Dongkwan Kim

Ph.D Candidate
School of Electrical Engineering
Korea Advanced Institute of Science and Technology (KAIST)
Email: 0xdkay@gmail.com
Homepage: https://0xdkay.me

Summary

I am a Ph.D candidate at the School of Electrical Engineering, KAIST. My research goal is to secure the IoT ecosystem. To achieve this, I have been studying on systematizing vulnerability analysis of IoT devices. As a case study, I have analyzed (1) smart home systems (*e.g.*, wired/wireless routers, IP cameras, smart TVs), (2) mobile systems (*e.g.*, Android applications, baseband software, wearable devices), (3) cellular infrastructures (*e.g.*, specifications, charging policy, VoLTE, femtocells), (4) smart infrastructure (*e.g.*, automobiles, commercial drones), and (5) blockchain systems (*e.g.*, Bitcoin, Ethereum, EOS). To expand my knowledge base, I have participated in several hacking contests worldwide: (1) U.S. (*e.g.*, DEFCON, Plaid CTF), (2) South Korea (*e.g.*, Codegate, Whitehat Contest, and HDCON), and (3) China (*e.g.*, 0CTF). Besides, I have been helping KAIST Computer Emergency Response Team (CERT) in analyzing real-time/postmortem intrusion cases from 2010.

Research Interest

Fundamental binary analysis

- Systematizing bug discovery with binary code similarity analysis
- Applying natural language processing to assembly languages

Cellular network as a target

- Analyzing security violations in specifications and actual implementations
- Discovering inconsistencies between specifications and actual implementations
- Investigating privacy-leaking side channels

Cyber-physical system as a target

- Discovering security (or safety) violations under adversarial environments
- Building an end-to-end fuzzer for sensing and actuation logic

Education

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

Ph.D. in School of Electrical Engineering — (expected) 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

Work Experience

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

Analyzed CAN, infotainment systems, telematics, smartkey, and ECUs of automobiles

CEO: Woongjun Jang (VP at Hyundai Motor Company as of Jan. 2021)

KAIST Computer Emergency Response Team, Consultant, South Korea — Sep. 2010 – Aug. 2012

Conducted periodic penetration testing on servers under the KAIST domain (∗.kaist.ac.kr)

Performed real-time/postmortem analysis of intrusion cases on the servers

Honors & Awards

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

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 Presentation Award, A3 Security Workshop — Aug. 2015

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 Vulnerabilties

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

Certificates

Engineer Information Security (*i.e.*, 정보보안기사), South Korea — Jun. 2016

Engineer Information Processing (*i.e.*, 정보처리기사), South Korea — May 2013

Scholarships

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

Patents

International Registrations

US 10111120 Oct. 2018

Method and Apparatus for Checking Problem in Mobile Communication Network

Domestic Registrations, South Korea

KR 10-1972825-0000 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

KR 10-1868836-0000 Jun. 2018

A method to attack commercial drones using the resonance effect of gyroscopes by sound waves

Applications

KR 10-2021-0136352 Oct. 2021

METHOD FOR PREVENTING MAPPING OF USER IDENTIFIERS IN MOBILE COMMUNICATION SYSTEM AND THE SYSTEM THEREOF

KR 10-2021-0088806 Jul. 2021

VIDEO IDENTIFICATION METHOD IN LTE NETWORKS AND THE SYSTEM THEREOF

KR 10-2021-0040795 Mar. 2021

ANALYSIS SYSTEM FOR DETECTION OF SIP IN VoLTE AND THE METHOD THEREOF

KR 10-2020-0177062 Dec. 2020

Analysis method for detection of SIP implementation vulnerability in VoLTE

KR 10-2020-0133926 Oct. 2020

Method to prevent mapping of user identifiers in mobile communication system

KR 10-2020-0133925 Oct. 2020

APPARATUS AND METHOD FOR VIDEO TITLE IDENTIFICATION OF MOBILE COMMUNICATION NETWORK USING ENCRYPTED TRAFFIC MONITORING

KR 10-2019-0005131 Jan. 2019

Large-scale honeypot system IoT botnet analysis

KR 10-2018-0036403 Mar. 2018

Dynamic analysis method for malicious embedded firmware detection

KR 10-2018-0036055 Mar. 2018

Emulation based security analysis method for embedded devices

KR 10-2018-0037291 Mar. 2018

Binary-Level Virtual Function Call Protection Method by Saving Type Information

KR 10-2018-0034616 Mar. 2018

ARCHITECTURE-INDEPENDENT SIMILARITY MEASURING METHOD FOR PROGRAM FUNCTION

KR 10-2017-0002925 Jan. 2017

Method and Apparatus for Checking Problem in Mobile Communication Network

Publications

(∗: co-first authors)

1. **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)
   Aug. 2022

2. **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

3. **Revisiting Binary Code Similarity Analysis using Interpretable Feature Engineering and Lessons Learned**
   Dongkwan Kim, Eunsoo Kim, Sang Kil Cha, Sooel Son, and Yongdae Kim
   Under Major Revision to IEEE Transactions on Software Engineering (TSE'21)
   Apr. 2021

4. **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)
   Virtual, Feb. 2021
   Acceptance rate: 15.18% (87 of 573)

5. **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)
   Virtual, Dec. 2020
   Acceptance rate: 23.18% (70 of 302)

6. **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

7. **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

8. **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)

Paris, France, Apr. 2017
Acceptance rate: 19.58% (38 of 194)

9. **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

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

11. **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)
Denver, CO, Oct. 2015
Acceptance rate: 19.81% (128 of 646)

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

13. **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)
Austin, TX, Aug. 2015
Acceptance rate: 15.73% (67 of 426)

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

15. **High-speed automatic segmentation of intravascular stent struts in optical coherence tomography images**
Proceedings of SPIE Biomedical Optics, Photonics West 2013 (BiOS'13)
Myounghee Han, **Dongkwan Kim**, Wang-Yuhl Oh, and Sukyoung Ryu
San Francisco, CA, Feb. 2013

Invited Presentations

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	Virtual, Feb. 2021

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	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. 2012 – Feb. 2022

Participated Projects

(∗: participated as a project leader)

Industrial Projects

An Industry-academia Task with Samsung Electronics Device Solutions Business — Jun. 2020 – Aug. 2020
Samsung Electronics

*Organizing 2018 Samsung Capture-the-flag (SCTF) — Apr. 2018 – Oct. 2018
Samsung Electronics

*Organizing 2017 Samsung Capture-the-flag (SCTF) — Dec. 2016 – Dec. 2017
Samsung Electronics

A Study on the Security Vulnerability Analysis and Response Method of LTE Networks — Aug. 2016 – Jul. 2017
SK Telecom

A Security Vulnerability Analysis of Smartcar Core Modules — Jul. 2016 – Jun. 2017
Hyundai NGV

A Study on the Security Analysis and Response Method of LTE Networks — Aug. 2015 – Apr. 2016
SK Telecom

A Security Analysis of Samsung SmartTV 2014 — Feb. 2014 – Dec. 2015
Samsung Electronics

International Projects

*Cyber Physical Analysis of System Software Survivability by Stimulating Sensors on Drones — Jun. 2020 – May 2021
Air Force Office of Scientific Research (AFOSR), Air Force Research Laboratory (AFRL)

Governmental Projects

*A Study on the Android-based Security Analysis Technology — May 2020 – Dec. 2020
National Security Research (NSR)

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

*A Study on the Firmware Emulation Technology for Linux-based Routers — May 2017 – Oct. 2017
NSR

A Development of Automated Reverse Engineering and Vulnerability Detection Base Technology through Binary Code Analysis — Apr. 2016 – Dec. 2018
IITP

*A CAPTCHA Design based on Human Perception Characteristics — Apr. 2016 – Dec. 2016
KAIST

*A Study on the Vulnerability Analysis Method of Domestic/International Smartcars — Apr. 2015 – Nov. 2015
NSR

A Study on the Analysis of Technology and Security Threats in LTE Femtocell — Sep. 2013 – Jan. 2014
Korea Internet & Security Agency (KISA)

A Stduy on the Analysis and Response Method of Vulnerabilities in Network Devices — Mar. 2013 – Dec. 2013
NSR

A Stduy on the Vulnerability Analysis of Network Devices — Apr. 2011 – Oct. 2011
NSR

Other Activities

Student Representative of School of Computing, KAIST — Feb. 2011 – Dec. 2013

Teaching Experience

Teaching Assistant, Introduction to Electronics Design Lab. (EE305), KAIST	Fall 2019
Teaching Assistant, Discrete Methods for Electrical Engineering (EE213), KAIST	Spring 2017
Teaching Assistant, Network Programming (EE324), KAIST	Fall 2016
Teaching Assistant, Cryptography Engineering (EE817/IS893), KAIST	Spring 2016
Teaching Assistant, Security 101: Think Like an Adversary (EE515/IS523), KAIST	Fall 2015
Head Instructor, Information Security 101 for Freshmen (HSS062), KAIST	Sep. 2011 – Feb. 2013
Teaching Assistant, Information Security 101 for Freshmen (HSS062), KAIST	Sep. 2010 – Aug. 2011

List of References

Dr. Yongdae Kim

Chair Professor, 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/

Dr. Sang Kil Cha

Director, Cyber Sercurity 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/

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/

Dr. Yeongjin Jang

Assistant Professor, Computer Science, Oregon State University

Email: yeongjin.jang@oregonstate.edu

Homepage: http://people.oregonstate.edu/~jangye

Dr. Insu Yun

Assistant Professor, School of Electrical Engineering and Graduate School of Information Security, KAIST

Email: insuyun@kaist.ac.kr

Homepage: https://insuyun.github.io/

Dr. Sukyoung Ryu

Head, School of Computing, KAIST

Professor, School of Computing, KAIST

Email: sryu.cs@kaist.ac.kr

Homepage: https://plrg.kaist.ac.kr/ryu