 잠수함 무기체계에 적용해 보고 현재 잠수함 무기체계에 적용된 보안 활동과 비교해본다.

먼저 잠수함 무기체계는 총 196 개의 요구사항과 82개의 장비 간 인터페이스 자료(System External Interface Requirements)에서 39개의 세부 정보 유형을 추출할 수 있었다. [15]에 따르면 정보의 분류 범위가 너무 넓으면 임시 영향 수준이 너무 일반화되어 유용하지 않을 수 있고, 반대로 분류 범위가 너무 작을 경우 유사 무기체계 개발 시 임시 영향 수준을 재활용하지 못하고 무기체계 개발을 진행할 때마다 새로 추출해야 될 수 있다. 본 논문에서는 이 세부 정보 유형들을 다시 그 유사성을 고려하여 8개의 정보 유형으로 재분류하였다. 분류된 8가지 유형의 정보는 무기체계 운용 중에 발생할 수 있는 보안 위험의 기밀성, 무결성 및 가용성을 고려하여 임시 영향 값을 측정하였다.

재분류한 8개의 정보 유형 중 항해정보(Nautical Information)의 임시 영향 값 분석 내용을 본 논문에서 제시하도록 하겠다. Table 4.과 같이 잠수함의 항해정보(Nautical Information)는 6개의 세부 정보 유형을 이용해 재분류된 정보 유형이다. 항해정보의 임시 영향 값 분석은 다음과 같이 분석되었다.

Table 4. Information type of Nautical Information

Information type	Detail information type
Nautical Information	Submarine pose
	Submarine bearing
	Submarine location
	Submarine depth
	Submarine speed
	Satellite navigation information

- **기밀성(High)**: 잠수함의 주 임무는 수중에서 적에게 탐지되지 않고 대잠전, 대함전, 기뢰전, 해상로 감시정찰을 수행하는 것이다. 잠수함은 [19]에 따르면 수상함과 다르게 적에게 항해위치가 발각 되면 빠르게 움직일 수 없기 때문에 바로 격침될 수 있다. [20]은 중국에서 위성 레이저를 통한 잠수함 탐지 기술을 개발 중이라는 기사다. 잠수함을 탐지하는 기술이 발달됨에 따라 항해정보는 노출되기 쉬워지기 때문에 기밀성에대한 영향도가 높다.
- **무결성(High)**: 잠수함의 수중 이동은 수중으로 들어가기 전 수신한 위성항법정보(GPS정보)를 기준으로 표시하고 수중으로 잠수하면 자함 위치, 속력, 방위, 자세 정보를 계산하여 위치를 측정한다. 잠수함이 수중에 들어가기 전 [21]과 같은 GPS 교란 공격을 당하면 잠수함은 수중에서 어떠한 상황에 직면할지 모른다. 임무를 수행하지 못할뿐더러 적군이 의도한 경로대로 움직일 수 있다. [22]에서는 악성코드로 인해 측정 데이터 값이 정확하지 않게 될 수 있고 이는 항로 이탈을 시키거나 충돌을 일으킬 수 있다고 언급되어 있다.
- **가용성(High)**: 잠수함이 수중 또는 수상에서 작전수행 중 시스템 고장으로 인해 항해정보를 이용할 수 없다면 침몰 또는 적군에게 격침될 위험에 빠질 가능성이 높아진다. 1968년 소련의 골프급 핵잠수함 K-129호는 침몰 원인이 정확하게 밝혀지지 않았지만 계획된 항해 경로를 벗어나 침몰까지 간 사례이다.

정보 유형 별 임시영향 값 분석이 완료되면 대상 무기체계의 보안 분류를 정한다. 정보 유형 별 임시영향 값을 분석한 결과는 Table 5.와 같았다. 재분류된 8개의 각 정보 유형 별 세부 정보 유형의 수는 괄호 안에 숫자로 표기하였다.

본 논문에서 RMF를 적용한 잠수함 무기체계는 전시에 적 수중에서 작전을 수행하기 때문에 대부분의 정보 유형이 High로 분류되었다. 동일한 잠수함 무기체계라 하더라도 훈련을 목적으로 만들어진다면 각 정보 유형별 임시 영향 값은 High 보다는 낮게 측정될 것이다. 이처럼 임시영향 값은 반드시 적용하는 무기체계의 실제 운용환경을 고려하여야 한다.

Table 5.의 내용을 정리하면 모든 정보 유형의 평균값을 적용한 결과 기밀성 2.87, 무결성 2.87, 가용

Table 5. Temporary Impact Level of Information Type

Information type	Confidentiality	Integrity	Availability
Underwater Environment Information (9)	M	H	H
Nautical Information (6)	H	H	H
Tactical Information (4)	H	H	H
Tactical Support Information (5)	H	M	H
Sensor Information (3)	H	H	H
Ship Status Information (8)	H	H	H
Video Information (3)	H	H	H
Audio Information (1)	H	H	H

성 3으로 도출되었다. 따라서 본 논문에서 RMF를 적용한 잠수함 무기체계의 보안 분류는 High로 분류되었다.

정해진 보안 분류는 최소 보안통제항목을 뽑는데 기준이 된다. 적용하는 잠수함 무기체계는 High로 분류하였기 때문에 그에 맞는 최소 보안통제항목을 선택하였다.

요구사항 분석 단계에서 식별한 보안 요구사항을 확인하고 그에 맞는 보안통제항목도 [16]에서 선택하였다. 최종 잠수함 무기체계의 보안통제항목은 최소 보안통제항목과 무기체계의 보안 요구사항으로부터 도출된 보안통제항목의 합이 된다.

Table 6.에서 'Proposal Security Controls'는 RMF를 적용하여 도출한 최종 보안통제항목이고, 'Original Security Controls'는 기존 잠수함 무기체계의 보안 요구사항을 보고 [16]에서 선택한 보안

Table 6. Comparison of Security Control Items

Protection control item	Proposal Security Controls	Original Security Controls
Access Control	19	10
Awareness and Training	4	0
Audit and Accountability	12	5
Security Assessment and Authorization	8	1
Configuration Management	11	4
Contingency Planning	9	0
Identification and Authentication	8	1
Incident Response	8	0
Maintenance	6	1
Media Protection	7	0
Physical and Environmental Protection	17	0
Planning	4	1
Personnel Security	8	0
Risk Assessment	4	1
System and Services Acquisition	13	0
System and Communications Protection	21	2
System and Information Integrity	12	1
Total	**171**	**27**

통제항목이다. 기존 보안 요구사항은 [16]의 보안통제항목과 27개가 맵핑된다. 반면에 RMF의 High 등급을 적용한 결과 보안통제항목은 총 171개로 확인되었다. 기존에 미반영된 144개의 보안통제항목을 추가로 확보할 수 있었다. 즉 현재 요구사항의 기능만 보고 보안통제항목을 선정하는 것보다 본 논문에서 제안하는 RMF를 적용하면 약 6.3배의 보안통제항목을 추가 확보할 수 있음을 확인하였다.

RMF를 적용한 결과와 미적용한 결과의 차이를 보면 기존 잠수함 무기체계에는 물리적/환경적 요소(Physical and Environmental Protection), 우발상황(Contingency Planning) 등에 대한 보안통제항목이 없다. 기존 잠수함 무기체계는 보안통제항목을 선정할 때 운용되는 환경에서의 보안을 고려하지 않고 기능만보고 보안통제항목을 추출했기 때문이다. 또한 접근통제(Access Control), 설정 관리

(Configuration Management) 등에 대한 기본적인 보안통제항목은 식별되어 있지만 그 수도 RMF를 적용했을 때보다 훨씬 적다. 잠수함 무기체계에서는 단말기를 이용하여 함 네트워크에 접근할 수 있고 중앙 서버는 잠수함 무기체계의 모든 작전과 잠수함 상태 정보를 가지고 있기 때문에 접근통제와 관련된 보안통제항목이 높은 비중으로 고려되어야 한다. 또한 모든 센서에서 수집된 신호는 하나의 장치로 모이기 때문에 설정관리와 관련된 보안통제항목도 높은 비중으로 고려되어야 한다.

SSDD에 보안통제항목을 반영하여 설계가 완료되면 설계 내용을 바탕으로 하드웨어와 소프트웨어로 나뉘어 구현이 진행된다. 이렇게 되면 자연스럽게 기존 SDLC와 융합될 수 있다. 본 논문에서는 새로 식별한 보안통제항목을 이용해서 다시 개발하는 것이 아니므로 구현 및 테스트의 실제 적용은 예측만 한다.

기존 잠수함 무기체계의 보안 분류는 운용 환경을 고려하지 않고 정부에서 미리 분류한 기준으로 분류되었다. 반면에 RMF를 적용하여 도출한 무기체계의 보안 분류는 운용 환경에서의 보안 위험을 고려하고 임시 영향 값을 이용해 보안 수준에 대한 정량적인 데이터를 획득할 수 있었다. 또 무기체계를 구성하는 모든 정보가 보안 요구사항에 식별되었는지 확인함으로써 보안 요구사항 누락을 방지할 수 있었다. 결과적으로 RMF를 적용함으로써 기존의 모호한 무기체계 보안 분류를 객관적인 기준을 가지고 분류할 수 있고, 보안 요구사항의 누락을 최소화할 수 있었다. 하지만 Fig. 3.에서 제시한 ①, ②, ③은 모두 보안 전문가의 검토가 필요한 부분이다. 현재 연구되고 있는 무기체계에 비해 보안 분야 전문 인력은 턱없이 부족하다. 때문에 RMF를 도입한다 해도 모든 무기체계의 보안 검토를 할 수 있는 Secure SDLC에 대한 전문 인력 확보가 먼저 이뤄져야 할 것으로 생각된다.

V. 추후 연구 활동

미국 무기체계의 구성품은 100% 자국에서 생산하기 때문에 RMF 적용 시 모든 구성품을 분석할 수 있다. 반면에 한국 무기체계는 구성품의 일부를 수입품에 의존하고 있다. 적용하는 잠수함 무기체계 또한 독일의 잠수함을 국산화한 무기체계이기 때문에 일부 구성품은 수입 상용품으로 구성되어 있다.

수입 상용품은 본 논문에서 제안하는 것만 수행해서는 그 보안성 검증을 수행하지 못한다. 그러므로 향후 상용품을 고려한 국내 무기체계 보안성 확보 방안을 추가로 연구해볼 필요가 있다.

References

[1] Military & Aerospace Electronics, "Iran - U.S. RQ-170" http://www.militaryaerospace.com/articles/2016/05/unmanned-cyber-warfare.html, May. 2019

[2] ITWorld Korea, "Network Hacking Cases in Korea" http://www.itworld.co.kr/news/102451, May. 2019

[3] etnews, "verified the weapon system SW security" http://www.etnews.com/20180619000155, May. 2019

[4] Sungyong Cha, Seungsoo Baek, Sooyoung Kang and Seungjoo Kim, "Security Evaluation Framework for Military IoT Devices," Security and Communication Networks, Vol. 2018, Article ID 6135845, 12 pages, Jul. 2018

[5] "Risk Management Framework (RMF) for DoD Information Technology (IT)," DoDI 8510.01, Mar. 2014

[6] "Guide for Applying the Risk Management Framework to Federal Information Systems," NIST SP 800-37 Rev.1, Feb. 2010

[7] "Weapon System Development and Management Manual," DAPA(Defense Acquisition Program Administration), Nov. 2018

[8] Heejin Jang, Jingoog Kim, Seunghoon Jeong, Heedong Kim and Hyeonsook Kim, "Security Weakness Identification Methodology for Weapon System Software," The Korean Institute of Information Scientists and Engineers, 2017(12), pp. 149-151, Dec. 2017

[9] Yongjun Lee, Joonseon Ahn and Jinyoung Choi, "Research on Improving Security of Software Coding Rule

Guide, SCR-G," The Korean Institute of Information Scientists and Engineers, 2018(12), pp. 462-464, Dec. 2018
〔10〕 "National Defense Work Instruction," Ministry of National Defense, No.2040, Jun. 2017
〔11〕 "National Defense Cyber Security Instruction," Ministry of National Defense No.1862, Dec. 2015
〔12〕 Woncheol Lee, Kanghyun Kim and Seunghyeon Lee, "A Study of Software Security of Embedded Weapon Software Development Lifecycle," The Korean Institute of Information Scientists and Engineers, 2016(12), pp. 92-94, Dec. 2016
〔13〕 Yeonoh Jeong, "A Study about Development Methodology for Ensure the Software Security of Weapon System," The Korean Institute of Information Scientists and Engineers, 2018(6), pp. 77-79, Jun. 2018
〔14〕 Jiseop Lee, Sungyong Cha, Seungsoo Baek and Seungjoo Kim, "Research for Construction Cybersecurity Test and Evaluation of Weapon System," Journal of The Korea Institute of information Security & Cryptology, 28(3), pp. 765-774, Jun. 2018
〔15〕 "Guide for Mapping Types of Information and Information Systems to Security Categories," NIST SP 800-60 Rev.1, Aug. 2008
〔16〕 "Security & Privacy Controls for Federal Information Systems and Organizations," NIST SP 800-53 Rev.4, Apr. 2013
〔17〕 "Security Categorization and Control Selection For National Security Systems," CNSSI No. 1253, Mar. 2014
〔18〕 "Cybersecurity Test and Evaluation Guidebook," DoD, Apr. 2018
〔19〕 subleague.org, "submarines look so slow when sailing" http://www.subleague.org/xe/sub0307/1220, Apr. 2019
〔20〕 MBN, "China develops underwater submarine detection technology" https://www.mk.co.kr/news/world/view/2018/10/613151/, Apr. 2019
〔21〕 ScienceTimes, "GPS jamming" https://www.sciencetimes.co.kr/?news=gps%EC%A0%84%ED%8C%8C-%EA%B5%90%EB%9E%80-%EB%AC%B4%EC%97%87%EC%9D%B4-%EB%AC%B8%EC%A0%9C%EC%9D%BC%EA%B9%8C, Apr. 2019
〔22〕 BASIC, "Hacking UK Trident" https://basicint.org/wp-content/uploads/2018/06/HACKING_UK_TRIDENT.pdf, Apr. 2019

〈저자소개〉

조 현 석 (Hyun-suk Cho) 정회원
2014년 2월: 한성대학교 컴퓨터공학과 학사
2014년 1월~현재: LIG넥스원 선임연구원
2017년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 위험관리, 무기체계 신뢰성/보안성 시험평가

차 성 용 (Sung-yong Cha) 정회원
2004년 2월: 육군 사관학교 전산학과 전공
2008년 8월: 뉴욕 주립 대학교 전자공학과 석사
2019년 8월: 고려대학교 정보보호대학원 박사
2019년 8월 ~현재: 국방부
〈관심분야〉 C4I, 위험관리, 무기체계 신뢰성/보안성 시험평가

김 승 주 (Seung-joo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년: 한국인터넷진흥원(KISA) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2011년~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2004년~현재: 한국정보보호학회 이사
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2011년~현재: (사)화이트해커연합 HARU 및 국제해킹대회 SECUINSIDE 설립자 및 이사
2012년: 선관위 디도스 특별검사팀 자문위원
2014년~2015년: 육군사관학교 초빙교수
2014년~2016년: 다음카카오 프라이버시 정책 자문위원회 위원
2015년~현재: 방위사업청 방산기술보호 자문관
2016년~2018년: 개인정보분쟁조정위원회 위원
2016년~현재: 산업통상자원부 전략물자기술 자문위원
2016년~현재: 한국카카오뱅크 정보보호부문 자문교수
2017년~현재: 국방보안연구소 정보보호분야 자문위원
2017년~현재: 여신금융협회 신용카드 단말기 시험 인증위원회 위원
2017년~현재: 국민생활과학자문단 사이버안전분과 위원
2018년~현재: 고신뢰 보안운영체제 연구센터(CHAOS) 센터장
2018년~현재: 원자력안전위원회 전문위원
2018년~현재: 국방부 정보화책임관(CIO) 자문위원
2018년~현재: 코인데스크코리아 암호화폐 평가분석위원회 위원장
2018년~현재: 대통령직속 4차산업혁명위원회 위원
2019년~현재: 중소벤처기업부 규제특례 등 심의위원회 위원
〈관심분야〉 보안공학 및 SDL, 위협 리스크 모델링, 보안성 평가/인증, 암호학, Usable Security