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

Binary analysis, system security and applied cryptography.

Education

Georgia Institute of Technology Aug. 2015 – Dec. 2020
Ph.D. in Computer Science
Advisor: Dr. Taesoo Kim

Korea Advanced Institute of Science and Technology (KAIST) Sep. 2008 – Feb. 2015
B.S. in Computer Science & Mathematics

Publications

International Conferences

1. **DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices (to appear)**
   CheolJun Park*, Sangwook Bae*, BeomSeok Oh, Jiho Lee, Eunkyu Lee, **Insu Yun**, and Yongdae Kim (* co-first)
   Proceedings of the 31th USENIX Security Symposium (Security 2022)
   Boston, MA, August 2022

2. **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

3. **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

4. **BaseSpec: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols**
   Eunsoo Kim*, Dongkwan Kim*, Cheoljun Park, **Insu Yun**, and Yongdae Kim (* co-first)
   Proceedings of the 2021 Annual Network and Distributed System Security Symposium (NDSS 2021)
   February 2021

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

6. **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

7. **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

8. **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

9. **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
   • **Jay Lepreau Best Paper Award**

10. **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
    • **Distinguished Paper Award**

11. **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

12. **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

13. **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
    • **Nominated as a finalist in CSAW Best Applied Research Paper Award 2016**

14. **HDFI: Hardware-Assisted Data-Fow 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

15. **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

16. **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

Domestic Conferences

17. **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

Work Experience

KAIST, Daejeon, South Korea — Feb. 2021 –
Assistant Professor

Microsoft Research, Research Intern, Seattle, WA — May. 2017 – Aug. 2017
Contributed to REPT, a system that utilizes Intel Processor Trace to diagnose production failures
Mentor: Weidong Cui

Georgia Tech, Research Assistant, Atlanta, GA — Aug. 2015 – Dec. 2020
Korean Cyber Command, Software Developer, Seoul, Korea — Apr. 2012 – Jan. 2014
Served for the mandatory military service

Professional Activities

International Conference Committee Activities

Program Committee, *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2022
Organization Committee, *ACM Conference on Computer and Communications Security (CCS)*, 2021

Domestic Conference Committee Activities

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

Teaching Experience

Instructor, Programming Structures for Electronical Engineering (EE209 at KAIST) — Fall 2021
- Evaluation – Average: 4.34 / 5

Instructor, Software development environment and tools practice (EE485-A at KAIST) — Fall 2021
- Evaluation – Average: 4.34 / 5

Instructor, My Life and Career in EE II (EE485-C at KAIST) — Fall 2021
- Evaluation – Average: 4.57 / 5

Instructor, Software Security (EE595-B at KAIST) — Spring 2021
- Evaluation – Average: 4.9 / 5

Teaching Assistant, Information Security Lab – Official (CS8803 at Georgia Tech) — Fall 2018
- Evaluation – Overall Effectiveness: 5 / 5

Teaching Assistant, Information Security Lab – Unofficial (CS8803 at Georgia Tech) — Fall 2017

Teaching Assistant, Information Security Lab – Official (CS6265 at Georgia Tech) — Fall 2016
- Evaluation – Overall Effectiveness: 4.9 / 5

Teaching Assistant, Information Security Lab – Unofficial (CS6265 at Georgia Tech) — Fall 2015

Head Instructor, Information Security class for freshmen (KAIST) — Mar. 2009 – Aug. 2011

Honors & Awards

Academic awards

Best Lecture Award, KAIST Electrical Engineering — Sep. 2021
Jay Lepreau Best Paper Award, USENIX OSDI 2018 — Aug. 2018
Distinguished Paper Award, USENIX Security 2018 — Aug. 2018

Capture-the-flag(CTF) contests

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 (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

Bug Hunting

PSV-2021-0304: afpd auth bypass ($300), NETGEAR Cash Rewards Mar. 2021
Pwn2Own Apple Safari with a kernel privilege escalation ($70K), Zero Day Initiative Mar. 2020
Apple Safari sandbox escape ($20K), 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

Scholarships

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

Invited Talks

Memory Allocator Security

Seminar at National Security Research Institute (NSRI) Dec. 2021
Seminar at Securty@KAIST Nov. 2021
Seminar at KAIST GSIS Nov. 2021

Browser Security: Hacking & Research

Seminar at Hanyang University Dec. 2021
Presented at KR Becks Meetup #1 by LINE Aug. 2021
Seminar at Security@KAIST Jun. 2021
Presented at Open Theori Research Seminar #6 Dec. 2021

HardsHeap: A Universal and Extensible Framework for Evaluating Secure Allocators

Presented at ACM CCS 2021 Nov. 2021

Automatic Techniques to Systematically Discover New Heap Exploitation Primitives

Presented at USENIX Security 2020 Aug. 2020

Scalable and Automatic Vulnerability Discovery Beyond Random Testing

Seminar at Seoul National Univeristy Mar. 2019

QSYM: A Practical Concolic Execution Engine Tailored for Hybrid Fuzzing

Presented at USENIX Security 2018 Aug. 2018

APISan: Sanitizing API Usages through Semantic Cross-checking

Presented at USENIX Security 2016 Aug. 2016

Advising and Mentoring

- **Ph.D. Students**

- Hyunseok Han (Co-advising with Yongdae Kim) — Starting from Spring 2022

- **M.S. Students**
  - Minwoo Baek — Starting from Spring 2022
  - Wonyeong Jung — Starting from Spring 2022
  - Haein Lee — Starting from Spring 2022
  - Junyeong Park — Starting from Spring 2022

- **Alumni**
  - Hyunsik Jeong (Co-advising with Yongdae Kim) — M.S. in Fall 2021
    First employment: S2W

Grants

In total, **$460K** is awarded, and my share is **$300K**.

1. **6G security technology**
   Agency/Company: Samsung Electronics
   Total amount: $100,000
   Collaborators: Yongdae Kim (PI)
   Role: co-PI
   Period: 2021/08/16 – 2022/08/15
   Share: 20%

2. **DRAM security**
   Agency/Company: Samsung Electronics
   Total amount: $100,000
   Collaborators: Yongdae Kim (PI)
   Role: co-PI
   Period: 2021/07/01 – 2022/06/30
   Share: 20%

3. **Systematic and precise transformation of the Qualcomm Hexagon architecture into intermediate representations for binary analysis**
   Agency/Company: National Research Foundation (NRF)
   Total amount: $50,000
   Role: PI
   Period: 2021/06/01 – 2022/05/31
   Share: 100%

4. **Automatic generation of security model for web browser vulnerability discovery**
   Agency/Company: National Security Research Institute (NSRI)
   Total amount: $60,000
   Role: PI
   Period: 2021/04/01 – 2021/11/31
   Share: 100%

5. **Building a scalable cyber reasoning system (Startup)**
   Agency/Company: KAIST
   Total amount: $150,000
   Role: PI
   Period: 2021/02/01 – 2024/12/31
   Share: 100%