

## Kyungtae Kim

---

CONTACT	305 N. University Street, West Lafayette, IN 47907, USA	+1 (765) 237 2533 <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; Deep Learning Security	
EDUCATION	<b>Purdue University</b> , West Lafayette, IN	
	Ph.D., Computer Science	Aug. 2014 to present
	• Advisor: Byoungyoung Lee, Dave(Jing) Tian	
	<b>Hongik University</b> , Seoul, South Korea	
	M.S., Computer Engineering	Aug. 2009 to Aug. 2011
	• Thesis: <i>Dual Encoding Technique for Protection of Data Pointers against Heap Attack</i>	
	B.S., Computer Engineering	Mar. 2003 to Aug. 2009
EMPLOYMENT HISTORY	<b>Research Assistant</b>	Aug. 2014 to present
	Department of Computer Science, Purdue University	
	<b>Research Intern</b>	May. 2019 to Aug.2019
	Data Science and System Security Department, NEC Laboratories America	
	<b>Teaching Assistant</b>	Jan. 2018 to May. 2018
	Department of Computer Science, Purdue University, Computer Security (CS 42600), Spring 2018	
	<b>Researcher</b>	Mar. 2012 to Feb. 2014
	Research Institute of Science and Technology, Hongik University	
	<b>Military Service</b>	Dec. 2004 to Dec. 2006
	Republic of Korea Army	
REFERRED INTERNATIONAL PUBLICATIONS	<ol style="list-style-type: none"><li>1. “<i>VESSELS: Efficient and Scalable Deep Learning Prediction on Trusted Processors.</i>” (under review).</li><li>2. “<i>HFL: Hybrid Fuzzing on the Linux Kernel.</i>” (under review).</li><li>3. Dae R. Jeong, <b>Kyungtae Kim</b>, Basavesh Ammanaghatta Shivakumar, Byoungyoung Lee, Insik Shin. “<i>Razzer: Finding Kernel Race Bugs through Fuzzing.</i>” In Proceedings of the 40th IEEE Symposium on Security and Privacy, San Francisco, CA, May 2019 (S&amp;P 2019).</li><li>4. Adil Ahmad, <b>Kyungtae Kim</b>, Muhammad Ihsanulhaq Sarfraz, Byoungyoung Lee. “<i>OBLIVATE: A Data Oblivious File System for Intel SGX.</i>” In Proceedings of the 25th Network and Distributed System Security Symposium, San Diego, CA, February 2018 (NDSS 2018).</li></ol>	

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, 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 Wilanders 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)

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  
 ● Expert in C/C++, x86, Python, fluent in JavaScript, Go

Development Knowledge

- Expert in GCC, GDB, Syzkaller, Darknet, WebKit, S2E, fluent in LLVM, QEMU, Klee

PROFESSIONAL  
SERVICE

External Reviewer

- CCS 2015, ISSTA 2016, CCS 2016, ICSE 2017, ASIACCS 2018, NDSS 2019

REFERENCES

Available on Request