Dongkwan Kim

Postdoctoral Fellow, SSLab
School of Cybersecurity and Privacy
Georgia Institute of Technology

0xdkay@gmail.com
https://0xdkay.me

Highlights

Cybersecurity researcher and engineer with 10+ years of experience in vulnerability discovery and large-scale system analysis across IoT/embedded devices, cellular networks, and cyber-physical systems. Currently focusing on AI-powered cybersecurity automation.

- **DARPA AIxCC 1st Place Winner ($4M):** Built fully autonomous AI agents for vulnerability discovery and exploit generation using LLMs.
- **Samsung Security Center:** Successfully secured 30+ products and services (protecting 1B+ users) across diverse domains, and contributed to executive-level reports and organization-wide presentations (500+ people).
- **Research & IP:** Published 27 papers (9 top-tier & 1,100+ citations), filed 7 patents, and completed 17 funding projects, while leading a subgroup, *software analysis team*, (∼8 people) in the SysSec lab.
- **Community Contribution:** Delivered 21 invited talks to diverse academic and industry audiences.
- **CTF Leadership:** Reached DEF CON CTF finals 5 times and won multiple CTFs (∼$115K). Organized Samsung CTF, while leading the KAIST graduate hacking team, *KaisHack*, (∼20 people).

Work Experience

Georgia Tech, Postdoctoral Fellow, Atlanta, GA — Feb 2025 – Present

DARPA AIxCC 1st Place Winner: Designed and implemented fully autonomous LLM-based agents for vulnerability discovery and exploit generation.

· Leveraging LangGraph, LangChain, LiteLLM, and Phoenix for multi-agent orchestration.

Currently leading the evaluation of AI's offensive potential in real-world cybersecurity scenarios.

Manager: Prof. Taesoo Kim

Samsung Security Center, Samsung SDS, Senior Engineer, South Korea — Aug 2022 – Dec 2024

Drove Red Team operations across AI systems, IoT devices, Android apps, and kernel-level mitigations.

· Secured 30+ consumer and enterprise products, protecting 1B+ users.

· Delivered executive-level reports and gave organization-wide presentations to 500+ security engineers.

Shared insights on AI system security at 6 industry and academic venues.

· Securing prompt injection chains against remote code execution, impersonation, and sensitive data leak.

KAIST, Postdoctoral Researcher, South Korea — Mar 2022 – Jul 2022

Conducted advanced research on:

· Smartphone baseband authentication bypass (USENIX Security '23)

· Acoustic signal injection attacks against drone sensors and recovery techniques (NDSS'23)

· EMI signal injection on drone sensory communication channels (NDSS'23)

Manager: Prof. Yongdae Kim

Pinion Industries, Research Intern, South Korea — Dec 2013 – Feb 2014

Analyzed automotive CAN messages and exploited in-vehicle components, achieving RCE and wiretapping.

KAIST CERT, Student Senior, South Korea — Sep 2010 – Aug 2012

Led the student team (Sep 2011 – Aug 2012) in campus-wide security assessment under the KAIST domain. Investigated security incidents, including probing a serious life-threatening email attack leading to arrest.

Education

Korea Advanced Institute of Science and Technology (KAIST), South Korea

Ph.D. in School of Electrical Engineering — Mar 2016 – Feb 2022

- Thesis Title: Improving Large-Scale Vulnerability Analysis of IoT Devices with Heuristics and Binary Code Similarity
- Advisor: Prof. Yongdae Kim

M.S. in School of Electrical Engineering — Mar 2014 – Feb 2016

- Thesis Title: Dissecting VoLTE: Exploiting Free Data Channels and Security Problems
- Advisor: Prof. Yongdae Kim

B.S. in School of Computing — Feb 2010 – Feb 2014

EURECOM, France

Visiting Scholar in Software and System Security — Jun 2014 – Jul 2014

- Learned embedded device analysis techniques, particularly for debugging interfaces
- Advisor: Prof. Aurélien Francillon

Honors & Awards

AI-Powered Security Competitions

1st place ($4,000,000), DARPA AIxCC — (Team Atlanta) Aug 2025

Hacking Contests (*i.e.*, Capture-the-flag, CTF)

Finalist, DEFCON 27 CTF — (Team KaisHack GoN) Aug 2019
Finalist, DEFCON 26 CTF — (Team KaisHack+PLUS+GoN) Aug 2018
1st place ($20,000), HDCON CTF — (Team maxlen) Nov 2017
1st place ($30,000), Whitehat Contest — (Team Old GoatskiN) Nov 2017
3rd place ($5,000), Codegate CTF — (Team Old GoatskiN) Apr 2017
Finalist, DEFCON 24 CTF — (Team KaisHack GoN) Aug 2016
1st place ($20,000), Whitehat Contest — (Team SysSec) Nov 2014
Finalist, DEFCON 22 CTF — (Team KAIST GoN) Aug 2014
Silver prize ($2,000), HDCON CTF — (Team GoN) Dec 2013
1st place ($20,000), Whitehat Contest — (Team KAIST GoN) Oct 2013
Finalist, DEFCON 20 CTF — (Team KAIST GoN) Jul 2012
Silver prize ($2,000), HDCON CTF — (Team KAIST GoN) Jul 2012
3rd place ($5,000), Codegate CTF 2012 — (Team KAIST GoN) Apr 2012
1st place ($10,000), ISEC CTF — (Team GoN) Sep 2011
1st place ($1,000), PADOCON CTF — (Team GoN) Jan 2011

Academic Awards

Best Paper Award, CISC-W — Nov 2020

- Title: Standard-based User Identifier Mapping Attack Prevention Method for LTE Network

Best Presentation Award, A3 Security Workshop — Feb 2016

- Title: Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations

Best Paper Award, WISA — Aug 2015

- Title: BurnFit: Analyzing and Exploiting Wearable Devices

Reported Security Vulnerabilities

CVE-2015-6614, Android telephony privilege escalation, Google — Oct 2015

Government-Issued Certificates

Engineer Information Security, South Korea — Jun 2016
Engineer Information Processing, South Korea — May 2013

Scholarships

National Scholarship (Science and Engineering), Korea Student Aid Foundation Feb 2010 – Feb 2020

Patents

International Registrations

[1] **US 10111120** Oct 2018
Method and Apparatus for Checking Problem in Mobile Communication Network

Domestic Registrations, South Korea

[1] **KR 10-2514809** Mar 2023
VIDEO IDENTIFICATION METHOD IN LTE NETWORKS AND THE SYSTEM THEREOF

[2] **KR 10-2418212** Jul 2022
ARCHITECTURE-INDEPENDENT SIMILARITY MEASURING METHOD FOR PROGRAM FUNCTION

[3] **KR 10-2415494** Jun 2022
Emulation based security analysis method for embedded devices

[4] **KR 10-2333866** Nov 2021
Method and Apparatus for Checking Problem in Mobile Communication Network

[5] **KR 10-1972825** Apr 2019
Method and apparatus for automatically analyzing vulnerable point of embedded appliance by using hybrid analysis technology, and computer program for executing the method

[6] **KR 10-1868836** Jun 2018
A method to attack commercial drones using the resonance effect of gyroscopes by sound waves

Applications

[1] **KR 10-2022-0132964** Oct 2022
ANTI-DRONE SYSTEM THROUGH COMMUNICATION DISTORTION BETWEEN SENSOR AND CONTROL UNIT AND ITS OPERATION METHOD

[2] **KR 10-2021-0168382** Nov 2021
Method and System for Automatically Analyzing Bugs in Cellular Baseband Software using Comparative Analysis based on Cellular Specifications

[3] **KR 10-2021-0136352** Oct 2021
METHOD FOR PREVENTING MAPPING OF USER IDENTIFIERS IN MOBILE COMMUNICATION SYSTEM AND THE SYSTEM THEREOF

[4] **KR 10-2021-0040795** Mar 2021
ANALYSIS SYSTEM FOR DETECTION OF SIP IN VoLTE AND THE METHOD THEREOF

[5] **KR 10-2020-0177062** Dec 2020
Analysis method for detection of SIP implementation vulnerability in VoLTE

[6] **KR 10-2020-0133926** Oct 2020
Method to prevent mapping of user identifiers in mobile communication system

[7] **KR 10-2020-0133925** Oct 2020
APPARATUS AND METHOD FOR VIDEO TITLE IDENTIFICATION OF MOBILE COMMUNICATION NETWORK USING ENCRYPTED TRAFFIC MONITORING

[8] **KR 10-2019-0005131** Jan 2019
Large-scale honeypot system IoT botnet analysis

[9] **KR 10-2018-0036403** Mar 2018
Dynamic analysis method for malicious embedded firmware detection

[10] **KR 10-2018-0036055** Mar 2018
Emulation based security analysis method for embedded devices

[11] **KR 10-2018-0037291** Mar 2018
Binary-Level Virtual Function Call Protection Method by Saving Type Information

[12] **KR 10-2018-0034616** Mar 2018
ARCHITECTURE-INDEPENDENT SIMILARITY MEASURING METHOD FOR PROGRAM FUNCTION

Publications (International)

(∗: co-first authors)

[1] **BaseComp: A Comparative Analysis for Integrity Protection in Cellular Baseband Software**
Eunsoo Kim*, Min Woo Baek*, CheolJun Park, **Dongkwan Kim**, Yongdae Kim, and Insu Yun
Proceedings of the 32nd USENIX Security Symposium (Security'23)
Acceptance rate: 29.22% (422 of 1,444) Aug 2023

[2] **Un-Rocking Drones: Foundations of Acoustic Injection Attacks and Recovery Thereof**
Jinseob Jung, **Dongkwan Kim**, Joonha Jang, Juhwan Noh, Changhun Song, and Yongdae Kim
Proceedings of the 2023 Annual Network and Distributed System Security Symposium (NDSS'23)
Acceptance rate: 16.18% (94 of 581) Mar 2023

[3] **Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels**
Junha Jang, ManGi Cho, Jaehoon Kim, **Dongkwan Kim**, and Yongdae Kim
Proceedings of the 2023 Annual Network and Distributed System Security Symposium (NDSS'23)
Acceptance rate: 16.18% (94 of 581) Mar 2023

[4] **Watching the Watchers: Practical Video Identification Attack in LTE Networks**
Sangwook Bae, Mincheol Son, **Dongkwan Kim**, CheolJun Park, Jiho Lee, Sooel Son, and Yongdae Kim
Proceedings of the 31st USENIX Security Symposium (Security'22)
Acceptance rate: 18.10% (256 of 1,414) Aug 2022

[5] **Revisiting Binary Code Similarity Analysis using Interpretable Feature Engineering and Lessons Learned**
Dongkwan Kim, Eunsoo Kim, Sang Kil Cha, Sooel Son, and Yongdae Kim
IEEE Transactions on Software Engineering (TSE'22) Jul 2022

[6] **Improving Large-Scale Vulnerability Analysis of IoT Devices with Heuristics and Binary Code Similarity**
Dongkwan Kim
Ph.D. Thesis, KAIST Daejeon, South Korea, Feb 2022

[7] **Enabling the Large-Scale Emulation of Internet of Things Firmware With Heuristic Workarounds**
Dongkwan Kim, Eunsoo Kim, Mingeun Kim, Yeongjin Jang, and Yongdae Kim
IEEE Security & Privacy May 2021

[8] **BaseSpec: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols**
Dongkwan Kim*, Eunsoo Kim*, CheolJun Park, Insu Yun, and Yongdae Kim
Proceedings of the 2021 Annual Network and Distributed System Security Symposium (NDSS'21)
Acceptance rate: 15.18% (87 of 573) Virtual, Feb 2021

[9] **FirmAE: Towards Large-Scale Emulation of IoT Firmware for Dynamic Analysis**
Mingeun Kim, **Dongkwan Kim**, Eunsoo Kim, Suryeon Kim, Yeongjin Jang, and Yongdae Kim

Proceedings of the 2020 Annual Computer Security Applications Conference (ACSAC'20)
Acceptance rate: 23.18% (70 of 302) Virtual, Dec 2020

[10] **Who Spent My EOS? On the (In)Security of Resource Management of EOS.IO**
Sangsup Lee, Daejun Kim, **Dongkwan Kim**, Sooel Son, and Yongdae Kim
Proceedings of the 13th USENIX Workshop on Offensive Technologies
(WOOT'19) Santa Clara, CA, Aug 2019

[11] **Peeking over the Cellular Walled Gardens - A Method for Closed Network Diagnosis**
Byeongdo Hong, Shinjo Park, Hongil Kim, **Dongkwan Kim**, Hyunwook Hong, Hyunwoo Choi, Jean-Pierre Seifert, Sung-Ju Lee, and Yongdae Kim
IEEE Transactions on Mobile Computing (TMC'18) Feb 2018

[12] **When Cellular Networks Met IPv6: Security Problems of Middleboxes in IPv6 Cellular Networks**
Hyunwook Hong, Hyunwoo Choi, **Dongkwan Kim**, Hongil Kim, Byeongdo Hong, Jiseong Noh, and Yongdae Kim
Proceedings of the 2nd IEEE European Symposium on Security and Privacy (EuroS&P'17)
Acceptance rate: 19.58% (38 of 194) Paris, France, Apr 2017

[13] **Pay As You Want: Bypassing Charging System in Operational Cellular Networks**
Hyunwook Hong, Hongil Kim, Byeongdo Hong, **Dongkwan Kim**, Hyunwoo Choi, Eunkyu Lee, and Yongdae Kim
Proceedings of the 17th International Workshop on Information Security Applications
(WISA'16) Jeju, South Korea, Aug 2016

[14] **Dissecting VoLTE: Exploiting Free Data Channels and Security Problems**
Dongkwan Kim
M.S. Thesis, KAIST Daejeon, South Korea, Feb 2016

[15] **Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations**
Dongkwan Kim*, Hongil Kim*, Minhee Kwon, Hyungseok Han, Yeongjin Jang, Dongsu Han, Taesoo Kim, and Yongdae Kim
Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS'15)
Acceptance rate: 19.81% (128 of 646) Denver, CO, Oct 2015

[16] **BurnFit: Analyzing and Exploiting Wearable Devices**
Dongkwan Kim, Suwan Park, Kibum Choi, and Yongdae Kim
Proceedings of the 16th International Workshop on Information Security Applications (WISA'15)
Best Paper Award Jeju, South Korea, Aug 2015

[17] **Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors**
Yunmok Son, Hocheol Shin, **Dongkwan Kim**, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim
Proceedings of the 24th USENIX Security Symposium (Security'15)
Acceptance rate: 15.73% (67 of 426) Austin, TX, Aug 2015

[18] **Analyzing Security of Korean USIM-based PKI Certificate Service**
Shinjo Park, Suwan Park, Insu Yun, **Dongkwan Kim**, and Yongdae Kim
Proceedings of the 15th International Workshop on Information Security Applications
(WISA'14) Jeju, South Korea, Aug 2014

[19] **High-speed Automatic Segmentation of Intravascular Stent Struts in Optical Coherence Tomography Images**
Myounghee Han, **Dongkwan Kim**, Wang-Yuhl Oh, and Sukyoung Ryu
Proceedings of SPIE Biomedical Optics, Photonics West 2013 (BiOS'13) San Francisco, CA, Feb 2013

Publications (Domestic, South Korea)

[20] **Video Service Identification Attack in LTE by Monitoring Encrypted Traffic**
Mincheol Son, Sangwook Bae, **Dongkwan Kim**, Jiho Lee, CheolJun Park, BeomSeok Oh, Sooel Son, and Yongdae Kim
Proceedings of Symposium of the Korean Institute of Communications and Information Sciences (KCIS'21) Virtual, Jun 2021

[21] **Standard-based User Identifier Mapping Attack Prevention Method for LTE Network**
CheolJun Park, Sangwook Bae, Jiho Lee, Mincheol Son, **Dongkwan Kim**, Sooel Son, and Yongdae Kim
Conference on Information Security and Cryptography Winter (CISC-W'20)
Best Paper Award South Korea, Nov 2020

[22] **VoLTEFuzz: Framework for Comprehensive Analysis of SIP in VoLTE**
Seokbin Yun, Sangwook Bae, Mincheol Son, **Dongkwan Kim**, Jiho Lee, CheolJun Park, Yeongbin Hwang, and Yongdae Kim
Conference on Information Security and Cryptography Winter (CISC-W'20) South Korea, Nov 2020

[23] **Firm-Pot: Large-scale Firmware Honey-Pot for Malware Analysis**
Minguen Kim, Eunsoo Kim, **Dongkwan Kim**, and Yongdae Kim
Conference on Information Security and Cryptography Winter (CISC-W'18) South Korea, Dec 2018

[24] **TVT: Typed Virtual Table for Mitigating VTable Hijacking**
Jeongoh Kyea, Eunsoo Kim, **Dongkwan Kim**, and Yongdae Kim
Conference on Information Security and Cryptography Winter (CISC-W'17) South Korea, Dec 2017

[25] **Design and Implementation of GPS Spoofer Software**
Juhwan Noh, **Dongkwan Kim**, and Yongdae Kim
Conference on Information Security and Cryptography Summer (CISC-S'15) South Korea, Jun 2015

[26] **Security Analysis of USIM-based certificate service in Korea**
Shinjo Park, Suwan Park, Insu Yun, **Dongkwan Kim**, and Yongdae Kim
Conference on Information Security and Cryptography Summer (CISC-S'14) South Korea, Jun 2014

[27] **Security Analysis of Femtocells in Korea**
Eunsoo Kim, **Dongkwan Kim**, Youjin Lee, Shinjo Park, and Yongdae Kim
Conference on Information Security and Cryptography Summer (CISC-S'14) South Korea, Jun 2014

Invited Talks

AI Security Primer: Red Team Perspectives on Navigating New Threats and Safeguarding AI Frontier
Special Lecture for Hyundai Motors Group Security Center Seoul, South Korea, Jan 2025
3rd Workshop of IT Platform Security Research Group by Korea Institute of Information Security & Cryptology (KIISC) Seoul, South Korea, Nov 2024

Special Lecture for SungSungshin Women's University — Seoul, South Korea, Oct 2024
Special Lecture for SK Telecom Security Team — Seoul, South Korea, Jul 2024
SIS 2024: MERGE conference by S2W — Seoul, South Korea, Jul 2024
.HACK Conference by Theori — Seoul, South Korea, May 2024

Scaling up Vulnerability Analysis of IoT Devices with Heuristics and Binary Code Similarity

Technology Exchange Meeting between Samsung Mobile Security Team and Hyundai Motor Company Vehicle Cyber Security Team — Seoul, South Korea, Jul 2024
Special Lecture for Kyung Hee University — Yongin, South Korea, Aug 2024
Colloquium at School of Cybersecurity, Korea University — Seoul, South Korea, Oct 2023

Peeking over Industry's Patch Gap: Case Study of Samsung SmartTV's Web Browser

KAIST-Samsung SDS Tech Seminar — Daejeon, South Korea, Mar 2023

BaseSpec: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols

Annual Network and Distributed System Security Symposium — Virtual, Feb 2021
KAIST-CISPA Workshop — Seoul, South Korea, Aug 2019

Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations A.k.a. Dissecting VoLTE: Exploiting Free Data Channels and Security Problems

GSMA RCS/VoLTE Security Regulatory workshop — Toronto, Canada, Sep 2016
A3 Foresight Program Annual Workshop — Okinawa, Japan, Feb 2016
Chaos Communication Congress (CCC) Conference (32C3) — Hamburg, Germany, Dec 2015
National Security Research Institute — Daejeon, South Korea, Nov 2015
Power of Community (PoC) Conference — Seoul, South Korea, Nov 2015
ACM Conference on Computer and Communications Security (CCS) — Denver, CO, Oct 2015
Seminar at the Georgia Institute of Technology — Atlanta, GA, Oct 2015

BurnFit: Analyzing and Exploiting Wearable Devices

16th WISA — Jeju, South Korea, Aug 2015

International CTF Challenge Solving

NetSec-KR — Seoul, South Korea, Apr 2013

Professional Activities

Secondary Reviewer (Security)

IEEE Symposium on Security and Privacy (Oakland)	2021
USENIX Security Symposium (Security)	2019–2021
Network and Distributed System Security Symposium (NDSS)	2017–2018, 2020–2021
ACM Conference on Computer and Communications Security (CCS)	2017, 2019–2021
IEEE European Symposium on Security and Privacy (EuroS&P)	2016, 2018, 2020
ACM ASIA Conference on Computer and Communications Security (ASIACCS)	2016–2017, 2019–2020
The WEB Conference (WWW)	2018, 2020
International Symposium on Research in Attacks, Intrusions and Defenses (RAID)	2017
IEEE Symposium on Privacy-Aware Computing (PAC)	2017

Secondary Reviewer (System)

ACM Symposium on Operating Systems Principles (SOSP)	2019
Symposium on Operating Systems Design and Implementation (OSDI)	2016

External Security Consultant

KAIST Computer Emergency Response Team Sep 2010 – Feb 2022

Participated Projects

(∗: participated as a project leader)

Industrial Projects

[1] **An Industry-academia Task with Samsung Electronics Device Solutions Business** Jun 2020 – Aug 2020
· Samsung Electronics

[2] ∗**Organizing 2018 Samsung Capture-the-flag (SCTF)** Apr 2018 – Oct 2018
· Samsung Electronics

[3] ∗**Organizing 2017 Samsung Capture-the-flag (SCTF)** Dec 2016 – Dec 2017
· Samsung Electronics

[4] **A Study on the Security Vulnerability Analysis and Response Method of LTE Networks** Aug 2016 – Jul 2017
· SK Telecom

[5] **A Security Vulnerability Analysis of Smartcar Core Modules** Jul 2016 – Jun 2017
· Hyundai NGV

[6] **A Study on the Security Analysis and Response Method of LTE Networks** Aug 2015 – Apr 2016
· SK Telecom

[7] **A Security Analysis of Samsung SmartTV 2014** Feb 2014 – Dec 2015
· Samsung Electronics

International Projects

[1] ∗**Cyber Physical Analysis of System Software Survivability by Stimulating Sensors on Drones** Jun 2020 – Feb 2022
· Air Force Office of Scientific Research (AFOSR), Air Force Research Laboratory (AFRL)

Governmental Projects

[1] ∗**A Study on the Android-based Security Analysis Technology** May 2020 – Dec 2020
· National Security Research (NSR)

[2] **A Study on the Security of Random Number Generator and Embedded Devices** Jul 2017 – Jun 2019
· Institute for Information & Communications Technology Planning & Evaluation (IITP)

[3] ∗**A Study on the Firmware Emulation Technology for Linux-based Routers** May 2017 – Oct 2017
· NSR

[4] **A Development of Automated Reverse Engineering and Vulnerability Detection Base Technology through Binary Code Analysis** Apr 2016 – Dec 2018
· IITP

[5] ∗**A CAPTCHA Design based on Human Perception Characteristics** Apr 2016 – Dec 2016
· KAIST

[6] ∗**A Study on the Vulnerability Analysis Method of Domestic/International Smartcars** Apr 2015 – Nov 2015
· NSR

[7] **A Study on the Analysis of Technology and Security Threats in LTE Femtocell** Sep 2013 – Jan 2014
· Korea Internet & Security Agency (KISA)

[8] **A Study on the Analysis and Response Method of Vulnerabilities in Network Devices** Mar 2013 – Dec 2013
· NSR

[9] **A Study on the Vulnerability Analysis of Network Devices** Apr 2011 – Oct 2011
· NSR

Other Activities

[1] **Teaching Assistant, Introduction to Electronics Design Lab. (EE305), KAIST** Fall 2019
[2] **Teaching Assistant, Discrete Methods for Electrical Engineering (EE213), KAIST** Spring 2017
[3] **Teaching Assistant, Network Programming (EE324), KAIST** Fall 2016
[4] **Teaching Assistant, Cryptography Engineering (EE817/IS893), KAIST** Spring 2016
[5] **Teaching Assistant, Security 101: Think Like an Adversary (EE515/IS523), KAIST** Fall 2015
[6] **Student Representative of School of Computing, KAIST** Feb 2011 – Dec 2013
[7] **Head Instructor, Information Security 101 for Freshmen (HSS062), KAIST** Sep 2011 – Feb 2013
[8] **Teaching Assistant, Information Security 101 for Freshmen (HSS062), KAIST** Sep 2010 – Aug 2011

List of References

[1] **Dr. Yongdae Kim**
Director, Cyber Security Research Center (CSRC), KAIST
Professor, School of Electrical Engineering and Graduate School of Information Security, KAIST
Email: yongdaek@kaist.ac.kr
Homepage: https://syssec.kaist.ac.kr/~yongdaek/

[2] **Dr. Taesoo Kim**
Professor, School of Cybersecurity and Privacy (SCP) and Computer Science (SCS), Georgia Tech
Email: taesoo@gatech.edu
Homepage: https://taesoo.kim/

[3] **Dr. Sang Kil Cha**
Director, Cyber Security Research Center (CSRC), KAIST
Associate Professor, School of Computing and Graduate School of Information Security, KAIST
Email: sangkilc@kaist.ac.kr
Homepage: https://softsec.kaist.ac.kr/~sangkilc/

[4] **Dr. Sooel Son**
Associate Professor, School of Computing and Graduate School of Information Security, KAIST
Email: sl.son@kaist.ac.kr
Homepage: https://sites.google.com/site/ssonkaist/

[5] **Dr. Yeongjin Jang**
Principal Software Engineer, Samsung Research America
Email: y.jang1@samsung.com
Homepage: https://www.unexploitable.systems/

[6] **Dr. Insu Yun**
Associate Professor, School of Electrical Engineering, KAIST
Email: insuyun@kaist.ac.kr
Homepage: https://insuyun.github.io/