

## Kyungtae Kim

---

CONTACT	305 N. University Street, West Lafayette, IN 47907, USA	<a href="mailto:kim1798@purdue.edu">kim1798@purdue.edu</a> <a href="https://github.com/kt0755">kt0755.github.io</a>
RESEARCH INTERESTS	Systems and Software Security; Program Analysis	
EDUCATION	<b>Purdue University</b> , West Lafayette, IN	
	Ph.D., Computer Science	Aug. 2014 – Dec. 2022
	<ul style="list-style-type: none"><li>• Thesis: <i>Securing System and Embedded Software via Fuzzing</i></li><li>• Advisors: Prof. Dave (Jing) Tian and Prof. Byoungyoung Lee</li></ul>	
	<b>Hongik University</b> , Seoul, South Korea	
	M.S., Computer Engineering	Aug. 2009 – Aug. 2011
	<ul style="list-style-type: none"><li>• Thesis: <i>Dual Encoding Technique for Protection of Data Pointers against Heap Attack</i></li></ul>	
	B.S., Computer Engineering	Mar. 2003 – Aug. 2009
EMPLOYMENT HISTORY	<b>Postdoctoral Researcher</b>	Jan. 2023 – present
	Department of Computer Science, Purdue University	
	<b>Research Assistant</b>	Aug. 2014 – Dec. 2022
	Department of Computer Science, Purdue University	
	<b>Research Intern</b>	May. 2019 – Aug. 2019
	Data Science and System Security Department, NEC Laboratories America	
	<b>Researcher</b>	Mar. 2012 – Feb. 2014
	Research Institute of Science and Technology, Hongik University	
	<b>Military Service</b>	Dec. 2004 – Dec. 2006
	Republic of Korea Army	
PUBLICATIONS	<ol style="list-style-type: none"><li>1. Arslan Khan, Muqi Zou, <b>Kyungtae Kim</b>, 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&amp;P 2023).</li><li>2. Trung Nguyen, <b>Kyungtae Kim</b>, Antonio Bianchi, Dave (Jing) Tian. “<i>TruEMU: An Extensible, Open-Source, Whole-System iOS Emulator</i>” BlackHat USA 2022.</li><li>3. <b>Kyungtae Kim</b>, 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&amp;P 2022).</li><li>4. Taegyu Kim, Vireshwar Kumar, Junghwan Rhee, Jizhou Chen, <b>Kyungtae Kim</b>, Chung Hwan Kim, Dongyan Xu, Dave Tian. “<i>PASAN: Detecting Peripheral Access Concurrency Bugs within Bare-metal Embedded Applications.</i>” In Proceedings of the 30th USENIX Security Symposium, Virtual Event, August 2021 (USENIX Sec 2021)</li></ol>	

5. **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)
6. **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)
7. Dae R. Jeong, **Kyungtae Kim**, Basavesh Ammanaghatta Shivakumar, Byoungyoung Lee, Insik Shin. “*Razzler: 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).
8. 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).
9. **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)
10. 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)
11. 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)
12. **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

Linux Kernel

#### SECURITY

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

#### VULNERABILITIES

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	<ul style="list-style-type: none"> <li>– Efficient and scalable enclave protection for machine learning programs (US 20210081122A1)</li> <li>– Dynamic memory management system and the management methods for defense against heap attacks (Korea 10-1166051)</li> </ul>
STUDENT MENTORING EXPERIENCE	<p>Trung Nguyen Sep. 2021 – Aug. 2022</p> <ul style="list-style-type: none"> <li>• Undergraduate student at Purdue University</li> <li>• Research interest: iOS system security</li> </ul> <p>Jenny Mendez May. 2022 – Aug. 2022</p> <ul style="list-style-type: none"> <li>• Undergraduate student intern from University of California, Berkeley</li> <li>• Research interest: CPU dynamic testing</li> </ul>
TEACHING EXPERIENCE	<p>Guest Lecturer</p> <ul style="list-style-type: none"> <li>• CS 528 - Network Security (Spring 2023) Purdue University</li> <li>• CIS 5370 - Computer and Information Security (Spring 2023) University of Florida</li> </ul> <p>Teaching Assistant</p> <ul style="list-style-type: none"> <li>• CS 426 - Computer Security (Spring 2018) Department of Computer Science, Purdue University</li> </ul>
PROFESSIONAL SERVICE	<p>Program Committee</p> <ul style="list-style-type: none"> <li>• IEEE SafeThings 2023</li> <li>• ISOC NDSS BAR 2023</li> <li>• IEEE SafeThings 2022</li> </ul> <p>Artifact Evaluation Committee</p> <ul style="list-style-type: none"> <li>• USENIX Security 2021</li> </ul> <p>Replicability Committee</p> <ul style="list-style-type: none"> <li>• ACM WiSec 2021</li> </ul> <p>Conference External Reviewer</p> <ul style="list-style-type: none"> <li>• ISOC NDSS 2019, 2021, 2023</li> <li>• ACSAC 2021</li> <li>• ACM CCS 2015, 2016</li> <li>• ACM ASIACCS 2018, 2021</li> <li>• IEEE ICDCS 2021</li> <li>• ICSE 2017</li> <li>• IEEE/IFIP DSN 2020</li> <li>• ACM SIGSOFT ISSTA 2016</li> </ul>
SOFTWARE ENGINEERING SKILLS	<p>Programming Languages</p> <ul style="list-style-type: none"> <li>• C/C++, x86, Python, JavaScript, Go</li> </ul> <p>Development Knowledge</p> <ul style="list-style-type: none"> <li>• GCC, GDB, Syzkaller, Darknet, WebKit, S2E, LLVM, QEMU, Klee</li> </ul>
REFERENCES	Available on Request