

Kyungtae Kim

CONTACT	15 Thayer Drive, Hanover, NH 03755, USA	kyungtae.kim@dartmouth.edu kt0755.github.io
RESEARCH INTERESTS	Systems and Software Security; Program Analysis	
WORK EXPERIENCE	Assistant Professor	Jan. 2024 –
	Department of Computer Science, Dartmouth College	
	Postdoctoral Researcher	Jan. 2023 – Dec. 2023
	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	
EDUCATION	Purdue University , West Lafayette, IN	
	Ph.D., Computer Science	Aug. 2014 – Dec. 2022
	<ul style="list-style-type: none">• Thesis: <i>Securing System and Embedded Software via Fuzzing</i>• Advisors: Prof. Dave (Jing) Tian and Prof. Byoungyoung Lee	
	Hongik University , Seoul, South Korea	
	M.S., Computer Engineering	Aug. 2009 – Aug. 2011
	<ul style="list-style-type: none">• Thesis: <i>Dual Encoding Technique for Protection of Data Pointers against Heap Attack</i>	
	B.S., Computer Engineering	Mar. 2003 – Aug. 2009
PUBLICATIONS	<ol style="list-style-type: none">1. Kyungtae Kim, Sungwoo Kim, Kevin Butler, Antonio Bianchi, Rick Kennell, Dave (Jing) Tian. “<i>Fuzz The Power: Dual-role State Guided Black-box Fuzzing for USB Power Delivery.</i>” 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. “<i>Fuzzing SGX Enclaves via Host Program Mutations.</i>” 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. “<i>TruEMU: An Extensible, Open-Source, Whole-System iOS Emulator</i>” BlackHat USA 2022.4. Kyungtae Kim, Taegyu Kim, Ertza Warraich, Byoungyoung Lee, Kevin Butler, Antonio Bianchi, Dave (Jing) Tian. “<i>FuzzUSB: Hybrid Stateful Fuzzing of USB Gadget Stacks.</i>” 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, October 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. “*OBLIVIAE: 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 <ul style="list-style-type: none"> • 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)	
PROFESSIONAL SERVICE	Student Grant Chair <ul style="list-style-type: none"> • SecDev 2024 	
	Program Committee <ul style="list-style-type: none"> • IEEE EuroS&P 2024 • IEEE SafeThings 2022, 2023 • ISOC NDSS BAR 2023 	
	Artifact Evaluation Committee <ul style="list-style-type: none"> • USENIX Security 2021 	
	Replicability Committee <ul style="list-style-type: none"> • ACM WiSec 2021 	
	Conference External Reviewer <ul style="list-style-type: none"> • USENIX Security 2024 • 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 	
	Instructor, Dept. of Computer Science, Dartmouth College, Hanover, NH <ul style="list-style-type: none"> • CS 2/69.17 - Software Security (Winter 2024) 	
	Guest Lecturer <ul style="list-style-type: none"> • CS 528 - Network Security (Spring 2023) <ul style="list-style-type: none"> Purdue University • CIS 5370 - Computer and Information Security (Spring 2023) <ul style="list-style-type: none"> University of Florida 	
	Teaching Assistant <ul style="list-style-type: none"> • CS 426 - Computer Security (Spring 2018) <ul style="list-style-type: none"> Department of Computer Science, Purdue University 	
	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	
	Programming Languages	
	SOFTWARE ENGINEERING SKILLS	

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

Development Knowledge

- GCC, GDB, Syzkaller, Darknet, WebKit, S2E, LLVM, QEMU, Klee, Pin

REFERENCES

Available on Request