Kyungtae Kim

CONTACT

305 N. University Street,
West Lafayette, IN 47907, USA

kim1798@purdue.edu
kt0755.github.io

RESEARCH INTERESTS

Systems and Software Security; Program Analysis

EDUCATION

Purdue University, West Lafayette, IN

Ph.D., Computer Science — Aug. 2014 – Dec. 2022

- Thesis: *Securing System and Embedded Software via Fuzzing*
- Advisors: Prof. Dave (Jing) Tian and Prof. Byoungyoung Lee

Hongik University, Seoul, South Korea

M.S., Computer Engineering — Aug. 2009 – Aug. 2011

- Thesis: *Dual Encoding Technique for Protection of Data Pointers against Heap Attack*

B.S., Computer Engineering — Mar. 2003 – Aug. 2009

WORK EXPERIENCE

Postdoctoral Researcher — Jan. 2023 – present

Department of Computer Science,
Purdue University

Research Assistant — Aug. 2014 – Dec. 2022

Department of Computer Science,
Purdue University

Research Intern — May. 2019 – Aug.2019

Data Science and System Security Department,
NEC Laboratories America

Researcher — Mar. 2012 – Feb. 2014

Research Institute of Science and Technology,
Hongik University

Military Service — Dec. 2004 – Dec. 2006

Republic of Korea Army

PUBLICATIONS

1. **Kyungtae Kim**, Sungwoo Kim, Kevin Buttler, Antonio Bianchi, Rick Kennell, Dave (Jing) Tian. *"Fuzz The Power: Dual-role State Guided Black-box Fuzzing for USB Power Delivery."* In Proceedings of the 32nd USENIX Security Symposium, Anaheim, CA, August 2023 (USENIX Sec 2023)
2. Arslan Khan, Muqi Zou, **Kyungtae Kim**, Antonio Bianchi, Dave (Jing) Tian. *"Fuzzing SGX Enclaves via Host Program Mutations."* In Proceedings of the 8th IEEE European Symposium on Security and Privacy, Delft, Netherlands, July 2023 (Euro S&P 2023).
3. Trung Nguyen, **Kyungtae Kim**, Antonio Bianchi, Dave (Jing) Tian. *"TruEMU: An Extensible, Open-Source, Whole-System iOS Emulator"* BlackHat USA 2022.
4. **Kyungtae Kim**, Taegyu Kim, Ertza Warraich, Byoungyoung Lee, Kevin Butler, Antonio Bianchi, Dave (Jing) Tian. *"FuzzUSB: Hybrid Stateful Fuzzing of USB Gadget Stacks."* In Proceedings of the 43rd IEEE Symposium on Security and Privacy, San Francisco, CA, May 2022 (S&P 2022).

5. Taegyu Kim, Vireshwar Kumar, Junghwan Rhee, Jizhou Chen, **Kyungtae Kim**, Chung Hwan Kim, Dongyan Xu, Dave Tian. *"PASAN: Detecting Peripheral Access Concurrency Bugs within Bare-metal Embedded Applications."* In Proceedings of the 30th USENIX Security Symposium, Virtual Event, August 2021 (USENIX Sec 2021)

6. **Kyungtae Kim**, Chung Hwan Kim, Junghwan Rhee, Xiao Yu, Haifeng Chen, Dave (Jing) Tian, Byoungyoung Lee. *"VESSELS: Efficient and Scalable DNN Prediction on Trusted Processors."* In Proceedings of the 11th ACM Symposium on Cloud Computing, Virtual Event, Octobor 2020 (SoCC 2020)

7. **Kyungtae Kim**, Dae R. Jeong, Chung Hwan Kim, Yeongjin Jang, Insik Shin, Byoungyoung Lee. *"HFL: Hybrid Fuzzing on the Linux Kernel."* In Proceedings of the 27th Network and Distributed System Security Symposium, San Diego, CA, February 2020 (NDSS 2020)

8. Dae R. Jeong, **Kyungtae Kim**, Basavesh Ammanaghatta Shivakumar, Byoungyoung Lee, Insik Shin. *"Razzer: Finding Kernel Race Bugs through Fuzzing."* In Proceedings of the 40th IEEE Symposium on Security and Privacy, San Francisco, CA, May 2019 (S&P 2019).

9. Adil Ahmad, **Kyungtae Kim**, Muhammad Ihsanulhaq Sarfraz, Byoungyoung Lee. *"OBLIVIATE: A Data Oblivious File System for Intel SGX."* In Proceedings of the 25th Network and Distributed System Security Symposium, San Diego, CA, February 2018 (NDSS 2018).

10. **Kyungtae Kim**, I Luk Kim, Chung-hwan Kim, Yonghwi Kwon, Yunhui Zheng, Xiangyu Zhang, Dongyan Xu. *"J-Force: Forced Execution on JavaScript."* In Proceedings of the 26th International Conference on World Wide Web, Perth, Australia, April 2017 (WWW 2017)

11. Yonghwi Kwon, Dohyeong Kim, William N. Sumner, **Kyungtae Kim**, Brendan Saltaformaggio, Xiangyu Zhang, Dongyan Xu. *"LDX: Causality Inference by Lightweight Dual Execution."* In Proceedings of the 21st International Conference on Architectural Support for Programming Language and Operating Systems, Atlanta, GA, April 2016 (ASPLOS 2016)

12. Yonghwi Kwon, Fei Peng, Dohyeong Kim, **Kyungtae Kim**, Xiangyu Zhang, Dongyan Xu, Vinod Yegneswaran, John Qian. *"P2C: Understanding Output Data Files via On-the-Fly Transformation from Producer to Consumer Executions."* In Proceedings of the 22nd Network and Distributed System Security Symposium, San Diego, CA, February 2015 (NDSS 2015)

13. **Kyungtae Kim**, Changwoo Pyo. *"Securing Heap Memory by Data Pointer Encoding."* Future Generation Computer Systems, 28(8), 2012 (FGCS 2012)

POSTERS

1. **Kyungtae Kim**, Byoungyoung Lee. *"Alexkidd-Fuzzer: Kernel Fuzzing Guided by Symbolic Information."* 20th Annual Information Security Symposium (CERIAS 2018)

REPORTED SECURITY VULNERABILITIES

Linux Kernel

- CVE-2020-12464, CVE-2020-13143, CVE-2020-13974, CVE-2020-15393, CVE-2020-27784

Android Kernel

- CVE-2021-26689, CVE-2021-0936, CVE-2021-30313

AWARDS

- Bilsland Dissertation Fellowship — Purdue University 2022
- Vulnerability Bounty Award by Android, Google ($600) 2021
- Vulnerability Bounty Award by Android, Samsung ($156) 2021
- ACSAC Student Conferenceship 2021
- Travel Awards — Purdue University, College of Science
  - Graduate Student International Travel Awards ($800) 2017

PATENTS

- Efficient and scalable enclave protection for machine learning programs (US 20210081122A1)
- Dynamic memory management system and the management methods for defense against heap attacks (Korea 10-1166051)

STUDENT MENTORING EXPERIENCE

Trung Nguyen Sep. 2021 – Aug. 2022
- Undergraduate student at Purdue University
- Research interest: iOS system security

Jenny Mendez May. 2022 – Aug. 2022
- Undergraduate student intern from University of California, Berkeley
- Research interest: CPU dynamic testing

TEACHING EXPERIENCE

Guest Lecturer
- CS 528 - Network Security (Spring 2023)
  Purdue University
- CIS 5370 - Computer and Information Security (Spring 2023)
  University of Florida

Teaching Assistant
- CS 426 - Computer Security (Spring 2018)
  Department of Computer Science,
  Purdue University

PROFESSIONAL SERVICE

Program Committee
- IEEE SafeThings 2023
- ISOC NDSS BAR 2023
- IEEE SafeThings 2022

Artifact Evaluation Committee
- USENIX Security 2021

Replicability Committee
- ACM WiSec 2021

Conference External Reviewer
- ISOC NDSS 2019, 2021, 2023
- ACSAC 2021
- ACM CCS 2015, 2016
- ACM ASIACCS 2018, 2021
- IEEE ICDCS 2021
- ICSE 2017
- IEEE/IFIP DSN 2020
- ACM SIGSOFT ISSTA 2016

SOFTWARE ENGINEERING SKILLS

Programming Languages
- C/C++, x86, Python, JavaScript, Go

Development Knowledge
- GCC, GDB, Syzkaller, Darknet, WebKit, S2E, LLVM, QEMU, Klee

REFERENCES

Available on Request