https://doi.org/10.33778/kcsa.2021.21.4.101

사이버전 대응을 위한 무기체계 보안통제 시스템 구축 방안

장 석 우*, 이 용 준**

요 약

최근 무기체계는 폐쇄망 특성상 신뢰된 기능성만을 강조하였으나 사이버전 공격 사례가 발생하고 있어 무기체계에 대한 특성화된 보안통제 시스템 구축이 요구되고 있다. 미국, 이스라엘을 중심으로 무기체계에 대한 보안통제 시스템을 구축하여 사이버전 위협을 모니터링하여 신종 사이버전 위협에 대처하고 있다. 이에 본 연구에서는 국내외 무기체계 보안통제 시스템에 대한 기술을 분석하여 계층화된 무기체계 Gateway를 통해 부하가 최소화된 보안통제 모니터링 방법과 무기체계 Device 위변조·업데이트 방안, 인공지능 활용을 통한 신종 사이버전 위협 탐지 방법을 제안한다.

Weapon Security Control System for Respond to Cyber Warfare

Seok-Woo Jang*, Yong-Joon Lee**

ABSTRACT

Recently, only trusted functionality has been emphasized due to the nature of the weapon system, which is a closed network. We are responding to new cyber warfare threats by monitoring cyber warfare threats by establishing a security control system for weapons systems that are closed networks centered on the United States and Israel. Therefore, in this study, the security control monitoring method that minimizes the load through the layered weapon system gateway by analyzing the technology of the domestic and foreign weapon system security control system, the weapon system device forgery, change, update method, and the detection of new cyber warfare threats through the use of artificial intelligence method was proposed.

Key words : Defense ICT Supply Chain, Supply Chain Threat, Supply Chain Threat Response, ICT Threat, ICT Vulneravility

접수일(2021년 10월 07일), 수정일(2021년 10월 20일), 게재확정일(2021년 10월 31일)

* 안양대학교 소프트웨어학과(주저자)
** 극동대학교 해킹보안학과(교신저자)

1. 서 론

최근 폐쇄망인 무기체계 특성상 신뢰된 기능성만을 강조하였으나 최근 사이버전 공격 사례가 발생하고 있어 무기체계에 특성화된 보안통제 시스템 구축이 요구되고 있다. 미국, 이스라엘을 중심으로 폐쇄망인 무기체계에 대한 보안통제 시스템을 구축하여 사이버전 위협을 모니터링하여 신종 사이버전 위협에 대처하고 있다.

이에 본 연구에서는 국내외 무기체계 보안통제 시스템에 대한 기술을 분석하여 계층화된 무기체계 Gateway를 통한 부하가 최소화된 보안통제 모니터링 방법과 무기체계 Device 위변조·업데이트 방안, 인공지능 활용을 통한 신종 사이버전 위협 탐지 방법을 제시하고자 한다.

2. 관련 연구

무기체계 시스템은 임베디드 H/W상에서 무기체계 운영을 위한 S/W가 제한적인 자원을 최적으로 사용하도록 구성되어 있다.

<표 1>에는 함정, 미사일 등 부품에 내장되어 있는 무기체계 시스템에 대한 분류체계를 제시하였다[1].

<표 1> 무기체계 시스템 구성

구분		기능
H/W	마이크로 프로세스	• 무기체계 H/W 기능 처리
H/W 인터페이스	펌웨어	• 무기체계 H/W 제어용 기계어
	신호처리	• 무기체계 운영기능을 H/W에 전송
시스템 제어 S/W	시스템 운영체제	• 실시간 운영체제
	시스템 미들웨어	• 실시간 상태확인 미들웨어 • 센서 제어
	시스템 응용제어	• 무기체계 통합제어 • 무기체계 운영기능
입출력 S/W	실시간/비실시간 입출력	• 무기체계 데이터 교환
	시각화 기능	• 무기체계 상태 모니터링

무기체계 시스템은 군사적 목적을 위해 임베디드 H/W와 특정 목적으로 개발된 S/W로 정의할 수 있다. 기존에는 폐쇄형 무기체계 특성상 제한적 자원에서 신뢰된 기능을 운영하는 것을 목표로 하고 있으나 최근 무기체계 시스템에 대한 사이버전 사례가 증가하고 있어 보안성에 대한 중요성이 높아지고 있다. 무기체계 시스템은 다음과 같은 특징을 가지게 된다[2].

- 실시간성(Real-Time) : 무기체계 제어센서에 대한 제한시간 안에서 신뢰된 기능이 동작되어야 한다.
- 고신뢰성(High-Assurance) : 무기체계 시스템 오류나 오동작을 최소화하여 감내할 수 있는 기능을 제공해야 한다.
- 생존성(Liveness) : 열악한 군사적 환경에 대비하여 비, 바람, 온도, 습기 등 악조건의 환경에서도 동작되어야 한다.
- 자원제약(Constraints) : 무기체계 특성상 제약적인 연산기능, 저장용량, 저전력 등 리소스에서도 동작되어야 한다.
- 경량화(Light-Weighted) : 제한적인 센서, 부품에서 무기체계 기능이 수행되어야 하여 S/W 경량화되어야 한다.
- 이질성(Heterogeneity) : 기존 범용 운영체제가 아닌 특정 무기체계 운영을 위한 임베디드 S/W로 구성된다.
- 보안성(Security) : 무기체계 시스템은 사이버전 공격에 대비한 보안통제 모니터링을 제공해야 한다.

3. 무기체계 시스템 대상 사이버전 현황

3.1 미국 Left of Launch 작전

전자기파, 악성코드 유포 등을 통해 미사일 발사전에 통제시스템을 교란하는 무력화 작전으로 미사일 발사를 준비 → 발사 → 상승 단계로 분류

할 때 발사 왼쪽 단계인 준비 단계에서 전자기파, 악성코드 유포로 교란하는 작전이다. 미국은 2013년 2월 북한 3차 핵실험 이후에 Left of Launch 작전 가능성을 제시하였으며 2017년 4월 16일 북한이 발사한 미사일이 발사 직후 폭발한 것은 Left of Launch 작전의 사례로 보고되고 있다[3].

3.2 미국 F-22 사이버전 취약점

미국 전투기 F-22는 무기체계 통제 S/W를 통해 통합정보체계와 통신기능을 가지고 있다. F-22는 폐쇄형 무기체계가 아니고 전투작전을 위해 외부 연계를 해야 하는데 임베디드 H/W, 시스템 S/W 취약점을 대상으로 하는 사이버전 가능성이 제기 되었다. 전투기 무기체계는 작전 명령을 실시간으로 전송받아야 하기 때문에 사이버전에서 발생할 수 있는 해킹, 악성코드 유포 등에 대한 대응이 필요하다[4].

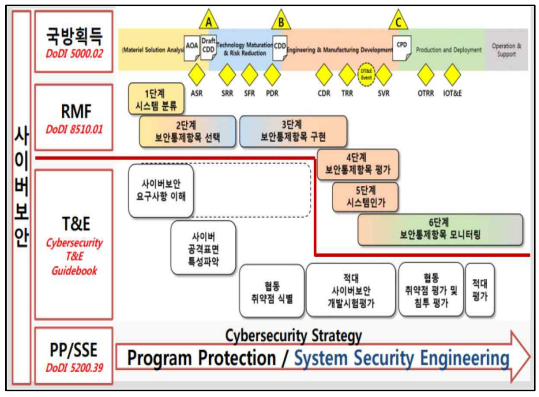
3.3 이란 UAV RQ-170 포획 작전

이란은 2011년 미국의 정찰용 무인기 RQ-170에 대한 제어기능 탈취 교란, GPS 탐지기능에 대한 사이버공격을 통해 포획하였다. 이란은 포획단 RQ-170에 대한 역공학을 통해서 이란의 신형 UAC(Uncrewed Aerial Vehicle)를 개발하여 미국 항공모함에 대한 정찰로 사용하고 있다. 이란이 RQ-170을 획득하는 과정에서 무기체계 시스템에 대한 취약점을 분석하여 사이버전을 감행한 것으로 알려져 있다[5].

4. 국내외 무기체계 사이버전 대응 현황

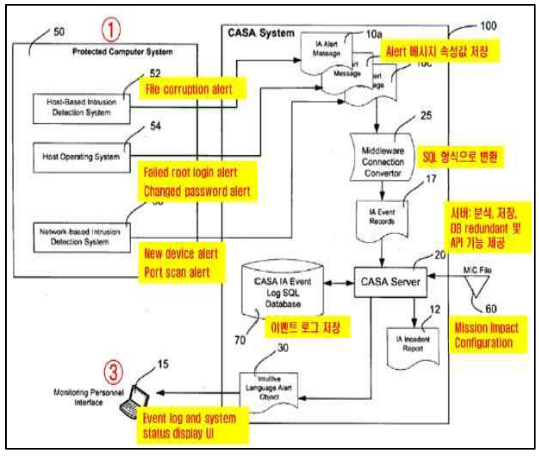
4.1 미국 무기체계 사이버전 대응방안

(그림 1)에서 미국의 사이버보안 시험평가 절차를 제시하였다. 무기체계 시험평가는 OSD(Office of the Secretary of Defense)에서 담당하며 무기체계 획득체계 전체 단계에서 평가하고 한다. 평가단계는 개발시험평가와 운용시험평가로 나누어 실시하고 있다. 개발시험 평가단계에서는 설계, 구현에서 발생한 취약점 분석, 모의해킹으로 점검한다. 운용시험 평가단계에서는 실제 운영환경에서 취약점 제거와 사이버전 대응대책을 평가한다[6].



(그림 1) 미국 사이버보안 시험평가 제도

미 해군 NSWCDD(Naval Surface Warfare Center Dahlgren Division)에서 개발한 함정용 보안시스템 통제체계로 무기체계 시스템, 네트워크에서 사이버 위협 관련 이벤트를 수집하여 분석하는 모니터링 체계를 가지고 있다[7].



(그림 2) CSCA 보안통제 시스템

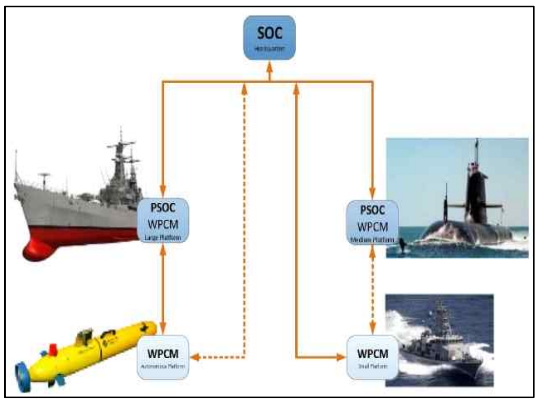
(그림 2)는 무기체계 보안통제 시스템 CASA (Common Architecture System Assurance)에 대한 구성도를 보여주고 있다. 함정 전투인원은 CASA를 통해 사이버 위협 이벤트를 탐지하여 생성한 경보 메시지를 확인할 수 있으며, 사이버 위협이 함정 임무에 주는 영향과 대응할 수 있도록 모니터링 기능을 제공한다.

4.2 이스라엘 무기체계 사이버전 대응방안

이스라엘 함정용 보안통제 시스템인 Neptune은 함정, 무인함, 잠수함 등 해군 전시 사이버전 모니터링 시스템으로 방화벽, 안티바이러스, 네트워크 장치, 센서로부터 사이버 위협 이벤트를 수집하여 함정 무기체계 이상 여부를 경고한다.

(그림 3)은 Neptune의 계층적 사이버 위협 모니터링 체계를 나타낸다. 탐지 / 모니터링 계층에서는 AI를 활용한 비정상 탐지(Anomaly Detection) 알고리즘을 사용하여 사이버 위협을 선제적으로 탐지한다. 통합 계층에서는 함정 무기체계, C4I체계 등에서 발생하는 사이버전 위협에 대해 통제한다.

이스라엘 해군 지휘부는 Neptune이 수집한 사이버 위협에 대해 함정 자체적으로 모니터링 및 복구 가능한 기능을 제공한다[7].

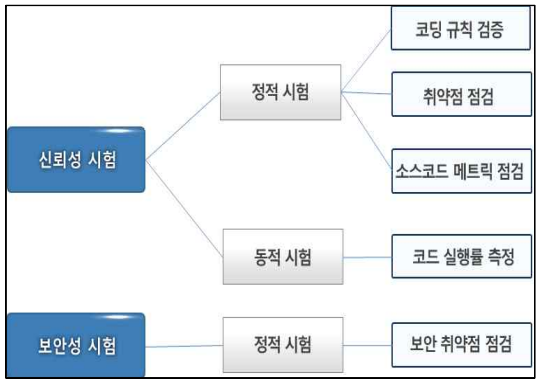


(그림 3) 이스라엘 Neptune 보안통제 시스템

4.3 한국 무기체계 사이버전 대응방안

한국 국방부는 기존의 무기체계 S/W 신뢰성 시험에 보안성을 강화하기 위해 국방전력 발전 업무 훈령에 무기체계 S/W 보안성 검증하도록 규정하였다. 무기체계 S/W 보안성 검증은 기동, 지휘통제, 연동 등 무기체계를 구성하는 S/W를 대상으로 취약점을 점검하게 된다. 무기체계 S/W 점검절차는 S/W 설계 산출물 검토와 구현 소스코드를 점검하도록 하고 있다[8].

(그림 4)는 한국 무기체계의 신뢰성 시험, 보안성 시험 항목을 보여주고 있다.



(그림 4) 한국 무기체계 사이버보안 점검항목

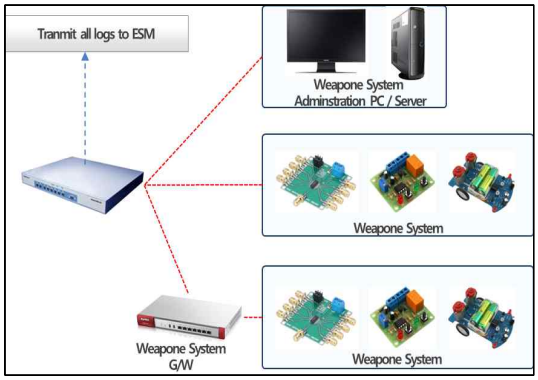
한국의 무기체계 보안위협 통제시스템은 화이트리스트 방식으로 국방과학연구소가 연구를 통해 시범 적용 중에 있다. 무기체계에 사이버전으로 인한 보안위협이 발생하면 무기체계 시스템, 응용 S/W 파일에 대한 변조가 발생하게 된다. S/W 실행파일에 대한 해시값을 화이트 리스트로 비교하여 미인가 S/W 실행을 원천적으로 차단하고 있다. 현재는 윈도우 운영체제만 지원하고 있어 함정, 미사일 분야에 임베디드 환경에 대한 연구개발이 필요하며 실제 사이버전이 발생하였을 때 원래 시스템으로 복구할 수 있는 복원력 연구가 필요하다[9].

4. 무기체계 보안통제 시스템 구축 방안

무기체계 대상으로 사이버전 위협에 방어하기 위한 에이전트 기술과 무기체계에 대한 사이버전 위협 시나리오에 따른 방어를 위한 보안통제 시스템 구축이 필요하다[10].

5.1 무기체계 Gateway 계층화

(그림 5)는 무기체계를 위한 보안통제 시스템 구축 방안을 제시하였다. 무기체계 Device는 제한적 기기의 특성을 가지기 때문에 보안통제 시스템 구축을 위해서는 사이버전으로 무기체계 시스템의 변경이 되는 통신체계에 보안장비를 통해서 수집이 가능하다[11].



(그림 5) 무기체계 보안통제 시스템

무기체계 보안통제 시스템은 다수의 무기체계 Device가 많을수록 발생한 로그 정보를 통합하여 중앙에서 보안통제 모니터링하기 어려운 문제가 있다. 무기체계 Device는 제한적인 성능을 가지고 있기 때문에 다수의 무기체계 Device에서 발생하는 로그정보 전체를 수신하기에는 전체 무기체계에 과부하를 발생하게 된다.

이러한 무기체계 제한적 환경을 고려해서 필요한 장치는 무기체계 Gateway 방식으로 구축이 필요하다. 무기체계 Gateway 방식으로 구축하는 이유는 중앙의 보안통제 시스템이 전체 무기체계 Device 변경 여부를 확인하기 어려운 환경으로 무기체계 통신망을 분할하여 무기체계 Gateway를 통해 4~5개 정도의 무기체계 Device별로 소규모 LAN을 구성할 수 있다. 무기체계 Gateway에 접점에 Packet Filtering Firewall, IDS(Intrusion Detection System)을 설치하여 통신패킷을 감시할 수 있다.

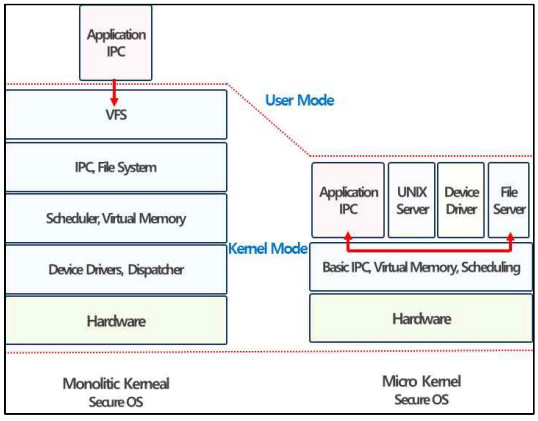
무기체계 Gateway 네트워크에 연결된 4~5개의 무기체계 Device로 외부 통신망으로 유입되는 통신패킷과 무기체계 Device 내부에서 외부로 통신하는 패킷을 검사한다. 사이버전 보안 위협을 시도를 차단하여 로그를 저장하도록 한다. 무기체계 Gateway를 접점으로 내부 LAN(Local Area Network)에 연결된 4~5개 모든 무기체계 Device는 1차적으로 무기체계 Gateway에 의해 감시가 가능하다. 이러한 분할 보안통제 시스템을 구축하여 중앙 보안통제 시스템은 모든 무기체계 Device를 검사하지 않으며 무기체계 Gateway에서 전송한 사이버전 위협 관련 로그만을 통합적으로 수집하여 2차적으로 분석할 수 있다. 이러한 무기체계 운영환경을 고려한 계층화된 보안통제 시스템을 구축하여 모니터링을 통한 부하를 최소화하면서 전체 무기체계 Device에 대한 위협을 감시할 수 있다.

5.2 무기체계 Device 위변조 방지 / 업데이트

사이버전 공격에 대한 탐지를 위해 무기체계 Device 위변조 방지용 SoC(System on Chip)이 필요하다. 무기체계 Device의 특성상 경량화, 저전력 Device가 많기 때문에 위변조 여부를 확인할 수 있는 SoC가 효과적이다. SoC는 반도체로 메모리 반도체, 마이크로 프로세서, 디지털 신호처리 회로(DSP), 마이크로컨트롤러(MCU) 등 개별 기능의 반도체를 한 개의 Chip에 통합하는 H/W 장치로 구성한다.

무기체계는 제한적 한계를 고려할 때 SoC에서 무기체계 시스템의 운영체제, 실행파일 위변조를 확인하고 회복할 수 있는 기능을 H/W로 구성하여 경량, 저전력 무기체계 Device 환경에 적합한 위변조 기능을 할 수 있다.

(그림 6)과 같이, 추가적으로 Micro-Kernal에 무기체계 보안 운영체제를 설치하는 방식이 있다. 무기체계 보안 운영 설계 방식에는 기존의 모놀리틱 커널(Monolithic Kernel) 방식은 운영체제의 핵심 기능을 모두 커널 레벨에 탑재하는 방식으로 무기체계 보안 운영체제 변경이 있는 경우 전체 운영체제를 설치하여 재가동해야 한다. 이외 대비하여 Micro-Kernel는 보안 운영체제의 핵심기능만 커널에 탑재하고 이외에 기능은 개별 프로세스로 구현하는 방식으로 특정 기능에 변경이 필요할 때 해당 기능이 설치된 프로세스 변경하여 재가동하면 되기 때문에 무기체계 보안통제 시스템에서 적합하다.



(그림 6) 무기체계 보안 운영체제

5.3 인공지능 기반 무기체계 위협 탐지

무기체계 보안통제 시스템에 대한 신종 사이버전 공격에 대비하여 인공지능를 활용한 보안통제가 필요하다. 인공지능 보안통제는 제한적 시간과 자원에서 발생한 다량의 무기체계 Device의 방대한 데이터를 자동화된 분석을 통해 무기체계 비이상 징후를 예측하여 능동 대처가 가능하도록 한다. 인공지능 보안통제를 위해 무기체계 Device로부터 위협 정보를 수집하여 기계학습을 통해 알려지지 않는 신종의 위협 탐지에 활용할 수 있다. 기본적인 무기체계 보안통제는 사이버전 시나리오에 대한 패턴화된 공격을 탐지하며 높은 수준의 탐지 효과를 보여주지만 기존 보안위협을 우회하거나 변경된 위협은 탐지가 어렵다. 따라서 무기체계 보안통제 시스템에 인공지능을 활용하기 위해서 사이버전 위협 식별과 실시간의 처리하기 위한 인공지능 침입탐지 알고리즘이 요구된다. 일반적으로 DBSCAN(Density-Based Spatial Clustering of Applications with Noise)과 같은 기계학습을 통해서 신종의 사이버전 위협을 선제적으로 탐지할 수 있다.

6. 결 론

국방 무기체계 시스템은 제한적 H/W, S/W 환경을 고려하여 발생 가능한 취약점을 제거하고 운영에 있어서 사이버전 위협을 탐지할 수 있는 보안통제가 요구되고 있다. 최근 폐쇄망인 무기체계 특성상 신뢰된 기능성을 강조하였으나 사이버전 공격 사례가 발생하고 있어 무기체계 특성화된 보안통제 시스템 구축이 필요하다.

미국, 이스라엘의 경우 함점 중심으로 폐쇄망인 무기체계에 대한 보안통제 시스템을 구축하여 사이버전 위협을 모니터링하여 신종 사이버전 위협에 대처하고 있다.

이에 국내외 무기체계 보안통제 시스템에 대한 기술을 분석하여 계층화된 무기체계 Gateway를 통한 부하가 최소화된 보안통제 모니터링 방법과 무기체계 Device 위변조/업데이트 방안, 인공지능 활용을 통한 신종 사이버전 위협 탐지 방법을 제시하였다. 본 연구를 통해 폐쇄망, 무기체계

Device 성능 제한성, 무기체계 기능 신뢰성의 특성을 고려한 신종 사이버전 위협을 탐지할 수 있는 무기체계 보안통제 시스템 구축안이 가능하다.

참고문헌

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

[2] 김권일, 김지원 "4차 산업혁명 기술 도입에 따른 하드웨어 공급망 위협과 대응 방안". 한국산업보안연구, 제10권, 제2호, pp.37-57, 2020.

[3] 김종화, 임재성, "사이버 위협 대응을 위한 軍정보화 자산관리시스템과 연계한 軍취약점 관리방안". 융합보안논문지, 제18권, 제1호,pp.111-116, 2018.

[4] 이대성, 안영규, 김민수, "북한의 사이버전 위협에 대한 분석과 전망". 융합보안논문지, 제16권, 제5호, pp.11-16, 2016.

[5] 이용준, "국방 ICT 공급에 대한 보안 위협 대응 방안", 한국융합보안학회 논문지, 제20권 4호, 2020.10.

[6] 고려대, '사이버보안시험평가를 위한 국방획득체계 RMF 프로세스 적용방안' 발표자료, 2017.

[7] 국방과학연구소, '함정 무기체계 운용 특성을 고려한 사이버 전술 훈련장 구축 설계 및 요구성능 연구', 2019.11.

[8] 권혁천, 박원형, 이용준, "한국의 사이버공격 비교분석과 정책적 대응방안", 한국융합보안학회 논문지, 제20권 5호, 2020.12.

[9] 고희재, 이용준, "국가 안보와 연계한 방위산업 보안 개념 정립", 한국산학기술학회 논문지, 제20권 12호, 2019.12.

[10] 하옥현, "산업보안을 위한 융합보안관제시스템에 관한 연구", 한국융합보안학회 논문지, 제9권 4호, 2009.

[11] 국방보안기술연구소, 'IoT 환경에서의 보안관제 발전방안', 2015.11.

〔저자소개〕

장 석 우(Seok-Woo Jang)
1995년 2월 : 숭실대학교 전자계산학과 학사
1997년 2월 : 숭실대학교 컴퓨터학과 석사
2000년 8월 : 숭실대학교 컴퓨터학과 박사
2009년~현재 : 안양대학교 소프트웨어학과 교수
email : swjang@anyang.ac.kr

이 용 준 (Yong-joon Lee)
1999년 2월 : 강남대학교 전자계산학과 학사
2001년 2월 : 숭실대학교 컴퓨터학과 석사
2005년 2월 : 숭실대학교 컴퓨터학과 박사
2020년~현재 : 극동대학교 해킹보안학과 교수
email : 2020032@kdu.ac.kr