

## 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	System and Software Security; Program Analysis	
EDUCATION	<b>Purdue University</b> , West Lafayette, IN	
	Ph.D., Computer Science	Aug. 2014 – present
	• Advisors: Prof. Dave (Jing) Tian and Prof. Byoungyoung Lee	
	<b>Hongik University</b> , Seoul, South Korea	
	M.S., Computer Engineering	Aug. 2009 – Aug. 2011
	• Thesis: <i>Dual Encoding Technique for Protection of Data Pointers against Heap Attack</i>	
	B.S., Computer Engineering	Mar. 2003 – Aug. 2009
EMPLOYMENT HISTORY	<b>Research Assistant</b>	Aug. 2014 – present
	Department of Computer Science, Purdue University	
	<b>Research Intern</b>	May. 2019 – Aug. 2019
	Data Science and System Security Department, NEC Laboratories America	
	<b>Teaching Assistant</b>	Jan. 2018 – May. 2018
	Department of Computer Science, Purdue University, Computer Security (CS 42600), Spring 2018	
	<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	
REFERRED INTERNATIONAL PUBLICATIONS	<ol style="list-style-type: none"><li>1. 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>2. <b>Kyungtae Kim</b>, Taegy 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>3. Taegy 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>	

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, October 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. “*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).
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 21st 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 22nd 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

- |  |      |
|--|------|
| 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 |

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 <ul style="list-style-type: none"> <li>• IEEE S&amp;P SafeThings 2022</li> </ul> Artifact Evaluation Committee <ul style="list-style-type: none"> <li>• USENIX Security 2021</li> </ul> Replicability Committee <ul style="list-style-type: none"> <li>• ACM WiSec 2021</li> </ul> Conference External Reviewer <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	Programming Languages <ul style="list-style-type: none"> <li>• C/C++, x86, Python, JavaScript, Go</li> </ul> Development Knowledge <ul style="list-style-type: none"> <li>• GCC, GDB, Syzkaller, Darknet, WebKit, S2E, LLVM, QEMU, Klee</li> </ul>
REFERENCES	Available on Request