정성훈 (Seonghoon Jeong)

Ph.D.   Phone: +82-10-6279-6283
Postdoctoral Research Associate   E-mail: seonghoon@korea.ac.kr
BK21 FOUR R&E Center for Cybersecurity, Korea University
Room #408-1, Robot Convergence Building, 145 Anam-ro, Seongbuk-gu, 02841 Seoul, Republic of Korea

About.—I investigate and address system security challenges through a data-driven approach that utilizes machine learning and deep learning methodologies. I have experience in a wide range of real-world services, including server-side online game transactions, root DNS servers, mobile payment transaction data, and vehicle system intrusion datasets.

Recently, my focus has been on vehicular system security as well as intrusion detection—a research area that requires urgent attention, given the severe consequences of compromised vehicle systems. Specifically, I have developed a standardized intrusion prevention system for connected vehicle systems to offer practical solutions to both industry and researchers in academia.

I have academic experience in teaching practical system hacking and defense techniques, such as reverse engineering, network hacking, smart car hacking, and attack defense strategies (*e.g.*, machine learning-based intrusion detection systems). I believe that is achieved through an in-depth understanding of traditional computer science and engineering concepts—including data structures, operating system concepts, system programming, data communications, and networking—so as to *really* understand security risks, threats, vulnerabilities, and proper countermeasures.

EDUCATION

Korea University, Seoul, Korea   Mar 2017–Feb 2023
Ph.D. in Information Security
- Dissertation: Network Intrusion Detection and Prevention System for Connected Vehicles
- Advisor: Prof. Huy Kang Kim
- Focus: Attack model study against IEEE 1722 AVB applications and Automotive Grade Linux, and then developing an intrusion detection and prevention system

Korea University, Seoul, Korea   Mar 2015–Feb 2017
M.S. in Information Security
- Thesis: A Longitudinal Analysis of .i2p Leakage in the Public DNS Infrastructure
- Advisor: Prof. Huy Kang Kim
- Focus: Measurement of DNS privacy leakage from Invisible Internet Project (I2P)

Chungbuk National University, Cheongju-si, Chungbuk, Korea   Mar 2011–Feb 2015
B.S. in Information and Communication Engineering
- Capstone Project: Design and Implementation of a Forensics tool designed for Windows 7 and Windows 8
- Advisor: Prof. Min Choi
- Focus: Recovering Deleted Files from Windows NT File System

EMPLOYMENT

BK21 FOUR R&E Center for Cybersecurity, Korea University   Mar 2024–Present
Job title: Postdoctoral Research Associate

Korea University   Mar 2024–Present
Job title: Lecturer

Institute of Cyber Security & Privacy, Korea University   Mar 2023–Feb 2024
Job title: Postdoctoral Research Associate

Korea University   Mar 2023–Aug 2023
Job title: Lecturer

Korea University   Mar 2022–Aug 2022
Job title: Lecturer

Institute of Cyber Security & Privacy, Korea University   Mar 2018–Feb 2022
Job title: Technical Research Personnel (전문연구요원)

PUBLICATIONS

The following list is also available at Google Scholar (#of citations ≥ 819 as of Apr. 2024) and ⓘ0000-0001-5638-2851.

JOURNAL (7)

[1] AERO: Automotive Ethernet Real-Time Observer for Anomaly Detection in In-Vehicle Networks
S Jeong, HK Kim, ML Han, BI Kwak
IEEE Transactions on Industrial Informatics (Mar 2024) (SCIE), doi: 10.1109/TII.2023.3324949
Remark: The first unsupervised network-IDS for heterogeneous automotive Ethernet communications, rating Q1—JCR top 2.3% journal in category COMPUTER SCIENCE, INTERDISCIPLINARY APPLICATIONS (3/110) in 2022

[2] X-CANIDS: Signal-Aware Explainable Intrusion Detection System for Controller Area Network-Based In-Vehicle Network
S Jeong, S Lee, H Lee, HK Kim
IEEE Transactions on Vehicular Technology (Mar 2024) (SCIE), doi: 10.1109/TVT.2023.3327275
Remark: The first unsupervised network-IDS for controller area network that identifies a specific target under attack, rating Q1—JCR top 14.0% journal

[3] Trading Behind-the-Scene: Analysis of Online Gold Farming Network in Auction House System
Y Noh, **S Jeong**, HK Kim
IEEE Transactions on Games (Jul 2021) (SCIE), doi: 10.1109/TG.2021.3094054
Remark: Industrial collaboration (Netmarble corp.), fraud detection on a server-side online game service

[4] Convolutional Neural Network-based Intrusion Detection System for AVTP Streams in Automotive Ethernet-based Networks
S Jeong, B Jeon, B Chung, HK Kim
Vehicular Communications (Jun 2021) (SCIE), doi: 10.1016/j.vehcom.2021.100338
Remark: the first network-IDS for automotive Ethernet, Q1 rating—JCR top 8.065% journal in category TELECOMMUNICATIONS (8/93) in 2021

[5] Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense
K Kim, JS Kim, **S Jeong**, JH Park, HK Kim
Computers & Security (Apr 2021) (SCIE), doi: 10.1016/j.cose.2020.102150
Remark: **#citations ≥ 250**

[6] Multimodal Game Bot Detection using User Behavioral Characteristics
AR Kang, **SH Jeong**, A Mohaisen, HK Kim
SpringerPlus (Apr 2016) (SCIE), doi: 10.1186/s40064-016-2122-8
Remark: **International & Industrial collaboration** (NCSOFT), **#citations ≥ 40**, data-driven system security

[7] Analysis of Game Bot's Behavioral Characteristics in Social Interaction Networks of MMORPG
SH Jeong, AR Kang, HK Kim
ACM SIGCOMM Computer Communication Review (Aug 2015) (SCIE)—doi: 10.1145/2829988.2790005,
ACM SIGCOMM (**SIGCOMM 2015**—a BK21-distinguished conference)
Remark: **One of Top Conferences**, Acceptance rate: **17%**, **Citation counts ≥ 28**, server-side data analysis

CONFERENCE/WORKSHOP (7)

[8] Infotainment System Matters: Understanding the Impact and Implications of In-Vehicle Infotainment System Hacking with Automotive Grade Linux
S Jeong, M Ryu, H Kang, HK Kim
ACM Conference on Data and Application Security and Privacy (**CODASPY 2023**), doi: 10.1145/3577923.3583650
Remark: **The Best Paper**, Acceptance rate ≈**30%**, Reported 3 vulnerabilities to the CVE database as well as 2 cases of vulnerability inheritances in a Linux OS

[9] MUVIDS: False MAVLink Injection Attack Detection in Communication for Unmanned Vehicles
S Jeong, E Park, KU Seo, JD Yoo, HK Kim
International Workshop on Automotive and Autonomous Vehicle Security (**AutoSec 2021 Workshop**), co-located with NDSS 2021, doi: 10.14722/autosec.2021.23036
Remark: Intrusion Detection System to secure **Unmanned Aerial System**

[10] Automated Reverse Engineering and Attack for CAN using OBD-II
TU Kang, HM Song, **S Jeong**, HK Kim
IEEE Vehicular Technology Conference (**VTC-Fall 2018**), doi: 10.1109/VTCFall.2018.8690781
Remark: **Unveiled a new kind of threats** leveraging the self-diagnostics system, **Citation counts ≥ 34**

[11] OTIDS: A Novel Intrusion Detection System for In-vehicle Network by using Remote Frame
H Lee, **SH Jeong**, HK Kim
Conference on Privacy, Security and Trust (**PST 2017**), doi: 10.1109/PST.2017.00017
Remark: **Citation counts ≥ 320**

[12] Transparency in the New gTLD Era: Evaluating the DNS Centralized Zone Data Service
AR Kang, **SH Jeong**, SY Ko, K Ren, A Mohaisen
IEEE Workshop on Hot Topics in Web Systems and Technologies (**HotWeb 2016 Workshop**), doi: 10.1109/HotWeb.2016.18
Remark: **International collaboration**

[13] A Longitudinal Analysis of. i2p Leakage in the Public DNS Infrastructure
SH Jeong, AR Kang, J Kim, HK Kim, A Mohaisen
ACM SIGCOMM (**SIGCOMM 2016**—a BK21-distinguished conference), doi: 10.1145/2934872.2960423, Poster
Remark: **One of Top Conferences**, **International collaboration**, Acceptance rate: **17%**, **Citation counts ≥ 10**, studies on 2 root DNS servers—A and J maintained by Version Inc.

DOMESTIC JOURNAL (2)

[14] The Big Data Analysis Framework of Information Security Policy based on Security Incidents
SH Jeong, HK Kim, J Woo
한국컴퓨터정보학회논문지 (Oct 2017), KCI, doi: 10.9708/jksci.2017.22.10.073

[15] A Survey of Fraud Detection Research based on Transaction Analysis and Data Mining Technique
SH Jeong, H Kim, S Shin, T Lee, HK Kim
정보보호학회논문지 (Dec 2015), KCI, doi: 10.13089/JKIISC.2015.25.6.1525

DOMESTIC CONFERENCE (1)

[16] Toward Understanding Network Intrusion on Vehicles: An eXplainable IDS Analyzing Signals and Time-series Periodicity
S Jeong
Conference on Information Security and Cryptography-Winter 2023 (CISC-W'23)
Remark: **Outstanding Paper Award** (정보보호학회장상-우수논문상)

PATENTS

Summary. 8 distinct patent items, 20 entries—namely 4 patent registrations in Korea, 4 PCTs, 8 international patents filed, and 4 domestic patents filed

Apparatus and Method for Detecting Vehicle Intrusion
- Korea, **Reg. No. 10-1853676**, Apr 2018

Device and Method for Analysing CAN Message Using OBD-II Query
- Korea, **Reg. No. 10-2028653**, Sep 2019

Device for Verifying Status and Detecting Anomaly of Vehicle and System Having the Same
- PCT/KR2018/009508, Aug 2018
- Korea, **Reg. No. 10-1995903**, Sep 2019

Method for SDN-based Intrusion Response or Prevention for In-vehicle Network and System using the same
- PCT/KR2020/010141, Jul 2020
- Korea, App. No. 10-2020-0095518, Jul 2020
- US, App. No. 17/631,8366, Jul 2020
- Germany, App. No. 112020003655.3T, Jul 2020
- China, App. No, 202080055869.XA, Jul 2020

Method for SDN-based Intrusion Response or Prevention for In-vehicle Network and System using the same
- PCT/KR2020/010142, Jul 2020
- Korea, App. No. 10-2020-0095519, Jul 2020
- US, App. No. 17/631,809, Jul 2020
- Germany, App. No. 112020003658.T5 , Jul 2020
- China, App. No. 202080055847.3A, Jul 2020

Anomaly Detection Model Using Message ID Sequence on Unmanned Moving Objects
- Korea, **Reg. No. 10-2476359**, Dec 2022
- US, App. 17/532,272, Nov 2021

Generative Adversarial Network Model and Training Method to Generate Message ID Sequence on Unmanned Moving Objects
- Korea, App. No. 10-2021-0009487, Jan 2021
- US App. 17/532,226, Nov 2021

Lightweight Real-Time Anomaly Detection Method Using CAN Message Analysis and Neural Network Model
- Korea, App. No. 10-2021-0174328, Dec 2021
- PCT/KR2022/017082, Nov 2022

AWARDS & SCHOLARSHIPS

Granite Tower Teaching Award—CYDF311 Class #37   Spring 2023
- Top 5% of student course evaluation in Korea Univ.
- The President of Korea University

Outstanding Paper Award   2023
- Korea Institute of Information Security & Cryptology (한국정보보호학회)

The Best Paper Award   2023
- Selected among 83 submitted papers
- ACM CODASPY 2023 Conference Organizing Committee

Excellent Teaching Award—AICS308 Reverse Engineering   Spring 2022
- Top 20% of student course evaluation in Korea Univ.
- The President of Korea University

BrainKorea21 Four Fellowship Program   2021
- Top 5% of Korea Univ. graduate students
- Outstanding international activities in ITU-T as a delegate of Republic of Korea

Teaching Assistant   2018S, 2018F
- Administration office of School of Cybersecurity, Korea University

Student Travel Grants   2016
- ACM SIGCOMM 2016 Conference Organizing Committee

TEACHING

Instructor

CYDF311: Class #37—*Attack & Defense: Theory and practice*   2024S, Present
- Dept. Cyber Defense, Korea University

CYDF311: Class #37—*Attack & Defense: Theory and practice*   2023S
- Dept. Cyber Defense, Korea University

AICS308: Reverse Engineering   2022S
- Dept. AI Cybersecurity, Sejong Campus of Korea University

Teaching Assistant

Lectured by Prof. Huy Kang Kim
- CYDF311: Class #37—*Attack & Defense: Theory and practice* 2021S
- IMS1004: Introduction Course for Information Security (Graduate School) 2021S

Lectured by Prof. Kyounggon Kim
- CYDF218: Class #66—*Cyber War* 2018F
- ISEC401: Advanced Hacking Practice 2018S
- ITCS302: Hacking and Security 2018S
- IMS756: Practical Cyber Security (Graduate school) 2018S
- CYDF218: Class #66—*Cyber War* 2017F
- ISEC302: Basic Hacking Practice 2017F
- ITCS302: Hacking and Security 2017S
- ISEC401: Advanced Hacking Practice 2017S

Lectured by Dr. Sanghyun Cho
- CYDF211: Class #18—*System Programming* 2018S

Special Lecture and Seminar

Hands-on-Practice: Penetration Test and Intrusion Detection System Development 2023
- Hosted by the University of Queensland in Australia (May 8–12, 2023)

Hands-on-Practice: Intrusion Detection System Development with Machine Learning 2022
- Hosted 20+ undergraduate students from the University of Western Australia

Smart Vehicle Security Training Course: Controller Area Network 2020
- Audiences included researchers from small/mid-size enterprises and cybersecurity research institutes
- hosted by the Korea Internet & Security Agency (KISA)

Data-Driven Security in Data Science Era 2018
- to graduate students of SungKyunKwan University
- hosted by SungKyunKwan University

KB-KAIST AI Intensive—A Practice on Detecting Fraudulent Credit Card Transactions 2018
- to data scientists in KB Kookmin Bank, Korea
- hosted by Korea Advanced Institute of Science and Technology (KAIST)

SERVICES

International Standard

Since Sep 2020, I have been attending ITU-T SG17 meetings as one of delegates who represent the Republic of Korea (MSIT). I am a main editor of ITU-T X.1377 in ITU-T SG17 (Security)/WP2/Q13 (Intelligent Transportation Systems).
- **ITU-T X.1377** (formerly X.ipscv): Guidelines for an intrusion prevention system for connected vehicles, **Approved** in Oct 2022, see ITU-T work programme

Program Committee
- **CSC 2021** Cyber Security Challenge 2021 "사이버 보안 챌린지 2021"
  –Host: Ministry of Science and ICT / Organizer: IITP / Committee: Korea Univ., Culture Makers, KISA
  – My role includes—Setting up an infotainment system testbed, Attack vector analysis, Penetration test, Vulnerability identification and disclosure, and the Development of a journal log collection framework for host-based IDSs.
  – I have evaluated the PoC exploit codes submitted by 102 researchers.
  – Live feed: The Final Round

External Reviewer
- Elsevier Computers & Security
- IEEE Transactions on Vehicular Technology
- SAE International Journal
- IEEE Networking Letters
- IEEE Transactions on Neural Networks and Learning Systems

Maintainer of the in-vehicle intrusion datasets
- **CAN Dataset for intrusion detection (OTIDS)** available at HCRLab
- **Automotive Ethernet Intrusion Dataset** available on IEEE DataPort (doi: 10.21227/1yr3-q009)
- **X-CANIDS Dataset (In-Vehicle Signal Dataset)** available on IEEE DataPort (doi: 10.21227/epsj-y384)

Vulnerability disclosure
- **CVE-2022-24595**
  Impact: Remote Code Execution, Information Disclosure, and Denial of Service
  `/usr/bin/afb-daemon` of Automotive Grade Linux 11.0.0–11.0.5 (Kooky Koi)
- **CVE-2022-24596**
  Impact: Denial of Service
  `/usr/bin/afb-daemon` of Automotive Grade Linux 11.0.0–11.0.5 (Kooky Koi)
- **CVE-2022-24597**
  Impact: Information Disclosure, Denial of Service
  `agl-service-weather` of Automotive Grade Linux 11.0.0–11.0.5 (Kooky Koi)

Technology transfer
- KU Research & Business Foundation → K-SIGN
  Patent No. 10-2021-0174328 Lightweight Real-Time Anomaly Detection Method Using CAN Message Analysis and Neural Network Model, 5,000,000 KRW

RESEARCH PROJECTS

Summary. As a research associate in the graduate school, I have participated 28 research projects funded by the Republic of Korea government as well as industries both internationally and at home.

Vehicle Cybersecurity

1. 자율주행차량의 차세대 내부 네트워크의 보안 및 초고속 무결성 부여 기술 개발, 정보통신기획평가원, Mar 2023–Feb 2024
2. 자동차 사이버보안 관리시스템 평가기술 및 보안위협 대응방안 기술 개발, 국토교통과학기술진흥원, Mar 2023–Feb 2024
3. 차세대보안 분야 챌린지 R&D 총괄 과제, 정보통신기획평가원, Apr 2020–Dec 2021, Apr 2023–Dec 2023
4. 가상화 기반 자율주행차 사이버훈련 환경 구축 및 콘텐츠 연구, 국가보안기술연구소, Apr 2023–Oct 2023
5. 무인이동체 공통핵심 보안기술 개발 연구, 정보통신기획평가원, Apr 2020–Sep 2022
6. Advanced Contextually-Aware On-board Monitoring for Self-Driving Cars, HUAWEI Singapore, Jul 2021–Apr 2022 (**International collaboration**)
7. Intrusion Resilient Sensor Perception for Autonomous Driving, HUAWEI Singapore, Aug 2020–Aug 2021 (**International collaboration**)
8. OTAC 인증 review task, 센스톤 주식회사, Aug 2021
9. IoT 관점에서의 차량 보안, 삼성전자주식회사, Nov 2015–Nov 2020 (**Long-term commitment**)
10. 차량 내부 네트워크 용 IDS(Intrusion detection System) 및 IRS(Intrusion Response System) 관련 국제 표준 개발, 현대NGV, Aug 2019–Feb 2020
11. 이더넷기반 차량 환경 공격발생시 자동 대응 방안 연구, 한국전자통신연구원, Jun 2019–Oct 2019
12. 자율주행 스마트자동차용 이상징후 탐지 핵심기술개발, 정보통신기술진흥센터, Jan 2017–Dec 2018
13. 다중 도메인 차량 이상징후 탐지 알고리즘 연구, 한국전자통신연구원, Aug 2018–Nov 2018
14. 차량 침입 탐지 기술, 삼성전자주식회사, May 2016–Dec 2016

System and Network Cybersecurity

1. 4단계 BK21 정보보호학교육연구단 국고 지원금, 교육부, Mar 2024–Present
2. System call 데이터의 filtering과 feature engineering을 통한 이상징후 탐지 패턴 생성, 주식회사 소테리아, Feb 2020–Jun 2020
3. AI기반 악성파일 탐지 모델 개발, 삼성전자주식회사, Apr 2019–Nov 2019
4. 사이버 공격 예측 및 자산 위험도 정량적 평가 기법 연구, 국방과학연구소, Mar 2018–Dec 2018
5. 스크립트 기반 사이버 공격 사전 예방 및 대응 기술 개발, 한국인터넷진흥원, Feb 2016–Feb 2017
6. 침입 탐지 방지 솔루션 연구, 삼성전자 주식회사, Jun 2015–Nov 2015

Data-driven Cybersecurity and Fraud Detection on Online Game Service

1. 광고사기탐지 프로젝트, AISpera, Feb 2021–Feb 2022
2. A3 시계열 이상 탐지 고도화 프로젝트, 넷마블주식회사, Aug 2020–Nov 2020
3. 게임 내 소셜 네트워크 분석을 통한 게이머간 상호 작용 분석 한국전자통신연구원, Apr 2018–Nov 2018
4. 온라인게임 내 작업장 알고리즘 개발연구, 넷마블주식회사, Jan 2018–May 2018
5. 인게임 환경 요소 변화와 게이머 행동 변화간 상관관계 연구, 한국전자통신연구원, May 2017–Nov 2017
6. 모바일 온라인 RPG 게임 플레이 활성화 요소 연구, 한국전자통신연구원, Jun 2016–Nov 2016
7. 데이터마이닝 기법을 통한 게임 봇 탐지 및 악성유저 행위 분석: 지하경제 분석을 중심으로, 한국연구재단, Sep 2015–Apr 2017
8. 텍스트 마이닝 및 빅데이타 감성분석 기반 기업이미지 관리 시스템 구축, 한국연구재단, Sep 2015–May 2016
9. 모바일 결제 정보에 대한 익명화 및 이상거래 탐지 기술 연구, 한국인터넷진흥원, Jul 2015–Jan 2016

Last update on Apr. 16, 2024