https://doi.org/10.33778/kcsa.2020.20.4.135

국방 네트워크 환경에서 ATT&CK 기반 취약점 완화 체계 구축 방안

안 광 현*, 이 한 희**, 박 원 형**, 강 지 원***

요 약

국방부는 주기적인 사이버방호 훈련을 실시함에 따라 사이버작전의 전력과 역량을 보강하고 있다. 하지만 적 사이버 공격 능력 수준을 고려할 때 군의 사이버방호 능력 수준은 현저히 낮으며 군용 네트워크망에 대한 사이버위협을 대응할 수 있는 보호대책과 대응체계가 명확하게 설계되어 있지 않아 민·관의 사이버보안 능력 수준에도 못 미치고 있는 실태이다. 따라서 본 논문에서는 국내·외 사이버보안 프레임워크를 참조하여 국방 네트워크망 취약점 완화 체계를 구축할 수 있는 요소로 군 특수성을 지닌 군 내부망 주요 위협 정보 및 국방정보시스템 보안 요구사항을 파악하고, 공격자의 의도파악과 전술, 기법 및 절차 정보(ATT&CK)를 적용하여 국방 네트워크 환경에 대한 사이버공격을 효율적으로 보호해주는 군 내부망 취약점 완화 체계 구축 방안을 제안한다.

Vulnerability Mitigation System Construction Method Based on ATT&CK in Military Internal Network Environment

Gwang Hyun Ahn*, Hanhee Lee**, Won Hyung Park**, Ji Won Kang***

ABSTRACT

The Ministry of National Defense is strengthening the power and capacity of cyber operations as cyber protection training is conducted. However, considering the level of enemy cyber attack capability, the level of cyber defense capability of the ministry of national defense is significantly low and the protection measures and response system for responding to cyber threats to military networks are not clearly designed, falling short of the level of cyber security capabilities of the public and private sectors. Therefore, this paper is to investigate and verify the establishment of a military internal network vulnerability mitigation system that applies the intention of attackers, tactics, techniques and procedures information (ATT&CK Framework), identified military internal network main threat information, and military information system security requirements with military specificity as factors that can establish a defense network vulnerability mitigation system by referring to the domestic and foreign cyber security framework It has the advantage of having.

Key words : Military Internal Network Vulnerability, ATT&CK, Cyber Operations, Cyber Protection

접수일(2020년 09월 29일), 수정일(1차: 2020년 10월 13일), 게재확정일(2020년 10월 21일)

* 국방부(주저자/종신회원)
** 국방부(제2저자)
** 상명대학교 정보보안공학과(제2저자)
*** 세종대학교 컴퓨터공학과(교신저자)

1. 서 론

최근 국방 분야의 사이버공간을 위협하려는 공격시도가 급증하고 있다. 사이버공간 내에서 발생하는 사이버공격은 국방정보체계의 취약점을 악용해 군 내부망을 침투하여 정보탈취, 시스템 장악 등의 사이버전이 발생하고 있다[6]. 2016년도 국방부에서 대규모 정보유출 사고가 발생하였다. 육·해·공군의 모든 데이터 수집, 처리, 관리 및 보존 등 하나로 통합화한 전군 데이터 중앙 관리 센터인 국방통합데이터센터(DIDC)에서 내외부 위협 요인(전장망과 외부망 혼용하여 자료획득)으로 인해 악성코드가 유입되어 최초 백신중계서버에 잠복기간을 걸쳐 중앙 데이터 수집 서버로 유포되어 감염된 사례이다[11].

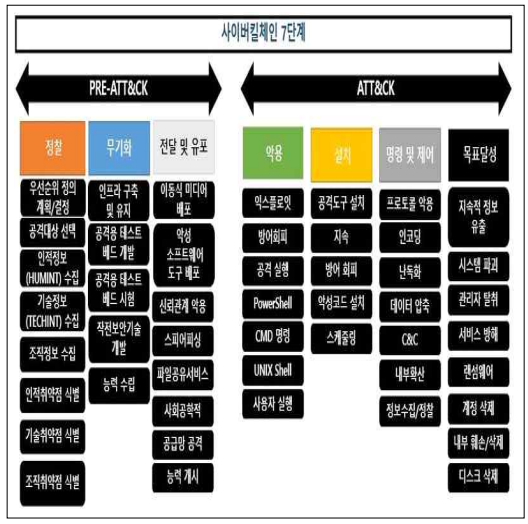
군의 네트워크 현황으로는 3대 통신망, 국방정보통신망 등으로 구성되어 있다. 군 내부망을 통해 시스템을 운영하기 위해서는 국방사이버안보훈령 제24조 국방정보시스템 보호기준과 보호요구사항 모두 충족해야만 구축이 가능하다. 이러한 특수성으로 군 네트워크 및 시스템 보안성 평가를 통해 안전하게 운용하고 있다.

그러나 적 사이버공격은 고도화·지능화를 넘어 첨단화 수준의 능력을 갖춰 국방 네트워크 취약점 발굴 및 지속적인 공격 시도를 수행하고 있다. 따라서 본 논문은 국내·외 사이버보안 프레임워크 및 ATT&CK 정보를 활용하고, 군의 특수성(국방정보체계 보호요구사항)을 맵핑시켜 군 내부망 취약점 완화 체계 구축 방안을 연구하여 검증한다. 효과성으로는 국방 네트워크 환경에 대한 사이버공격을 효율적으로 보호하여 주요 위협을 완화시킬 수 있는 장점을 가진다.

본 논문의 구성은 다음과 같다. 2장에서 ATT&CK & 사이버킬체인 모델 분석, 국내 사이버보안 프레임워크 실태를 소개한다. 3장에서는 본 논문에서 제안하는 군 내부망 취약점 완화 체계 구축 방안과 적용방향, 제안, 국방정보시스템 보호요구사항을 기술한다. 4장에서는 3장에서 제안된 군 내부망 취약점 완화 체계를 통한 실험 결과를 보이고, 5장에서는 결론과 향후 연구 방향을 설명한다.

2. 관련 연구

2.1 ATT&CK & 사이버킬체인 모델 분석

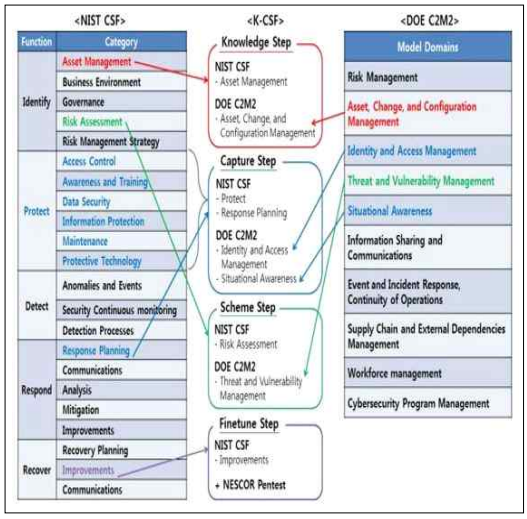


(그림 1) ATT&CK 및 사이버킬체인 모델 분석

사이버킬체인의 정찰과 공격대상에 대한 무기제작 단계에는 PRE-ATT&CK을 악용단계 이후에는 ATT&CK 모델을 맵핑시켜 네트워크 공격 행위를 신속·명확하게 탐지하고 공격행위에 대한 유형을 분류하기 위한 모델이다. 또한, PRE-ATT&CK는 군에서 수집되는 첩보수집 수단인 TECHINT(기술정보), HUMINT(인간정보), 조직정보 등을 활용 및 맵핑시킬 수 있다. (그림 1)을 설명하자면 사이버킬체인 7단계 중 정찰, 무기화, 전달 및 유포 단계는 PRE-ATT&CK 모델을 구성한 것이며 악용, 설치, 명령제어, 목표달성에는 ATT&CK 모델을 맵핑시켜 라이프사이클을 구성한 것이다[3].

2.2 국내 사이버보안 프레임워크 실태

국내 민간·공공 분야의 사이버보안 프레임워크에 대한 연구는 보통 NIST CSF(Cyber Security Framework)을 참조하여 개선 및 도출하고 있다. 민·관 사이버보안 프레임워크에 관한 연구로 기반시설 사이버보안 프레임워크 도출방안(著 권성문)을 제안하였지만 침입탐지를 참조 및 도출하지 않았다[12].



(그림 2) 기반시설 사이버보안 프레임워크[13]

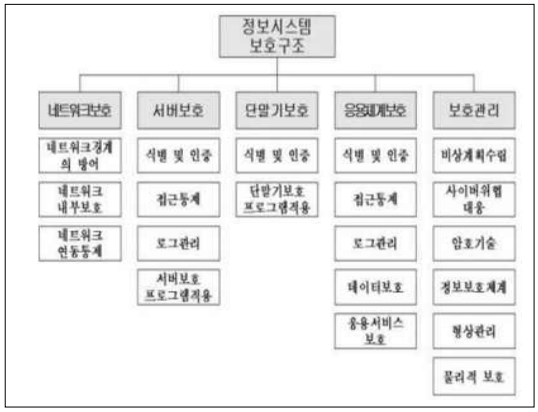
기반시설 사이버보안 프레임워크[12]에 참조된 NIST-CSF(Cybersecurity Framework)[18]는 사이버 보안 위험을 관리하는 Risk 기반 접근법으로 프레임워크 코어, 구현계층, 프로파일의 세부분으로 구성되어 있다. (그림 2)는 NIST CSF의 코어 항목을 중점적으로 주요 기능별(Detect 제외)로 검증하여 K-CSF를 도출한 것이다[12].

국내 사이버보안 프레임워크를 지속적으로 개선 및 도출하고 있으나 군에서는 폐쇄망에 대한 취약점 완화 방안에 관한 명확한 보호대책이 부실하여 국방 네트워크 환경의 내/외부, 잠재적 위협요소가 지속적으로 증가하는 추세이다.

3. ATT&CK 기반 군 내부망 취약점 완화 체계 구축 방안

3.1 국방정보시스템 보호요구사항

국방부는 사이버위협이 고도화됨에 따라 국방사이버안보훈령을 의거하여 국방정보시스템 보호기준과 보호요구사항을 중점적으로 네트워크 보호, 서버 보호, 단말 보호, 응용체계 보호, 보호관리 등 5개의 정보보호 분야별로 구성되어 있어 국방정보체계 도입 시 보안성 검토(기술적, 관리적, 물리적 보안 기준)를 받아 네트워크 보호(19개), 서버 보호(36개), 단말 보호(11개), 응용체계 보호(82개), 보호 관리(87개)를 모두 충족해야 만 구축 및 운영할 수 있다[15]. 상세한 도표는 (그림 4)와 같다.



(그림 3) 국방정보시스템 보호구조[15]

분야	세부분야(통계 수)	보호통제항목(통계 수)	보호요구사항(통계 수)
네트워크 보호	3	6	19
서버 보호	4	13	36
단말기 보호	2	4	11
응용체계 보호	5	28	82
보호 관리	6	26	87
총 계	20	77	235

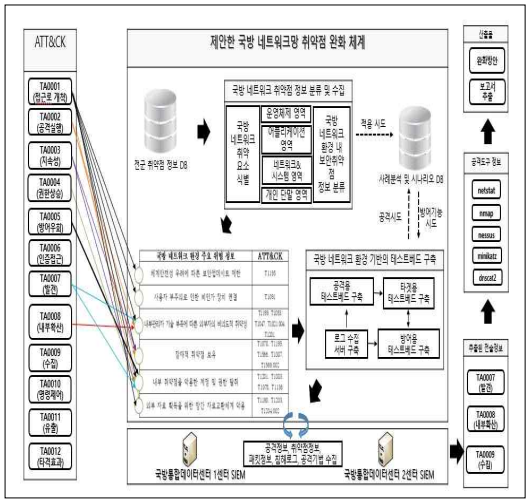
(그림 4) 보호통제항목 및 보호요구사항 통계[15]

3.2 군 내부망 취약점 완화 체계 적용 방향

국내 민·관 영역 사이버보안 프레임워크는 사이버 상황인식(Cyber Situational Awareness)을 중점적으로 다루어 개선 및 도출하고 있으나 주요기반시설의 사이버보안 프레임워크[12]에서는 사이버 상황인식의 핵심인 침입탐지를 참조 및 도출하지 않는 부분이 존재한다. 군은 국내 사이버 보안 프레임워크의 부족한 부분을 참고하여 구축하고자 하는 군 내부망 취약점 완화 체계를 ATT&CK를 중점적으로 활용할 것이며 군 특수성이 지닌 국방사이버안보훈령(국방정보시스템 보호기준 및 요구사항)과 맵핑시킬 수 있는 ATT&CK 기반의 국방 네트워크망 취약점 완화 체계를 구축 및 검증할 것이다. 그리고 검증된 완화체계는 국방

네트워크 환경에 대한 사이버공격을 효율적으로 보호하여 주요 위협을 완화시킬 수 있는 장점을 가진다.

3.3 ATT&CK 기반 군 내부망 취약점 완화 체계 설계



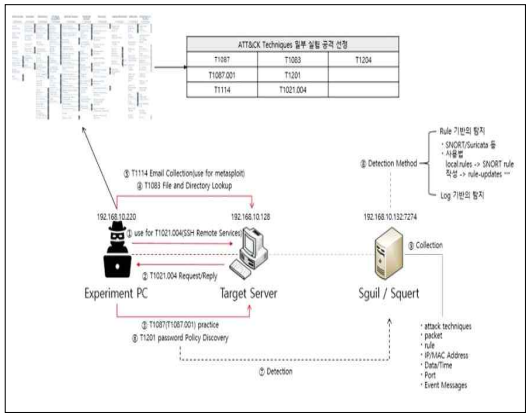
(그림 5) 군 내부망 취약점 완화 체계 구축

MITRE社 및 국내 민·관에서는 ATT&CK 기반으로 한 사이버보안 프레임워크는 개선 및 설계하고 있으나 모두 비공개로 전환하여 참고할 수 있는 사항이 극히 일부분이다. 군은 (그림 5)와 같이 국방 네트워크용 취약점 완화 체계를 제안했다. 목표는 군 내부망 취약점 완화 및 사이버방호 능력 수준을 보강할 목적으로 제안했으며 구축방법은 다음과 같다.

- 국방 네트워크 환경에서 발생되는 다양한 취약 요소를 사이버사령부 및 각 군 취약점 정보 데이터베이스를 활용하여 국방정보시스템 보호기준을 토대로 운영체제, 어플리케이션, 네트워크, 개인 단말 영역별로 취약점 정보를 수집하여 분류한다.
- 수집된 취약점 정보들을 활용하여 국방 네트워크 환경 주요 위협 정보를 추출하여 ATT&CK 기반으로 시나리오를 작성하여 예상된 전술 정보를 적용 한다.
  - 추가적으로 사례분석 및 시나리오 DB에 적용을 시도한다.
- 내부망과 유사한 환경의 테스트베드와 보호시스템(IPS/Firewall/DDoS 등)을 가상으로 구축한 후 시나리오 DB를 통해 모의 공격을 수행하여 방어기능을 할 수 있는 정보를 추출한다.
- 추출된 방어기능 정보와 추가적으로 공격정보, 취약점 정보, 패킷정보, 침해로그, 공격기법 정보 수집 등을 국방통합데이터센터 1센터와 2센터의 SIEM을 통해 국방 네트워크 환경에서 발생할 수 있는 공격유형과 원인, 특징들을 분석할 수 있다.
- 분석된 정보에는 ATT&CK 일부 전술정보인 TA0007, TA0008, TA0009와 해당 전술에서 사용된 공격도구도 추출할 수 있어 상관분석을 통해 완화 방안을 수립할 수 있다.

4. 국방 사이버위협 시나리오 및 제안 모델 검증

4.1 국방 네트워크 환경에서 사이버위협 시나리오



(그림 6) 공격 시나리오 구성

- 공격 시나리오
  - 공격 목적
    - 잠재적 위협을 활용하여 군 내부망 침투
      ① 공격자는 군 내부망을 침투하기 위해 사전에 SNS나 각 군 인터넷 홈페이지를 탐색하여 정보를 수집

② 침투하기 위한 공격유형과 정보, 도구들을 확보하기 위해 MITRE社 ATT&CK 정보를 수시로 확인

③ 공격자는 SNS를 통해 국방 네트워크망에 대한 구성과 해킹 사례를 수집하게 되었고, 정보 분석을 위한 악성코드 및 Tool를 다운로드한 후 각 군 인터넷 홈페이지에 정상적인 파일을 위장한 백도어 및 악성코드 삽입

④ 관리자는 의심 없이 해당 파일을 열람하였고, 심어진 백도어 및 악성코드가 웹서버에 실행되어 서비스 거부 및 내부 서버 정보와 일부 자료 획득

⑤ 내부 서버 정보를 활용하여 계정 및 패스워드 정보, 네트워크 연결 상태, 포트 정보, 취약점 점검, 원격 접속 및 권한 상승을 통해 군 내부망 침투 성공

• 공격 시나리오 준비 및 환경 구성

- 준비사항
  • Experiment PC : Kali Linux(Metasploit)
  • Target Server : ubuntu
  • Sguil / Squert : ubuntu 계열

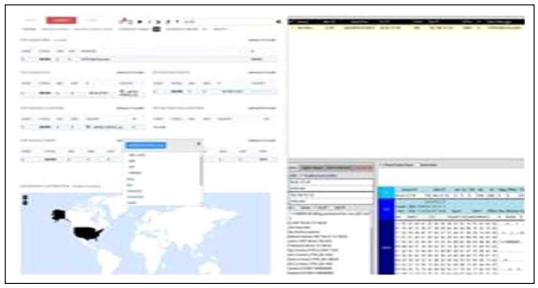
- 실행내용
  • ATT&CK Matrix를 이용하여 Techniques 일부 실험용 공격 기법 선정
  • Techniques ID : T1087(001), T1114, T1083, T1201(004), T1204

- 공격 순서
  • T1021.004 SSH Remote Services
  • T1087(001) Account Discovery(Local)
  • T1083 File and Directory Lookup
  • T1114 Email Collection
  • T1201 Password Policy Discovery

- 공격 시나리오에 활용된 도구
  • netstat을 사용하여 연결 상태 정보 조회
  • nmap을 사용하여 포트 스캔 수행
  • nessus을 사용하여 취약점 스캔 수행
  • mimikatz를 통한 계정 및 패스워드 정보 획득
  • dnscat2 tool을 이용한 시스템 통제

4.2 제안 모델 검증

(그림 7)은 ATT&CK Tactics 중 접근로 개척 단계에 포함되어 있는 Techniques ID 1078 Valid Account에 대한 데이터 소스를 수집하기 위해 Squert와 Sguil 프로그램을 사용하여 시각화를 구현하였다. 해당 기법에 대한 공격 시나리오 및 도구를 활용하여 공격 수행 시 특정 명령어, 경로, 이름 등에 대한 rule을 작성한 후 적용하여 탐지시스템에 해당 공격이 탐지되었다. 수집된 정보는 공격자IP, 공격대상IP, Port 정보, 이벤트 정보, TTL 정보, 패킷정보, 최초 탐지 시간 및 날짜, 장소 등 공격기법에 대한 정보를 수집 및 분석이 가능하다.



(그림 7) 실험 결과(시각화 구현)

- 탐지 및 방법
  • rule 기반의 탐지 / log 기반의 탐지
  (그림 8)과 같이 snort / suricata / yara 등을 이용하여 공격행위에 대한 특정 명령어 및 경로 등을 한정적으로 작성(local.rules)하여 rule-updates를 통해 적용

- 수집된 정보
  • attack techniques info
  • packet
  • rule info
  • IP/MAC/PORT
  • Date/Time info

• Event Messages

- rule 시그니처 및 적용

```
</etc/snort/rules/local.rules>
alert tcp any any -> any any(msg:"T1078 V
alid Account"; content:"ssh @"; content:"teln
et"; content:"su"; content:"/etc/passwd"; noca
se; sid:3000001;)
alert tcp $EXTERNAL_NET any -> $HO
ME_NET any (msg:"T1078 Valid Account";
content:"git"; content:"./dnscat"; content:"dn
scat"; content:"session"; nocase; sid:3000002;)
alert tcp any any -> any any(msg:"T1078 V
alid Account"; content:"password"; content:"/
"; content:"shadow"; nocase; sid:3000003;)
</ >
# snort -c /etc/snort/rules/local.rules.
# sudo rule-update
```

(그림 8) Rule 시그니처 및 적용(일부)

5. 결 론

본 연구에서는 ATT&CK 기반의 국방 네트워크망 취약점 완화 체계를 설계하여 검증하였다. 군 특수성을 지닌 군 내부망 주요 위협 정보 및 국방정보시스템 보안 요구사항을 파악하고, 공격자의 의도파악과 전술, 기법 및 절차 정보(ATT&CK Framework)를 적용하여 국방 네트워크 환경에 대한 사이버공격을 효율적으로 보호해주는 군 내부망 취약점 완화 체계 구축을 연구 및 검증하는데 효과를 발휘하였다. 향후 계획은 ELK(Elasticsearch, Logstash, Kibana) 기반으로 구현함으로써 국방 네트워크 취약점 완화 체계를 프레임워크화하여 새로운 패러다임의 국방 사이버보안 프레임워크를 설계할 계획이다.

참고문헌

[1] 최인수, “국방사이버방호 발전방향”, 한국국방연구원 주간국방논단, 제1659호(17-8), pp 1-8, 2017.

[2] 김재광, “사이버안보 위협에 대한 법제적 대응방안”, 경북대학교 법학연구원 법학논고, 제58권, pp 145-177, 2017.

[3] MITRE ATT&CK, https://attack.mitre.org

[4] 안광현, "ATT&CK 기반의 내부망 취약점 완화를 위한 사이버위협 대응 방안 연구“, 한국인터넷정보학회 국방정보기술연구회, 제21권, 제1호, pp 17-18, 2020.

[5] Houhua He and Lei Yu, "PPIDS : A Pyramid-Like Printer Intrusion Detection System Based on ATT&CK Framework", International Conference on Information Security and Cryptology, pp277-290, 2019.

[6] 최광복, “국가사이버위협에 따른 국방사이버대응 실태”, 한국정보보호학회 정보보호학회지, 제22권, 제8호, pp 36-40, 2012.

[7] 임병하, “정보보안을 위한 망분리 구축에 대한 연구”, 중앙대학교 한국전자무역연구소 제12권 제4호, pp 1-21, 2014.

[8] 안정언, “사이버전 모의훈련 모니터링을 위한 종합상황도 구성 방안 연구”, 한국인터넷정보학회 국방정보기술연구회, 제21권, 제1호, pp 9-10, 2020.

[9] 한인성, 서한샘. 오행록 “사이버위협 분석을 위한 ATT&CK 기반의 자동 사이버 공격 시뮬레이션 도구에 관한 연구”, 한국군사과학기술학회 종합학술대회 정보통신부문, 제1권, 제1호, pp 1115-1116, 2019.

[10] 송재익, “한국군 합동 사이버작전 강화방안 연구”, 한국군사문제연구원 한국군사, 제2호, pp 147-186, 2017.

[11] 한명길, 김용현, “사이버전사의 훈련을 위한 시스템 구축 방안 연구”, 한국정보보호학회 정보보호학회논문지, 제26권, 제2호, pp 533-540, 2016.

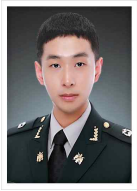
[12] 권성문, “기반시설 사이버보안 프레임워크 도출 방안”, 한국정보보호학회 정보보호학회논문지, 제27권, 제2호, pp 241-250, 2017.

[13] 이수연, “주요기반시설 서비스의 안정적 운영을 위한 보안 프레임워크 설계에 관한 연구”, 한국IT서비스학회 한국IT서비스학회지, 제15권, 제4호, pp 63-72, 2016.

[14] 전병욱, “국방정보통신망 개선 및 보호를 위한 계층적 접근방법”, 한국국방연구원 국방정책연구 특집논문, pp 1-26, 2003.

[15] 국방부, “국방사이버안보훈령”, 국방부 훈련 제 2234호, 2018.12.26
[16] 조창섭, “보안관제 조직을 위한 사이버보안 프레임워크 개선에 관한 연구”, 한국융합보안학회 융합보안논문지, 제19권, 제1호, pp 111-120, 2019.
[17] CYFIRMA, "cyber-situational-awareness“, 2020.
[18] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cyber security", April, 2018.
[19] SANS, "Measuring and Improving Cyber Defense Using the MITRE ATT&CK Framework", July, 2020.

〔저자소개〕



안 광 현 (Gwang-Hyun Ahn)
2018년 2월 극동대 산업보안학과 공학사
2018년~현재 국방부
2020년~현재 한국융합보안학회 종신회원
2020년 9월~현재 세종대학교 컴퓨터공학 석·박사통합과정

email : rhkdgus8781@sju.ac.kr

이 한 희 (Hanhee Lee)
1993년 2월 인제대학교 이학사
1993년~현재 국방부
2000년 1월 국방대학교 이학석사
2017년 10월 University of SouthWest America 심리경영학 박사

email : runhoney69@gmail.com

박 원 형 (Won-Hyung Park)
2002년 서울과학기술대 산업정보시스템 공학사
2005년 서울과학기술대 정보산업공학과 공학석사
2009년 경기대 정보보호학과 이학 박사
2012년~2020년 극동대학교 사이버보안학과 부교수/학과장
2016년 성균관대 컴퓨터교육학과 박사수료
2020년~현재 상명대학교 정보보안공학과 부교수

email : whpark@smu.ac.kr

강 지 원 (Ji-Won Kang)
1988년 2월 금오공대 전자공학 학사
1997년 2월 연세대 컴퓨터과학 (정보보호 전공) 석사
2012년 8월 경기대 정보보호학 박사
2017년 9월~현재 세종대학교 컴퓨터공학과 교수

email : jwkang@sejong.ac.kr