Kyungtae Kim

CONTACT

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

+1 (765) 237 2533
kim1798@purdue.edu
kt0755.github.io

RESEARCH INTERESTS

System and Software Security; Program Analysis; Deep Learning Security; Web Security

EDUCATION

Purdue University, West Lafayette, IN

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

- Advisors: Prof. Dave (Jing) Tian and Prof. Byoungyoung Lee

Hongik University, Seoul, South Korea

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

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

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

EMPLOYMENT HISTORY

Research Assistant — Aug. 2014 to present

Department of Computer Science,
Purdue University

Research Intern — May. 2019 to Aug.2019

Data Science and System Security Department,
NEC Laboratories America

Teaching Assistant — Jan. 2018 to May. 2018

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

Researcher — Mar. 2012 to Feb. 2014

Research Institute of Science and Technology,
Hongik University

Military Service — Dec. 2004 to Dec. 2006

Republic of Korea Army

REFERRED INTERNATIONAL PUBLICATIONS

1. **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, Renton, WA, Octobor 2020 (SoCC 2020)

2. **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)

3. 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).

4. 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).

5. **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)

6. 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)

7. 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)

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

Referred Domestic Publications

1. **Kyungtae Kim**, Taehwan Kim, Changwoo Pyo, Gyungho Lee, *"A Method Protecting Control Flow by Indirect Branch Monitoring and Program Counter Encoding,"* Journal of the Korea Institute of Information Scientists and Engineers: Computing Practices and Letters, 2014

2. **Kyungtae Kim**, Changwoo Pyo, Gyungho Lee, *"Expanding the Capability of Linkers for Protecting Function Addresses, The 38th Korea Institute of Information Scientists and Engineers,"* Fall Conference, 2011

3. **Kyungtae Kim**, Changwoo Pyo, Sunil Kim, Gyungho Lee, *"Dual-Encoding of Return Addresses for Detection and Defense against Stack Attacks,"* Journal of the Korea Institute of Information Scientists and Engineers: Computing Practices and Letters 17(3), 2011

4. Sungho Kwon, Youjin Kim, **Kyungtae Kim**, Changwoo Pyo, *"Analysis and Expansion of Wilander's Benchmarks,"* The 37th Korea Institute of Information Scientists and Engineers, Fall Conference, 2010

5. **Kyungtae Kim**, Sungho Kwon, Changwoo Pyo, *"Vulnerable Code Pointers in Android Platform,"* The 37th Korea Institute of Information Scientists and Engineers, Fall Conference, 2010

6. **Kyungtae Kim**, Changwoo Pyo, *"Data Pointer Encoding for Defense against Heap Attack,"* Korea Computer Congress, 2010

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

- CVE-2020-12464: Linux Kernel Use-after-free in USB hcd
- CVE-2020-13143: Linux Kernel Slab-out-of-bounds in USB gadget
- CVE-2020-13974: Linux Kernel Integer overflow in USB keyboard
- CVE-2020-15393: Linux Kernel Memory leak in USB test
- CVE-2020-27784: Linux Kernel Use-after-free in USB gadget

AWARD	Travel Awards — Purdue University, College of Science • Graduate Student International Travel Awards ($800) Feb. 2017
PATENT	Dynamic memory management system and the management methods for defense against heap attacks (No. 10-1166051)
SOFTWARE ENGINEERING SKILLS	Programming Languages • C/C++, x86, Python, JavaScript, Go Development Knowledge • GCC, GDB, Syzkaller, Darknet, WebKit, S2E, LLVM, QEMU, Klee
PROFESSIONAL SERVICE	Artifact Evaluation Committee • Usenix Security 2021 External Reviewer • CCS 2015, ISSTA 2016, CCS 2016, ICSE 2017, ASIACCS 2018, NDSS 2019, DSN 2020, NDSS 2021
REFERENCES	Available on Request