정 보 보 호 학 회 지
제24권 제5호, 2014. 10

실시간 분산 제어시스템 보안

신 인 철*

요 약

최근, 에너지, 정보통신, 방위산업, 정부, 금융 등 국가기반시설(national critical infrastructures)들에 대한 사이버 보안 위협이 급격히 증가하고 있으며 이에 대응하기 위해 미국을 비롯한 주요 국가에서는 감시제어 및 데이터 취득 시스템(SCADA: Supervisory Control and Data Acquisition)에 대한 사이버 보안에 많은 노력을 기울이고 있다. 특히, 주요 국가기반시설은 다양한 실시간 분산 제어시스템 및 네트워크를 통해 사이버 세계(cyber world)와 물리적 세계(physical world)를 연계한다. 하지만 이 같은 역동성(dynamic), 확장성(scalability), 다양성(diversity)으로 특징지어질수 있는 실시간 분산 제어시스템간의 상호연결과 연동을 통해 구성되는 해당시설은 기존의 보안기술 적용을 통해 보안성향상을 기대할 수 없다. 따라서 본고에서는 실시간 분산 제어시스템과 다양한 네트워크로 구성되는 기반시설들을 대상으로 하는 여러 가지 보안 위협 및 특징을 소개하고 이에 대응하기 위한 전략 및 연구기술 동향을 간략히 서술한다.

Ⅰ. 서 론

행정안전부에 따르면, 국가기반시설은 에너지·통신·교통·금융·의료·수도 등 국가기반체계의 보호를 위하여 계속적으로 관리할 필요가 있다고 인정되는 시설 중 다른 기반시설이나 체계 등에 미치는 연쇄효과, 둘 이상의 중앙행정기관의 공동대응 필요성, 재난이 발생하는 경우 국가안전 보장과 경제·사회에 미치는 피해규모 및 범위, 재난의발생가능성 또는 그 복구의 용이성을 고려하여 지정된 시설로 규정하고 있다. 하지만, 현재 국민의 생명과 재산, 경제에 막대한 영향을 미칠 수 있는 에너지(발전소 및 송・변전시설) 정보통신(주요 전산시스템) 교통수송(주요 철도, 공항, 복합 화물기지, 무역항, 고속・국도), 금융, 산업(방위산업체), 의료・보건(혈액원, 백신제조업체), 원자력(원자력발전소), 건설・환경(소각 및 매립시설, 종말처리장), 식・용수(다목적댐, 정수장)시설 내 물리적 공간과 사이버 공간의 개별적인 운영으로 인하여, 재해 사각지대가 존재할 뿐 아니라 해당 국가기반시설을 대상으로 하는 사이버공격 발생 시 그 파급효과는 전쟁 이상의 재앙으로 이어질 수 있다.

국가기반시설들은 다양한 제어시스템과 사이버시스템으로 구성되어 있다. 특히 제어시스템은 실시간에 즉각적으로 자료를 수집, 처리, 제어를 결정하여 수행하는 독립적인 실시간 시스템(센서, 액추에이터 및 원격단말기)들로써, 상호의존적으로 동작 가능하도록 지리적으로 넓은 지역에 분산되어 다양하고 복잡한 형태로 구성, 상호연계 및 연동을 통해 네트워크화(networked) 되는 실시간 분산 제어시스템이다. 기존 정보통신기술에서 사용되는 네트워크는 데이터 교환을 통한 통신을 주된 역할로 분류한다면, 실시간 제어 분산 제어시스템은 상태정보, 데이터, 제어신호, 통신 메시지 등의 흐름을 위한 통합 감시제어 및 데이터취득 시스템의 일부로 정의한다. 이 같은 특성을 통해 알 수 있듯, 제어실패(control failure)로 인한 피해는 정확한 예측이 불가능한 다양한 형태로 발생하기 때문에 실시간 분산 제어시스템은 어떠한 환경에서도 동작 가능하도록 무중단 운영이 보장되어야 한다.

하지만, 이와 같은 실시간 분산 제어시스템들은 과거 안전성 보장을 위해 물리적으로 분리된 독립망으로 구성되었으나 현재는 효율적인 시스템자원 관리 및 자료수집을 목적으로 공유 및 협력네트워크로 점차 구축됨으로써 다양한 사이버 공격들에 노출되기 시작하였다[1-19]. 특히나, 기존의 데이터 손실 및 노출 최소화를 목적으로 하는 IT(Information Technology) 보호기술들은 이 같은 특성을 지니고 있는 제어시스템에 적용할 경우, 적절한 성능을 발휘하지 못할 뿐 아니라 심지어

* 목포대학교 정보보호학과 (ishin@mokpo.ac.kr)

보호대상 시스템의 성능하락 혹은 보호대상 시스템을 위험에 빠뜨릴 수도 있다. 이를 극복하기 위해 많은 보안기술 연구가 수행되었으며, 심층방어(Defense-in-Depth)기법을 통한 네트워크 보호기법이 현재까지 제시되고 있다. 심층방어기법에서는 기능적 특성분석을 기반으로 상호 연동되는 기기 및 네트워크를 악성행위나 혹은 네트워크 침입으로부터 보호함으로써, 가용성 (availability), 감내 (tolerance) 및 생존성 (survivability)을 극대화함으로써 보호대상 제어시스템의 주요 기능 및 데이터들을 보호하는데 그 목적이 있다. 본 지에서는 실시간 분산 제어시스템을 위협하는 공격과 이에 대응하는 심층방어, 공격완화 및 복구기법들을 간략히 소개한다.

Ⅱ. 실시간 분산 제어시스템 개요

기존의 제어시스템들은 외부로 부터의 접근이 불가능한 격리된 네트워크 및 운영환경에서 설치부터 지속적인 유인(有人)감시를 통해 보호되었으나 다양한 운용 및 구동 환경(대중교통, 상·하수도, 에너지 생산 및 화학공장 등)으로의 변화로 인해 이 같은 보호가 불가능한 새로운 형태의 외부 공격이 예상된다. 또한, 다양한 사회 및 경제적 변화로 인해 외부 뿐 아니라 내부로부터의 예측 불가능한 공격이 발생가능하며 이를 극복하기 위해서는 새로운 보안 기법이 요구되고 있다.

현대의 제어시스템은 효율적인 자원관리 및 비용절감을 위해 신속, 정확 그리고 최적화된 운영환경 제공을 그 목적으로 하고 있으며 이를 위해서는 다양한 네트워크연계가 필수적이다. 예를 들어, 스마트그리드(Smart Grid)에서 사용되고 있는 동기위상기(syncrophasor)는 실시간으로 전압 및 전류를 측정하여 네트워크를 통해 할당된 분산 제어시스템으로 전달하며, 해당 시스템의 제어 알고리즘은 다양한 인자 값들과 함께 전달된 정보를 이용하여 에너지 전달 효율성을 극대화하기 위한 연산을 수행한다. 본 연산에는 운영적인 측면에서 사이버 공격으로부터 전체 시스템을 보호하기 위한 보안 기능이 필요할 뿐 아니라 보안과는 관련이 없지만 개인정보와 같은 민감성 정보를 유출 요소를 제거하기 위한 비운영 측면에서의 보안기능 또한 요구된다.

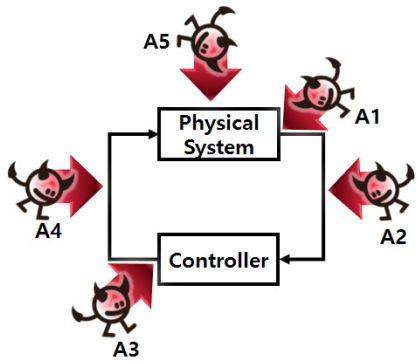
추가적으로, 제어시스템은 앞서 언급한 의도된 사이버 공격으로부터 시스템을 보호하기 위한 보안 조치뿐 아니라 비적대적인(non-hostile)요소로 부터의 의도되지 않은 오류로부터의 발생 가능한 위협을 최소화해야 한다. 다양한 분야에 대한 제어시스템 활용은 예측하지 못한 시스템 복잡도를 야기하며 이로 인해 앞서 언급한 의도되지 않은 위험도가 필연적으로 증가하고 있다.

2.1. 제어 시스템대상 공격

그림 1은 일반적인 제어시스템 개요 및 공격가능 대상지점을 표시하였으며, 해당 내용은 다음과 같다.

그림 1에서 감지기에서 측정한 데이터, 작동기(actuator)로 보내어지는 제어명령이 있으며, 제어기(controller)는 일반적으로 연계된 물리시스템(physical system)의 상태정보를 추적하기 위한 예측 알고리즘과 제어 명령을 선택하기 위한 제어 알고리즘으로 나누어진다.

제어시스템을 대상으로 하는 공격은 크게 5가지 형태로 분류된다. A1과 A3는 센서나 제어시스템으로부터의 정상적인 메시지가 아닌 부정확한 측정값, 시간, 전송기기 식별자 등을 포함 등의 조작된 임의 정보를 의미한다. A2와 A4는 서비스거부 공격이 발생 가능한 지점으로서 관련된 측정데이터를 제어 시스템에서 수신하지 못하거나 물리적 시스템에서 제어명령을 수신을 불가능 하도록 공격가능하다. A5의 경우 외부에서 작동기 등과 같이 외부에 설치된 물리 시스템에 직접적으로 공격 가능한 지점을 말한다. 많은 실험과 연구를 통해 보안 알고리즘만을 통해 이와 같은 물리적 사이버공격(physical cyber attack)들을 방어 하기는 불가능하다고 알려져 있으며, 이로 인해 복합적인 물리적 방호시스템 또한 요구되고 있다[11-15].



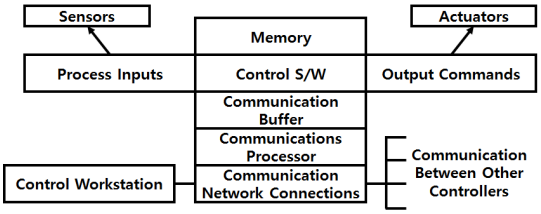
〔그림 1〕 분산 제어시스템 및 공격가능 대상 지점

2.2. 실시간 분산 제어 시스템 (Real-Time Distributed Control Systems) 구조

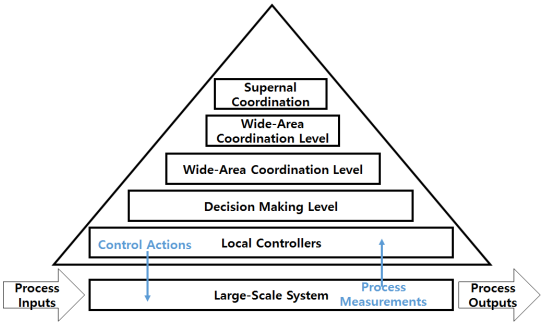
설명하는 실시간 분산 제어시스템은 센서, 제어기 및 작동기 등으로써, 몇 가지의 단순반복적인 기능들을 수행하며 통신 네트워크를 통해 상호연동 가능한 연산기기를 의미한다. 그림 2는 실시간 분산 제어시스템의 주요 기능을 설명하며, 이는 센서의 측정값 입력, 출력값 연산, 작동기로의 제어값 송신 기능 등을 포함한다.

이 같은 실시간 분산 제어시스템은 그림 3과 같이 계층적으로 구성되어 여러 단계의 시스템을 통해 운영된다. 일반적으로 두 가지 제어 원형 형태의 실시간 분산 제어시스템이 존재한다.

1. 동적원형 기반 시스템: 지속적인 흐름의 형태를 가진 정보를 제어하는 시스템으로 특정하게 제한된 구간 내에서 관련 정보가 유지될 수 있도록 하는 피드백 제어(feedback control)를 수행한다.
2. 상태원형 기반 시스템: 관련된 물리적 기기들의 전이 정보를 감시하고 유지, 갱신, 제어 등의 명령을 통해 특정한 상태로 유지한다.



〔그림 2〕 실시간 분산 제어시스템의 구조



〔그림 3〕 실시간 분산 제어시스템의 계층적 연동 구조

Ⅲ. 실시간 분산 제어 보안

3.1. 실시간 분산 제어 보안 이슈

실시간 제어시스템에 대한 사이버 취약점은 다음과 같이 알려져 있다[11].

1. Inadequate policies, procedures, and culture governing control system security
2. Inadequately designed networks with insufficient defense in depth
3. Remote access without appropriate access control
4. Separate auditable administration mechanisms
5. Inadequately secured wireless communication
6. Use of a non-dedicated communications channel for command and control
7. Lack of easy tools to detect/report anomalous activity
8. Installation of inappropriate applications on critical host computers
9. Inadequately scrutinized control system software
10. Unauthenticated command and control data

이 같은 취약점을 극복하기 위한 요구사항으로 신뢰성(Reliability), 대응능력(Resiliency), 보안(Security)는 안전한 실시간 분산 제어시스템 구축 및 운영을 위한 3가지 요소로 알려져 있다[12,13]. 신뢰성 확보를 위해 시스템 장애 발생 비율을 낮추며, 대응능력을 극대화하기 위해 시스템 감내(tolerance)를 극대화하기 위한 설계 및 구현이 요구된다.

표 1은 실시간 분산 제어시스템을 외부의 침입으로 보호하기 위한 심층방어기법을 연구 개발하는 핵심으로 취약점 발생 요소들을 설명하고 있다[20]. 또한, 표 2는 실시간 분산 제어시스템의 시스템 장애 발생 원인을 설명하고 있다.

3.2. 실시간 분산 제어시스템 장애 형태

실시간 분산 제어시스템에서 탐지가 어려운 장애발생 형태는 다음과 같이 분류된다[16].

Fail Arbitrary - 오류 식별 혹은 장애 감내기법들에

〔표 1〕 실시간 분산 제어시스템 시스템 장애 발생원인

발생 원인	설명
Random component failure	임의의 기기 혹은 제어시스템의 시스템 장애 발생
Common cause failure	연결되거나 공유되는 네트워크 공간에 대한 장애를 통해 관련 실시간 분산 제어시스템의 장애 발생
Latent fault (hardware or software)	소프트웨어나 하드웨어의 디자인 과정에서 발생한 오류로서 제조 과정 후 설치 혹은 제어시스템 운용 중에 발생하는 장애
Incorrect input (signal) values	센서나 제어시스템과 센서를 연결하는 네트워크가 정상적으로 동작하지 않거나 장애 시 발생되는 부정확한 메시지로 인한 장애
Incorrect application (software)	소프트웨어 구현이나 생산단계 이후 운용 중 네트워크를 통해 잘못 설치된 프로그램을 통한 장애 발생
Incorrect operating parameters (set point, alarm limits, etc.)	제어시스템의 설치이후 부정확한 환경설정을 통해 발생하는 시스템 장애

탐지되지 않고 발생한 장애

Fail Silent - 정확한 명령만을 생성하거나 혹은 명령어를 전혀 생성하지 않는 장애로서 오류관련 메시지는 만들지 않는 장애

Fail Bounded - 시스템이 부정확한 출력을 만들어 내지만, 특정한 범위 내에 존재하는 값들로서 오류 탐지가 불가능한 장애

이와 같은 장애로 인해 독립적으로 동작하는 실시간 분산 제어시스템은 아래의 4가지 상태로 전이된다.

1. Off-Line 상태 - 동작하지 않음
2. Degrade 상태 - 성능이 저하됨
3. Erratic 상태 - 타 기기에서 이해할 수 없는 정해지지 않은 출력 생성
4. Alien 상태 - 타 기기 및 제어시스템에 악 영향을 미치는 출력 값 생성

이 같은 상태는 직접적으로 연결된 기기의 장애를 발생, 네트워크를 통한 장애 전파 혹은 공유 자원을 통해 장애를 발생시키게 된다. 또한, 이 같은 장애는 지속 시간에 따라 영구장애(permanent failure), 일시장애(temporary failure) 및 순간장애(transient tailure)로 분류된다.

〔표 2〕 실시간 분산 제어시스템 침입공격 발생원인

발생 원인	설명
Change software code to achieve a new control object	펌웨어등과 같은 제어시스템 내 프로그램 수정을 통해 임의의 프로그램 동작 변경
Introduce incorrect (spoofing) input signals	네트워크에 대한 접근이 가능하여 시스템 장애를 일으킬 수 있는 통신 메시지를 제어시스템으로 전송
Generate incorrect output values or commands	네트워크에 대한 접근이 가능하여 시스템 장애를 일으킬 수 있는 통신 메시지를 물리시스템으로 전송
Insert messages to indicate incorrect operational status of parts of system	제어대상 물리 시스템의 상태 정보를 임의로 조작하여 전체 시스템의 상태 정보를 조작
Collect operational information (data, set points)	제어대상 물리 시스템의 상태 정보를 손쉽게 취득하여 시스템의 주요정보 탈취
Interrupt or corrupt communications between control system components	제어시스템과 물리시스템 간 통신 메시지를 조작 • Corruption • Unintended Repetition • Incorrect Sequence • Loss • Unacceptable Delay • Insertion • Masquerade • Addressing • Broadcast Storm (Denial of Service) • Babbling Idiot (Commission Fault) • Inconsistency (Byzantine Generals'Problem) • Excessive Jitter • Collision

3.3. 실시간 분산 제어시스템대상 공격 형태

다양한 연구들이 앞서 언급한 실시간 분산 제어시스템의 장애를 유발하는 공격 모델(cybersecurity attack-vulnerability-damage model)을 개발하였으며 그 내용은 표 3과 같다[16]. 이 같은 공격 모델에서는 해당 제어시스템이 수행하는 작업의 중요성으로 인해 오류 발생이후 오동작으로 인한 네트워크 내 비정상 메시지 유입 시간을 중요 고려 대상으로 인식하고 보안기술을 개발해야 한다고 언급하고 있다.

〔표 3〕 Cybersecurity AVD Model

Attack			Vulnerability Weakness	Damage		
Origin	Action	Target		State Effect	Performance Effect	Severity
Local Remote	Probe Scan Flood Authenticate Bypass Spoof Eavesdrop Misdirect Read/Copy Terminate Execute Modify Delete	Network Process System Data User	Configuration Specification Implementation	None Availability Integrity Confidentiality	None Timeliness Precision Accuracy	None Low Medium High

NIST(National Institute of Standards and Technology)에서는 능동(active) 및 수동(passive) 공격에 대한 내용을 기반으로 공격을 분류하기도 한다.

Ⅳ. 실시간 분산 제어시스템대상 공격 대응

핵 발전소관련 보안을 지속적으로 연구해온 미국의 Oak Ridge 국립연구소는 안전한 실시간 분산 제어시스템을 구축하기 위한 다음의 8가지 보안 기법들을 제시하고 있다.

1. Authentication
2. Redundancy and diversity
3. Design and Analysis Principles
4. Specification and design of continuously available secondary systems
5. Distributed, federated systems that do not depend on a central system as used in the Purdue Model
6. System recovery of critical functions for fail-safe or “safe mode” end state
7. Robust networked control systems
8. Defense in depth where de-perimeterized protection is distributed throughout the control system

이 같은 보안 기법들은 기존의 사이버보안 기술들을 기반으로 새로이 구성한 것으로서 참고 내용은 표 4와 같다.

〔표 4〕 기존 사이버보안 관련 자료

이름	설명
DHS Catalog	Catalog of Control Systems Security: Recommendations for Standards Developers
DHS CS2SAT	Control System Cyber Security Self-Assessment Tool (CS2SAT)
NIST SP 800-82	DRAFT Guide to Industrial Control Systems (ICS) Security
NIST SP 800-30	Risk Management Guide for Information Technology Systems
NIST SP 800-53 Rev. 3	Recommended Security Controls for Federal Information Systems and Organizations
NIST SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)
AMI SEC SSR	AMI System Security Requirements
ISA99	Industrial Automation and Control System Security
ISA100	Wireless standard for industrial automation

Ⅴ. 결 론

현대 각국의 주요 국가기반시설은 다양한 실시간 분산 제어시스템을 이용하여 사이버 세계와 물리적 세계를 연계한다. 하지만 역동성(dynamic), 확장성(scalability), 다양성(diversity)으로 특징지어질수 있는 실시간 분산 제어시스템간의 네트워크 상호연결과 연동을 통해 구성되는 해당시설은 기존의 보안기술 적용만으로 보안성향상을 기대할 수 없다. 본 지에서는 이 같은 실시간 분산 제어시스템의 특성 및 보안 위협을 나열하고 이를 극복하기 위한 대응 기술의 연구 방향에 대해 논의하였다.

참 고 문 헌

[1] J. Eisenhauer, P. Donnelly, M. Ellis, and M. O'Brien, "Roadmap to Secure Control Systems in the Energy Sector," Energetics Incorporated, sponsored by the U.S. Department of Energy and the U.S. Department of Homeland Security, January 2006.

[2] U. S. G. A. Office, Critical infrastructure protection: Multiple efforts to secure control systems are under way, but challenges remain, Technical Report GAO-07-1036, Report to Congressional Requesters, 2007.

[3] R. J. Turk, Cyber incidents involving control systems, Technical Report INL/EXT-05-00671,Idaho National Laboratory, October 2005.

[4] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," ACM Trans. Programming Languages and Systems 4(3), 382–401, July 1982.

[5] J. Sykes, K. Koellner, W. Premerlani, B. Kasztenny, and M. Adamiak, "Synchrophasors: A primer and practical applications," Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, 2007. PSC 2007, pp.213–240, March 13–16, 2007.

[6] S. Amin, A. Cardenas, and S. Sastry, "Safe and Secure Networked Control Systems Under Denial-of-Service Attacks," Hybrid Systems: Computation and Control, Lecture Notes in Computer Science. Springer Berlin/Heidelberg, 30, pp. 31–45, April 2009.

[7] "The Smart Grid: An Introduction," prepared for the U.S. Department of Energy by Litos Strategic Communication under contract No. DE-AC26-04NT41817, Subtask 560.01.04, http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages.pdf(checked 9/21/2009).

[8] IEEE 100, The Authoritative Dictionary of IEEE Standards Terms, Seventh Edition, IEEE, 2000.

[9] M. Jamshidi, Large-Scale Systems, Series Volume 9, North-Holland Series in System Science and Engineering, Elsevier Science Publishing, Inc., pp. 103–104, 1983.

[10] H. J. Reekie and R. J. McAdam, A Software Architecture Primer, Angophora Press, Sydney, Australia, 2006.

[11] "Top 10 Vulnerabilities of Control Systems and their Associated Mitigations－2006," North American Electric Reliability Council, Control Systems Security Working Group, U.S. Department of Energy, National SCADA Test Bed Program, March 16, 2006.

[12] K. Stouffer et al., "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, U.S. Dept. of Commerce, Special Publication 800-82, Draft, September 2008.

[13] Common Cybersecurity Vulnerabilities Observed in Control System Assessments by the INLNSTB Program, INL/EXT-08-13979, Idaho National Laboratory, November 2008.

[14] R. Kisner et al., Design Practices for Communications and Workstations in Highly Integrated Control Rooms, NUREG/CR-6991, September 2009.

[15] L. Xie et al., "Data Mapping and the Prediction of Common Cause Failure Probability," IEEE Trans. on Reliability 54(2), June 2005.

[16] J. C. Cunha et al., "A Study of Failure Models

in Feedback Control Systems," The International Conference on Dependable Systems and Networks (DSN), Göteborg, Sweden, 1 – 4 July 2001.

[17] T. Fleury et al., "Towards a Taxonomy of Attacks Against Energy Control Systems," Proceedings of the IFIP International Conference on Critical Infrastructure Protection, March 2008.

[18] P. Marti et al., "Jitter Compensation for Real-Time Control Systems," Real-Time Systems Symposium, 2001 (RTSS 2001) Proceedings, 22nd IEEE, Dec. 3 – 6, 2001.

[19] P. Marti et al., "An Integrated Approach to Real-time Distributed Control Systems Over Fieldbuses," pp. 177 – 182 in 8th IEEE International Conference on Emerging Technologies and Factory Automation, 2001 Proceedings, Vol. 1, 2001.

[20] R. Kisner et al., Design Practices for Communications and Workstations in Highly Integrated Control Rooms, NUREG/CR-6991, September 2009.

〈저 자 소 개〉

신 인 철 (Incheol Shin)
정회원

2002년 2월 : 한성대학교 컴퓨터공학과 졸업
2006년 8월 : University of Florida 컴퓨터공학과석사
2010년 8월 : University of Florida 컴퓨터공학과 박사
2010년 6월~2014년 2월 : 한국전자통신연구원 부설 국가보안기술연구소 선임연구원
2014년 3월~현재 : 국립목포대학교 정보보호학과 조교수
관심분야 : 컴퓨터공학, 네트워크, 정보보호