Kyungtae Kim

CONTACT

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

kim1798@purdue.edu
kt0755.github.io

RESEARCH INTERESTS

Software Security; Program Analysis

EDUCATION

Purdue University, West Lafayette, IN

Ph.D., Computer Science — Aug. 2014 – present

- 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

EMPLOYMENT HISTORY

Research Assistant — Aug. 2014 – present

Department of Computer Science,
Purdue University

Research Intern — May. 2019 – Aug.2019

Data Science and System Security Department,
NEC Laboratories America

Teaching Assistant — Jan. 2018 – May. 2018

Department of Computer Science,
Purdue University,
Computer Security (CS 42600), Spring 2018

Researcher — Mar. 2012 – Feb. 2014

Research Institute of Science and Technology,
Hongik University

Military Service — Dec. 2004 – Dec. 2006

Republic of Korea Army

REFERRED INTERNATIONAL PUBLICATIONS

1. Trung Nguyen, **Kyungtae Kim**, Antonio Bianchi, Dave (Jing) Tian. *"TruEMU: An Extensible, Open-Source, Whole-System iOS Emulator"* BlackHat USA 2022.
2. **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 43th IEEE Symposium on Security and Privacy, San Francisco, CA, May 2022 (S&P 2022).
3. 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)

4. **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)

5. **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)

6. 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).

7. 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).

8. **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 17)

9. 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 21th International Conference on Architectural Support for Programming Language and Operating Systems, Atlanta, GA, April 2016 (ASPLOS 16)

10. 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 22th Network and Distributed System Security Symposium, San Diego, CA, February 2015 (NDSS 15)

11. **Kyungtae Kim**, Changwoo Pyo. *"Securing Heap Memory by Data Pointer Encoding."* Future Generation Computer Systems, 28(8), 2012 (FGCS 12)

REFERRED 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

AWARD

Travel Awards — Purdue University, College of Science
- Graduate Student International Travel Awards ($800) 2017

ACSAC Student Conferenceship 2021
Vulnerability Bounty Award by Android, Google ($400) 2021
Vulnerability Bounty Award by Android, Samsung ($156) 2021
Bilsland Dissertation Fellowship — Purdue University 2022

PATENT

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)

Professional Service

Program Committee

- SafeThings 2022

Artifact Evaluation Committee

- Usenix Security 2021

Replicability Committee

- ACM WiSec 2021

External Reviewer

- CCS 2015, ISSTA 2016, CCS 2016, ICSE 2017, ASIACCS 2018, NDSS 2019, DSN 2020, NDSS 2021, ASIACCS 2021, ICDCS 2021, ACSAC 2021

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