

Insu Yun

Assistant Professor
School of Electrical Engineering,
Korea Advanced Institute of Science and Technology (KAIST)

Email: insuyun@kaist.ac.kr
Web: <https://insuyun.github.io>

Research Interests

System security, software security, binary analysis, fuzzing, and applied cryptography.

Education

| | |
|---|-----------------------|
| Georgia Institute of Technology Ph.D. in Computer Science Advisor: Dr. Taesoo Kim | Aug. 2015 – Dec. 2020 |
| Korea Advanced Institute of Science and Technology (KAIST) B.S. in Computer Science & Mathematics | Sep. 2008 – Feb. 2015 |

Work Experience

| | |
|--|-----------------------|
| KAIST , Daejeon, South Korea Assistant Professor | Feb. 2021 – |
| Microsoft Research , Research Intern, Seattle, WA Contributed to REPT, a system that utilizes Intel Processor Trace to diagnose production failures Mentor: Weidong Cui | May. 2017 – Aug. 2017 |
| Georgia Tech , Research Assistant, Atlanta, GA | Aug. 2015 – Dec. 2020 |
| Korean Cyber Command , Software Developer, Seoul, Korea Served for the mandatory military service | Apr. 2012 – Jan. 2014 |

Publications

International Journal

1. **Scalable and Secure Virtualization of HSM with ScaleTrust**
Juhyang Han, **Insu Yun**, Seongmin Kim, Taesoo Kim, Soeul Son, and Dongsu Han
IEEE/ACM Transactions on Networking (ToN)
November 2022

International Conferences (**Top-tier** and others)

18. **BaseComp: A Comparative Analysis for Integrity Protection in Cellular Baseband Software (to appear)**
Eunsoo Kim*, Min Woo Baek*, CheolJun Park, Dongkwan Kim, Yongdae Kim, and **Insu Yun**
Proceedings of the 32nd USENIX Security Symposium (**Security 2023**)
Anaheim, CA, August 2023
17. **QueryX: Symbolic Query on Decompiled Code for Finding Bugs in COTS Binaries**
HyungSeok Han, JeongOh Kyea, Yonghwi Jin, Jinoh Kang, Brian Park, and **Insu Yun**
Proceedings of the 44th IEEE Symposium on Security and Privacy (**Oakland 2023**)
San Francisco, CA, May 2023

16. **Fuzzing@Home: Distributed Fuzzing on Untrusted Heterogeneous Clients**
Daehee Jang, Ammar Askar, **Insu Yun**, Stephen Tong, Yiqin Cai, and Taesoo Kim
Proceedings of the 2022 International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2022)
October 2022
15. **DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices**
CheolJun Park*, Sangwook Bae*, BeomSeok Oh, Jiho Lee, Eunkyu Lee, **Insu Yun**, and Yongdae Kim
Proceedings of the 31th USENIX Security Symposium ([Security 2022](#))
Boston, MA, August 2022
(Acceptance rates: 18%, 256/1414)
14. **HardsHeap: A Universal and Extensible Framework for Evaluating Secure Allocators**
Insu Yun, Woosun Song, Seunggi Min, and Taesoo Kim
Proceedings of the 28th ACM Conference on Computer and Communications Security ([CCS 2021](#))
Seoul, South Korea, November 2021
(Acceptance rates: 22%, 196/880)
13. **Preventing Use-After-Free Attacks with Fast Forward Allocation**
Brian Wickman, Hong Hu, **Insu Yun**, Daehee Jang, JungWon Lim, Sanidhya Kashyap, and Taesoo Kim
Proceedings of the 30th USENIX Security Symposium ([Security 2021](#))
Vancouver, B.C., Canada, August 2021
(Acceptance rates: 19%, 246/1316)
12. **BaseSpec: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols**
Eunsoo Kim*, Dongkwan Kim*, Cheoljun Park, **Insu Yun**, and Yongdae Kim
Proceedings of the 2021 Annual Network and Distributed System Security Symposium ([NDSS 2021](#))
February 2021
(Acceptance rates: 15%, 87/578)
11. **Automatic Techniques to Systematically Discover New Heap Exploitation Primitives**
Insu Yun, Dhaval Kapil, and Taesoo Kim
Proceedings of the 29th USENIX Security Symposium ([Security 2020](#))
Boston, MA, August 2020
(Acceptance rates: 16%, 157/977)
10. **Compromising the macOS kernel through Safari by chaining six vulnerabilities**
Yonghwi Jin, Jungwon Lim, **Insu Yun**, and Taesoo Kim
Black Hat USA Briefings (Black Hat USA 2020)
Las Vegas, NV, August 2020
9. **Fuzzing JavaScript Engines with Aspect-preserving Mutation**
Soyeon Park, Wen Xu, **Insu Yun**, Daehee Jang, and Taesoo Kim
Proceedings of the 41st IEEE Symposium on Security and Privacy ([Oakland 2020](#))
San Francisco, CA, May 2020
(Acceptance rates: 12%, 104/841)
[Nominated as a finalist in CSAW Best Applied Research Paper Award 2020](#)
8. **REPT: Reverse Debugging of Failures in Deployed Software**
Weidong Cui, Xinyang Ge, Baris Kasikci, Ben Niu, Upamanyu Sharma, Ruoyu Wang, and **Insu Yun** (alphabetical)
Proceedings of the 13th USENIX Symposium on Operating Systems Design and Implementation ([OSDI 2018](#))
Carlsbad, CA, October 2018
(Acceptance rates: 18%, 47/257)
[Jay Lepreau Best Paper Award \(3 out of 257 submissions\)](#)
7. **QSYM: A Practical Concolic Execution Engine Tailored for Hybrid Fuzzing**

Insu Yun, Sangho Lee, Meng Xu, Yeongjin Jang, and Taesoo Kim
Proceedings of the 27th USENIX Security Symposium (**Security 2018**)
Baltimore, MD, August 2018
(Acceptance rates: 19%, 100/524)

Distinguished Paper Award (5 out of 524 submissions)

6. **AVPASS: Leaking and Bypassing Antivirus Detection Model Automatically**

Jinho Jung, Chanil Jeon, Max Wolotsky, **Insu Yun**, and Taesoo Kim
Black Hat USA Briefings (Black Hat USA 2017)
Las Vegas, NV, July 2017

5. **CAB-Fuzz: Practical Concolic Testing Techniques for COTS Operating Systems**

Su Yong Kim, Sangho Lee, **Insu Yun**, Wen Xu, Byoungyoung Lee, Youngtae Yun, and Taesoo Kim
Proceedings of the 2017 USENIX Annual Technical Conference (**ATC 2017**)
Santa Clara, CA, July 2017
(Acceptance rates: 21%, 60/283)

4. **APISan: Sanitizing API Usages through Semantic Cross-checking**

Insu Yun, Changwoo Min, Xujie Si, Yeongjin Jang, Taesoo Kim, and Mayur Naik
Proceedings of the 25th USENIX Security Symposium (**Security 2016**)
Austin, TX, August 2016
(Acceptance rates: 16%, 72/463)

Nominated as a finalist in CSAW Best Applied Research Paper Award 2016

3. **HDFI: Hardware-Assisted Data-Flow Isolation**

Chengyu Song, Hyungon Moon, Monjur Alam, **Insu Yun**, Byoungyoung Lee, Taesoo Kim, Wenke Lee, and Yunheung Paek
Proceedings of the 37th IEEE Symposium on Security and Privacy (**Oakland 2016**)
San Jose, CA, May 2016
(Acceptance rates: 13%, 55/413)

2. **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 2014)
Jeju Island, Korea, August 2014

1. **Kargus: A Highly-scalable Software-based Intrusion Detection System**

Muhammad Jamshed, Jihyung Lee, Sangwoo Moon, **Insu Yun**, Deokjin Kim, Sungryoul Lee, Yung Yi, and KyoungSoo Park
Proceedings of the 19th ACM Conference on Computer and Communications Security (**CCS 2012**)
Raleigh, NC, October 2012
(Acceptance rates: 19%, 81/426)

Domestic Conferences

1. **Analyzing Qualcomm Hexagon Emulators via Differential Testing**

Hyunsik Jung, **Insu Yun**, and Yongdae Kim
Proceedings of the Conference on Information Security and Cryptography Summer(CISC-S) 2021
June 2021

Thesis

1. **Concolic Execution Tailored for Hybrid Fuzzing**

Insu Yun
Ph.D. thesis, Georgia Institute of Technology
Atlanta, GA, December 2020

Professional Activities

Technical Program Committee (International)

Program Committee, *Network and Distributed System Security Symposium (NDSS)*, 2024

Program Committee, *IEEE Symposium on Security and Privacy (Oakland)*, 2024

Program Committee, *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2023

Program Committee, *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2022

Others (International & Domestic)

Artifact Evaluation Committee, *USENIX Security Symposium (Security)*, 2023

Organization Committee, *ACM Conference on Computer and Communications Security (CCS)*, 2021

Organization Committee, *Conference on Information Security and Cryptography Summer (CISC-S)*, 2021

Teaching Experience

| | |
|--|-------------|
| Software Hacking Theory and Practice (EE517 at KAIST) | Spring 2023 |
| • Evaluation – Average: 4.54 / 5 | |
| My Life and Career in EE I (EE485-C at KAIST) | Spring 2023 |
| • Evaluation – Average: 4.80 / 5 | |
| Programming Structures for Electrical Engineering (EE209 at KAIST) | Fall 2022 |
| • Evaluation – Average: 4.65 / 5 | |
| Software development environment and tools practice (EE485-A at KAIST) | Fall 2022 |
| • Evaluation – Average: 4.43 / 5 | |
| My Life and Career in EE II (EE485-C at KAIST) | Fall 2022 |
| • Evaluation – Average: 4.70 / 5 | |
| Software Security (EE595-B at KAIST) | Spring 2022 |
| • Evaluation – Average: 5 / 5 | |
| My Life and Career in EE I (EE485-C at KAIST) | Spring 2022 |
| • Evaluation – Average: 4.65 / 5 | |
| Programming Structures for Electrical Engineering (EE209 at KAIST) | Fall 2021 |
| • Evaluation – Average: 4.34 / 5 | |
| Software development environment and tools practice (EE485-A at KAIST) | Fall 2021 |
| • Evaluation – Average: 4.34 / 5 | |
| My Life and Career in EE II (EE485-C at KAIST) | Fall 2021 |
| • Evaluation – Average: 4.57 / 5 | |
| Software Security (EE595-B at KAIST) | Spring 2021 |
| • Evaluation – Average: 4.9 / 5 | |

Honors & Awards

Academic awards

| | |
|---|-----------|
| Best Teaching Award, KAIST Electrical Engineering | Sep. 2021 |
| Jay Lepreau Best Paper Award, USENIX OSDI 2018 | Aug. 2018 |
| Distinguished Paper Award, USENIX Security 2018 | Aug. 2018 |
| KISA Bug Bounty Program's Hall of Fame | 2013 |

Hacking competitions

| | |
|---|-----------|
| DEFCON 26 CTF, 1st place (Team DEFKOR00T) | Aug. 2018 |
| DEFCON 24 CTF, 3rd place (Team DEFKOR) | Aug. 2016 |
| DARPA Cyber Grand Challenge (Team Disekt) | Aug. 2016 |

| | |
|--|-----------|
| DEFCON 23 CTF, 1st place (Team DEFKOR) | Aug. 2015 |
| Whitehat contest 2014, 1st place (Team SysSec) | Nov. 2014 |
| DEFCON 22 CTF, 10th place (Team GoN) | Aug. 2014 |
| SECCON CTF 2014, 1st place (TOEFL Beginner) | Feb. 2014 |
| Codegate CTF 2012, 3rd place (Team GoN) | Apr. 2012 |
| Secuinside CTF, 3rd place (Team GoN) | Oct. 2011 |
| ISEC CTF, 1st place (Team GoN) | Sep. 2011 |
| DEFCON 18 CTF, 3rd place (Team GoN) | Aug. 2010 |
| Codegate CTF 2010, 5th place (Team GoN) | Apr. 2010 |
| KISA HDCON, Gold Medal, 2nd place (Team GoN) | May 2009 |
| Codegate CTF 2009, 4th place (Team GoN) | Apr. 2009 |

Scholarships

| | |
|---|-----------------------|
| National Research Foundation of Korea Scholarship for Undergraduate | Mar. 2008 – Dec. 2013 |
|---|-----------------------|

Vulnerability Discovery Reward (aka Bug bounty)

To summarize, \$113K bug bounties are awarded so far.

With my students

| | |
|--|-----------|
| Type confusion in V8 (\$7,000), Google, by Haein Lee | Mar. 2023 |
| NAS authentication bypass in Exynos (\$14,760), Samsung Electronics, by Eunsoo Kim and CheolJun Park | Feb. 2022 |

By myself

| | |
|---|-----------|
| PSV-2021-0304: afpd auth bypass (\$300), NETGEAR | Mar. 2021 |
| Pwn2Own Apple Safari with a kernel privilege escalation (\$70,000), Zero Day Initiative, with Yonghwi Jin and Jungwon Lim | Mar. 2020 |
| Apple Safari sandbox escape (\$20,000), Apple | Dec. 2019 |
| Three integer overflow vulnerabilities in PHP (\$1,500), the Internet Bug Bounty | Jun. 2016 |
| An Integer Overflow in Python zipimport (\$1,000), the Internet Bug Bounty | Apr. 2016 |

Patents

International

2. Security analysis system and method based on negative testing for protocol implementation of LTE device (Pending)

Inventors: Yongdae Kim, Cheoljun Park, Sangwook Bae, Beomseok Oh, Jiho Lee, Mincheol Son, Insu Yun
Application date: 2022.10.05
Application number: 17960246
Country: US

1. Reverse debugging of software failures

Inventors: Weidong Cui, Xinyang Ge, Baris Kasikci, Cengiz Can, Ben Niu, Ruoyu Wang, Insu Yun
Registration date: 10565511
Patent number: 2020.02.18
Country: US

Domestic

3. Security analysis system and method based on negative testing for protocol implementation of LTE device

Inventors: Yongdae Kim, CheolJun Park, Sangwook Bae, BeomSeok Oh, Jiho Lee, Eunkyu Lee, Insu Yun

Registration date: 10-2514797-0000

Patent number: 2023.03.23

Country: Korea

2. Method and system for automatically analyzing bugs in cellular baseband software using comparative analysis based on cellular specifications

Inventors: Yongdae Kim, Eunsoo Kim, Dongkwan Kim, CheolJun Park, Insu Yun

Registration date: 10-2546946-0000

Patent number: 2023.06.20

Country: Korea

1. Methods and systems for key management service provision (Pending)

Inventors: Dongsoo Han, JuHyeng Han, Insu Yun

Application date: 10-2021-0154174

Application number: 2021.11.10

Country: Korea

Invited Talks

International

Title: How to build Skynet — a system that hacks systems

Keynote speech at TyphoonCon, Seoul, Korea

Jun. 2023

Title: HardsHeap: A Universal and Extensible Framework for Evaluating Secure Allocators

Presented at ACM CCS 2021, Online

Nov. 2021

Title: Automatic Techniques to Systematically Discover New Heap Exploitation Primitives

Presented at USENIX Security 2020, Online

Aug. 2020

Title: QSYM: A Practical Concolic Execution Engine Tailored for Hybrid Fuzzing

Presented at USENIX Security 2018, Baltimore, MD

Aug. 2018

Title: APISan: Sanitizing API Usages through Semantic Cross-checking

Presented at USENIX Security 2016, Austin, TX

Aug. 2016

Domestic

Title: Human-friendly binary analysis

Presented at Korea Computer Congress (KCC), Seoul, Korea

Jun. 2023

Title: Exploit in the wild

Presented at ETRI, Daejeon

Jun. 2023

Title: Hacking 101

Presented at WISC, Seoul

Sep. 2022

Title: Attack and Defenses for Heap Vulnerabilities in 2022

Seminar at ETRI, Daejeon

Apr. 2022

Title: Comparative Analysis of Baseband Software and Cellular Specifications for Finding Vulnerabilities

Seminar at UNIST, Ulsan

May. 2023

Seminar at Security@KAIST, Online

Jun. 2022

Seminar at Cyber Operations Command, Seoul

Jun. 2022

| | |
|---|-----------|
| Title: Scalable and Automatic Vulnerability Discovery Beyond Random Testing | |
| Seminar at Seoul National University, Seoul, Korea, Mar. 2019 | |
| Title: Memory Allocator Security | |
| Presented at Best of Best (BoB), Seoul | Feb. 2023 |
| Presented at Computer System Society Conference (CSC), Pyeongchang | Feb. 2023 |
| Seminar at UNIST, Online | May. 2022 |
| Seminar at Yonsei university, Online | Apr. 2022 |
| Seminar at Sungkyunkwan university, Online | Apr. 2022 |
| Seminar at ETRI, Daejeon | Jan. 2022 |
| Seminar at National Security Research Institute (NSRI), Daejeon | Dec. 2021 |
| Seminar at Securty@KAIST, Online | Nov. 2021 |
| Seminar at KAIST GSIS, Online | Nov. 2021 |
| Title: Browser Security: Hacking & Research | |
| Presented at Open Theori Research Seminar #6, Online | Dec. 2021 |
| Seminar at Hanyang University, Online | Nov. 2021 |
| Presented at KR Becks Meetup #1 by LINE, Online | Aug. 2021 |
| Seminar at Security@KAIST, Online | Jun. 2021 |

Grants

To summarize, \$1.4 million is awarded, and my portion is \$0.93 million. Please note that I have accounted for the exchange rate of 1,000 won to one dollar.

| | |
|---|---------------|
| Building a system to assist variant analysis for browser | 23.06 – 24.05 |
| Agency/Company: NRF | |
| Money: \$65K | |
| Role: PI | |
| Generating a security model based on JavaScript intermediate language | 23.04 – 23.10 |
| Agency/Company: NSRI | |
| Money: \$54.5K | |
| Role: PI | |
| Verifying security threats in open-source operating systems | 23.04 – 23.10 |
| Agency/Company: NSRI | |
| Money: \$54.5K | |
| Role: PI | |
| An automated framework that generates exploit for multi-type kernel bugs | 23.02 – 23.11 |
| Agency/Company: CISC | |
| Money: \$100K | |
| Role: PI | |
| Browser fuzzing with formal verification for cross architectures | 22.09 – 23.09 |
| Agency/Company: NRF | |
| Money: \$110K | |
| Role: PI | |
| Building test suites for validating vulnerability detection | 22.08 – 22.11 |
| Agency/Company: ETRI | |
| Money: \$27.3K | |
| Role: PI | |
| Generating a security model based on JavaScript security analysis | 22.04 – 22.10 |
| Agency/Company: NSRI | |
| Money: \$54.5K | |
| Role: PI | |

| | |
|---|---------------|
| Developing techniques for collection and integrated analysis of automotive systems through event-based experimental systems | 22.04 – 23.12 |
| Agency/Company: Dankook university | |
| Money: \$300K \times 0.5 | |
| Role: PI working with Prof. Yujip Won | |
| 6G security | 21.08 – 23.09 |
| Agency/Company: Samsung Electronics | |
| Money: \$200K \times 0.2 | |
| Role: Co-PI with Prof. Yongdae Kim | |
| DRAM security | 21.07 – 24.06 |
| Agency/Company: Samsung Electronics | |
| Money: \$180K \times 0.2 | |
| Role: Co-PI with Prof. Yongdae Kim | |
| Systematic and precise transformation of the Qualcomm Hexagon architecture into intermediate representations for binary analysis | 21.06 – 22.05 |
| Agency/Company: NRF | |
| Money: \$46.7K | |
| Role: PI | |
| Automatically generating a security model for discovering web browser vulnerabilities | 21.04 – 21.10 |
| Agency/Company: NSRI | |
| Money: \$54.5K | |
| Role: PI | |
| Developing a scalable cyber reasoning system (Start-up) | 21.02 – 24.12 |
| Agency/Company: KAIST | |
| Money: \$150K | |
| Role: PI | |

Advising and Mentoring

Ph.D./M.S Students

| | |
|--------------|-----------|
| - Eunkyu Lee | Fall 2023 |
|--------------|-----------|

Ph.D./M.S Students

| | |
|-------------|-------------|
| - Haein Lee | Spring 2022 |
|-------------|-------------|

M.S. Students

| | |
|-----------------|-------------|
| - Minwoo Baek | Spring 2022 |
| - Wonyeong Jung | Spring 2022 |
| - Junyeong Park | Spring 2022 |
| - Dongok Kim | Spring 2023 |
| - Seunggi Min | Fall 2023 |

Alumni

| | |
|--|--------------------|
| - Hyunsik Jeong (Co-advising with Yongdae Kim), S2W | M.S. in Fall 2021 |
| - Hyunseok Han (Co-advising with Yongdae Kim), Postdoc at Georgia Tech | Ph.D. in Fall 2022 |