TAESOO KIM

PROFESSOR

SCHOOL OF COMPUTER SCIENCE
SCHOOL OF CYBERSECURITY AND PRIVACY
College of Computing
Georgia Institute of Technology
Atlanta, GA 30332, USA

https://taesoo.kim/
taesoo@gatech.edu

Table of Contents

I. Earned Degrees

Ph.D.	2014	Massachusetts Institute of Technology (MIT)	*Electrical Engineering and Computer Science*
M.S.	2011	Massachusetts Institute of Technology (MIT)	*Electrical Engineering and Computer Science*
B.S.	2009	Korea Advanced Institute of Science and Technology	*Computer Science*
B.S.	2009	Korea Advanced Institute of Science and Technology	*Electrical Engineering*

II. Employment History

Professor	School of Computer Science and School of Cybersecurity and Privacy Georgia Institute of Technology, Atlanta, GA	*April 2022–present*
Corporate VP	Samsung Electronics Seoul, South Korea	*May 2021–present*
Chief Scientist	Furiosa.ai Seoul, South Korea	*May 2020–April 2021*
Associate Professor	School of Computer Science Georgia Institute of Technology, Atlanta, GA	*Aug 2019–April 2022*
Adjunct Professor	Computer Science and Engineering SNU, Seoul, South Korea	*Sept 2017–present*
Adjunct Professor	Electrical Engineering KAIST, Daejeon, South Korea	*July 2017–present*
Director	GTS3: System Software and Security Center Georgia Institute of Technology, Atlanta, GA	*Mar 2017–present*
Assistant Professor	School of Computer Science Georgia Institute of Technology, Atlanta, GA	*Aug 2014–Aug 2019*
Visiting Scholar	Computer Science and Engineering University of Washington, Seattle, WA	*Jun 2014–Jul 2014*
Research Intern	Memory R&D Center Samsung Electronics, South Korea	*Jul 2012–Aug 2012*
Co-founder/Programmer	Nerati (now Compass), Cambridge, MA	*Jan 2012–May 2012*
Research Intern	Extreme Computing Group (XCG) Microsoft Research, Redmond, WA	*Jun 2010–Sept 2010*
Republic of Korea Army	Seoul, South Korea	*Jun 2006–Jun 2008*

III. Honors and Awards

1. Best Paper Award in Theoretical Computer and Information Sciences (QSYM, $25k), 07/17/2024
2. DARPA Information Science and Technology (ISAT) Study Group, 08/2021-08/2024
3. Distinguished Artifact Award from SOSP21, 2021
4. Google Research Award, 2019
5. Distinguished Paper Award at USENIX Security'18, 2018
6. DEFKOR00T won DEF CON CTF'18, 2018
7. VMware Early Career Faculty Award ($35k), 2018
8. The Lockheed Martin Inspirational Young Faculty, 2018
9. NSF CAREER Award, 2018
10. 100 Future Technologies and Leaders, The National Academy of Engineering of Korea (NAEK), 2017
11. The Catherine M. and James E. Allchin Early Career Professorship, 2017-2019
12. Mozilla Research Award ($60k), 2017
13. James D. Lester III Family Award, 2017
14. Best Student Paper at EuroSys, 2017
15. The Lockheed Excellence in Teaching Award, 2017

16. CTL/BP Junior Faculty Teaching Excellence Award, 2017
17. Class of 1969 Teaching Fellows Award, 2016
18. Microsoft Azure Research Award ($20k), 2016
19. Best Paper at SDN/NFV workshop (invited for NFV World Congress), 2016
20. Best Applied Security Research Paper (CSAW15), 2015
21. Georgia Power Professor of Excellence ($1,000), 2015
22. Best Paper at APSys15 (invited for OSR), 2015
23. 2015 Internet Defense Prize ($100k), 2015
24. Finalist to DARPA Cyber Grand Challenge ($750k, Disekt), 2015
25. GT-FIRE: Transformative Research and Education Annual Awards ($7,000), 2015
26. Samsung Scholarship ($250k for 5 years), 09/2009–06/2014
27. Korea Presidential Science Scholarship ($40k for 4 years), 03/2003–09/2008
28. Global Leader Scholarship ($10k for 2.5 years), 03/2004–06/2006

IV. Research, Scholarship, and Creative Activities

A. Published Books, Book Chapters, and Edited Volumes

A.1. Books

[1] **Taesoo Kim**, Reverse Engineering and Binary Exploitation (pdf / online), 2019-

[2] **Taesoo Kim**, The Emacs Book, (Korean, online), 2011,

B. Refereed Publications and Submitted Articles

B.1. Thesis

[1] **Ph.D. Thesis**
Title: *Automatic Intrusion Recovery with System-wide History*
Date: June 2014
Advisor: Nickolai Zeldovich
Massachusetts Institute of Technology (MIT)

[2] **S.M. Thesis**
Title: *Making Linux Protection Mechanisms Egalitarian with UserFS.*
Date: June 2011
Advisor: Nickolai Zeldovich
Massachusetts Institute of Technology (MIT)

B.2. Published and Accepted Journal Articles

[1] Hoseok Seol, Minhye Kim, Taesoo Kim, Yongdae Kim, and Lee-Sup Kim. Amnesiac DRAM: A Proactive Defense Mechanism Against Cold Boot Attacks. *IEEE Transactions on Computers (ToC), Vol 70, No 4,* April 2021.

[2] Steffen Maass, Mohan Kumar, Taesoo Kim, Tushar Krishna and Abhishek Bhattacharjee. EcoTLB: Eventually Consistent TLBs. *ACM Transactions on Architecture and Code Optimization (TACO '20),* July 2020.

[3] Seulbae Kim, Meng Xu, Sanidhya Kashyap, Jungyeon Yoon, Wen Xu, and Taesoo Kim. Finding Bugs in File Systems with an Extensible Fuzzing Framework. *ACM Transactions on Storage (ToS), 16(10),* May 2020.

[4] Kangjie Lu, Meng Xu, Chengyu Song, Taesoo Kim, and Wenke Lee. Stopping Memory Disclosures via Diversification and Replicated Execution. *IEEE Transactions on Dependable and Secure Computing (TDSC),* October 2018.

[5] Seongmin Kim, Juhyeng Han, Jaehyeong Ha, Taesoo Kim, and Dongsu Han. SGX-Tor: A Secure and Practical Tor Anonymity Network With SGX Enclaves. *IEEE/ACM Transactions on Networking (ToN), Volumn. 26, No. 5, pp. 2174-2187,* October 2018.

[6] Beumjin Cho, Sangho Lee, Meng Xu, Sangwoo Ji, Taesoo Kim, and Jong Kim. Prevention of Cross-update Privacy Leaks on Android. *Computer Science and Information Systems 15(1),* January 2018.

[7] Meng Xu, Chengyu Song, Yang ji, Ming-Wei Shih, Kangjie Lu, Cong Zheng, Ruian Duan, Yeongjin Jang, Byoungyoung Lee, Chenxiong Qian, Sangho Lee, and Taesoo Kim. Toward Engineering a Secure Android Ecosystem: A Survey of Existing Techniques. *ACM Computing Surveys (CSUR 2016), Volumn 49-2,* August, 2016.

[8] Seungyeop Han, Haichen Shen, Taesoo Kim, Arvind Krishnamurthy, Thomas Anderson, and David Wetherall. MetaSync: Coordinating Storage Across Multiple File Synchronization Services. *IEEE Internet Computing (IEEE IC 2016),* May/June 2016.

[9] Sanidhya Kashyap, Changwoo Min, and Taesoo Kim. Opportunistic Spinlocks: Achieving Virtual Machine Scalability in the Clouds. *ACM SIGOPS Operating Systems Review (OSR), Volumn 50-1,* January 2016.
LWN: qspinlock in Linux

B.3. Conference Presentation with Proceedings (Refereed)

Year	Publication in Top Security and System Conferences							
	Security	CCS	NDSS	S&P	SOSP	OSDI	ATC	EuroSys
2023	3			2				
2022	1					1	2	
2021	1	2	1		1	1		
2020	1	2	1	2				
2019	2			1	4		1	
2018	2	1		1			1	2
2017	4	3	2				3	1
2016	1	2	3	1			2	
2015	1	3	1		1		2	
Pre Gatech	2			1	2	3	1	

The acceptance rate is omitted if not publicly announced; it is typically 10-15% in these conferences.

[1] Scott Constable, Jo Van Bulck, Xiang Cheng, Yuan Xiao, Cedric Xing, Ilya Alexandrovich, Taesoo Kim, Frank Piessens, Mona Vij and Mark Silberstein. AEX-Notify: Thwarting Precise Single-Stepping Attacks through Interrupt Awareness for Intel SGX Enclaves. *In Proceedings of the 31st USENIX Security Symposium (Security 2023),* Anaheim, CA, August 2023.

[2] Sangdon Park, Osbert Bastani and Taesoo Kim. ACon2: Adaptive Conformal Consensus for Provable Blockchain Oracles. *In Proceedings of the 31st USENIX Security Symposium (Security 2023),* Anaheim, CA, August 2023.

[3] Yu-Fu Fu, Jaehyuk Lee and Taesoo Kim. autofz: Automated Fuzzer Composition at Runtime. *In Proceedings of the 31st USENIX Security Symposium (Security 2023),* Anaheim, CA, August 2023.

[4] Soyeon Park, Sangho Lee and Taesoo Kim. Memory Protection Keys: facts, key extension perspectives, and discussions. *IEEE Security & Privacy,* May/June 2023.

[5] Ali Ahad, Chijung Jung, Ammar Askar, Doowon Kim, Taesoo Kim and Yonghwi Kwon. PyFET: Forensically Equivalent Transformation for Python Binary Decompilation. *In Proceedings of the 44th IEEE Symposium on Security and Privacy (S&P 2023),* San Francisco, CA, May 2023.

[6] Bokdeuk Jeong, Joonun Jang, Hayoon Yi, Jiin Moon, Junsik Kim, Intae Jeon, Taesoo Kim, WooChul Shim and Yong Ho Hwang. UTOPIA: Automatic Fuzz Driver Generation using Unit Tests. *In Proceedings of the 44th IEEE Symposium on Security and Privacy (S&P 2023),* San Francisco, CA, May 2023.

[7] Rajat Gupta, Lukas Dresel, Noah Spahn, Giovanni Vigna, Christopher Kruegel and Taesoo Kim. POPKORN: Popping Windows Kernel Drivers At Scale. *In Proceedings of the Annual Computer Security Applications Conference (ACSAC),* Austin, TX, Dec 2022.

[8] Seulbae Kim and Taesoo Kim. RoboFuzz: Fuzzing Robotic Systems over Robot Operating System (ROS) for Finding Correctness Bugs. *In Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE),* Singapore, November 2022.

[9] Juhyeng Han, Insu Yun, Seongmin Kim, Taesoo Kim, Sooel Son and Dongsu Han. Scalable and Secure Virtualization of HSM With ScaleTrust. *IEEE/ACM Transactions on Networking (ToN),* November 2022.

[10] Daehee Jang, Ammar Askar, Insu Yun, Stephen Tong, Yiqin Cai and Taesoo Kim. Fuzzing@Home: Distributed Fuzzing on Untrusted Heterogeneous Clients. *In Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2022),* Limassol, Cyprus, October 2022.

[11] Beom Heyn Kim, Taesoo Kim and David Lie. Modulo: Finding Convergence Failure Bugs in Distributed Systems with Divergence Resync Models. *In Proceedings of the 2022 USENIX Annual Technical Conference (ATC 2022),* Carlsbad, CA, July 2022.

[12] Fan Sang, Ming-Wei Shih, Sangho Lee, Xiaokuan Zhang, Michael Steiner, Mona Vij, and Taesoo Kim. Pridwen: Universally Hardening SGX Programs via Load-Time Synthesis. *In Proceedings of the 2022 USENIX Annual Technical Conference (ATC 2022),* Carlsbad, CA, July 2022.

[13] Sujin Park, Diyu Zhou, Yuchen Qian, Irina Calciu, Taesoo Kim, and Sanidhya Kashyap. Application-Informed Kernel Synchronization Primitives. *In Proceedings of the 16th Symposium on Operating Systems Design and Implementation (OSDI 2022),* Carlsbad, CA, July 2022. (acceptance rate: 19.4% = 49/253)

[14] Mingyu Guan, Anand Padmanabha Iyer and Taesoo Kim. DynaGraph: Dynamic Graph Neural Networks at Scale. *Joint Workshop on Graph Data Management Experiences and Systems and Network Data Analytics (GRADES-NDA),* Philadelphia, PA, June 2022.

[15] Sungbae Yoo, Jinbum Park, Seolheui Kim, Yeji Kim, and Taesoo Kim. In-Kernel Control-Flow Integrity on Commodity OSes using ARM Pointer Authentication. *In Proceedings of the 31st USENIX Security Symposium (Security 2022),* Boston, MA, August 2022.

[16] Hyungjoon Koo, Soyeon Park, and Taesoo Kim. A Look Back on a Function Identification Problem. *In Proceedings of the Annual Computer Security Applications Conference (ACSAC),* Virtual, December 2021. (acceptance rate: 17.2% = 56/326)

[17] Ren Ding, Yonghae Kim, Fan Sang, Wen Xu, Gururaj Saileshwar and Taesoo Kim. Hardware Support to Improve Fuzzing Performance and Precision. *In Proceedings of the 28th ACM Conference on Computer and Communications Security (CCS 2021),* Seoul, South Korea, November 2021.

[18] Insu Yun, Woosun Song, Seunggi Min, and Taesoo Kim. HARDSHEAP: An Universal and Extensible Framework for Evaluating Secure Allocators. *In Proceedings of the 28th ACM Conference on Computer and Communications Security (CCS 2021),* Seoul, South Korea, November 2021.

[19] Yechan Bae, Youngsuk Kim, Ammar Askar, Jungwon Lim and Taesoo Kim. Rudra: Finding Memory Safety Bugs in Rust at the Ecosystem Scale. *In Proceedings of the 28th ACM Symposium on Operating Systems Principles (SOSP 2021),* Virtual, October 2021. (acceptance rate: 15.5% = 54/348)
Distinguished Artifact Award

[20] Brian Wickman, Hong Hu, Insu Yun, Daehee Jang, JungWon Lim, Sanidhya Kashyap and Taesoo Kim. Preventing Use-After-Free Attacks with Fast Forward Allocation. *In Proceedings of the 30th USENIX Security Symposium (Security 2021),* August, 2021.

[21] Youngseok Yang, Taesoo Kim, and Byung-Gon Chun. Finding Consensus Bugs in Ethereum via Multi-transaction Differential Fuzzing. *In Proceedings of the 15th Symposium on Operating Systems Design and Implementation (OSDI 2021),* Virtual, July 2021. (acceptance rate: 18.8% = 31/165)
Coindesk, Yahoo Fiance

[22] Sujin Park, Irina Calciu, Taesoo Kim and Sanidhya Kashyap. Contextual Concurrency Control. *18th USENIX Workshop on Hot Topics in Operating Systems (HotOS XVIII),* Virtual, May 2021.

[23] Jinho Jung, Stephen Tong, Hong Hu, Jungwon Lim, Yonghwi Jin, and Taesoo Kim. WINNIE: Fuzzing Windows Applications with Harness Synthesis and Fast Cloning. *In Proceedings of the 2021 Network and Distributed System Security Symposium (NDSS 2021),* San Diego, CA, February 2021.

[24] Hyungjoon Koo, Soyeon Park, and Taesoo Kim. Revisiting Function Identification with Machine Learning. *In Proceedings of the 1st Machine Learning for Program Aanalysis (MLPA),* Yokohama, Japan, January 2021.

[25] Wen Xu, Soyeon Park, and Taesoo Kim. FREEDOM: Engineering a State-of-the-Art DOM Fuzzer. *In Proceedings of the 27th ACM Conference on Computer and Communications Security (CCS 2020),* Orlando, FL, November 2020. (acceptance rate: 16.9% = 121/715)
CVE-2019-6212, CVE-2019-8596, CVE-2019-8609, CVE-2019-8720, CVE-2020-9803, CVE-2020-9806, CVE-2020-9807, CVE-2020-9895, CVE-2019-5806, CVE-2019-5817

[26] Chenxiong Qian, Hyungjoon Koo, Changseok Oh, Taesoo Kim and Wenke Lee. Slimium: Debloating the Chromium Browser with Feature Subsetting. *In Proceedings of the 27th ACM Conference on Computer and Communications Security (CCS 2020),* Orlando, FL, November 2020. (acceptance rate: 16.9% = 121/715)

[27] Jinho Jung, Hong Hu, Joy Arulraj, Taesoo Kim, and Woonhak Kang. APOLLO: Automatic Detection and Diagnosis of Performance Regressions in Database Systems. *In Proceedings of the 46th International Conference on Very Large Data Bases (VLDB 2020),* Tokyo, Japan, August 2020. (acceptance rate: 24.8%)

[28] Insu Yun, Dhaval Kapil, and Taesoo Kim. Automatic Techniques to Systematically Discover New Heap Exploitation Primitives. *In Proceedings of the 29th USENIX Security Symposium (Security 2020),* Boston, MA, August 2020.

[29] Meng Xu, Sanidhya Kashyap, Hanqing Zhao and Taesoo Kim. KRACE: Data Race Fuzzing for Kernel File Systems. *In Proceedings of the 41st IEEE Symposium on Security and Privacy (S&P 2020),* San Francisco, CA, May 2020.

[30] Soyeon Park, Wen Xu, Insu Yun, Daehee Jang and Taesoo Kim. Fuzzing JavaScript Engines with Aspect-preserving Mutation. *In Proceedings of the 41st IEEE Symposium on Security and Privacy (S&P 2020),* San Francisco, CA, May 2020.
CVE-2020-6382, CVE-2019-13730, CVE-2019-13764, CVE-2019-8811, CVE-2019-8816, ... (12 CVEs)

[31] Ren Ding, Hong Hu, Wen Xu, and Taesoo Kim. DESENSITIZATION: Privacy-Aware and Attack-Preserving Crash Report. *In Proceedings of the 2020 Network and Distributed System Security Symposium (NDSS 2020),* San Diego, CA, February 2020.

[32] Nilaksh Das, Siwei Li, Chanil Jeon, Jinho Jung, Shang-Tse Chen, Carter Yagemann, Evan Downing, Haekyu Park, Evan Yang, Li Chen, Michael Kounavis, Ravi Sahita, David Durham, Scott Buck, Polo Chau, Taesoo Kim and Wenke Lee. MLsploit: A Framework for Interactive Experimentation with Adversarial Machine Learning Research. *In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD 2019, Project Showcase),* Anchorage, AK, August 2019.
BlackHat Asia/Arsenal

[33] Seulbae Kim, Meng Xu, Sanidhya Kashyap, Jungyeon Yoon, Wen Xu, and Taesoo Kim. Finding Semantic Bugs in File Systems with an Extensible Fuzzing Framework. *In Proceedings of the 27th ACM Symposium on Operating Systems Principles (SOSP 2019),* Ontario, Canada, October 2019. (acceptance rate: 13.8% = 38/276)

[34] Sanidhya Kashyap, Irina Calciu, Xiaohe Cheng, Changwoo Min, and Taesoo Kim. Scalable and Practical Locking With Shuffling. *In Proceedings of the 27th ACM Symposium on Operating Systems Principles (SOSP 2019),* Ontario, Canada, October 2019. (acceptance rate: 13.8% = 38/276)

[35] Se Kwon Lee, Jayashree Mohan, Sanidhya Kashyap, Taesoo Kim, and Vijay Chidambaram. RECIPE: Converting Concurrent DRAM Indexes to Persistent-Memory Indexes. *In Proceedings of the 27th ACM Symposium on Operating Systems Principles (SOSP 2019),* Ontario, Canada, October 2019. (acceptance rate: 13.8% = 38/276)

[36] Rohan Kadekodi, Se Kwon Lee, Sanidhya Kashyap, Taesoo Kim, Aasheesh Kolli, and Vijay Chidambaram. SplitFS: Reducing Software Overhead in File Systems for Persistent Memory. *In Proceedings of the 27th ACM Symposium on Operating Systems Principles (SOSP 2019),* Ontario, Canada, October 2019. (acceptance rate: 13.8% = 38/276)

[37] Juhyeng Han, Seongmin Kim, Taesoo Kim, and Dongsu Han. Toward Scaling Hardware Security Module for Emerging Cloud Services. *In Proceedings of the 4th Workshop on System Software for Trusted Execution (SysTEX 2019),* Ontario, Canada, October 2019.

[38] Hanqing Zhao, Yanyu Zhang, Kun Yang, and Taesoo Kim. Breaking Turtles All the Way Down: An Exploitation Chain to Break out of VMware ESXi. *In Proceedings of the 13th USENIX Workshop on Offensive Technologies (WOOT),* Santa Clara, CA, August 2019.
CVE-2018-6981, CVE-2018-6982

[39] Chenxiong Qian, Hong Hu, Mansour A Alharthi, Pak Ho Chung, Taesoo Kim, and Wenke Lee. RAZOR: A Framework for Post-deployment Software Debloating. *In Proceedings of the 28th USENIX Security Symposium (Security 2019),* Santa Clara, CA, August 2019.

[40] Jinho Jung, Hong Hu, David Solodukhin, Daniel Pagan, Kyu Hyung Lee, and Taesoo Kim. Fuzzification: Anti-Fuzzing Techniques. *In Proceedings of the 28th USENIX Security Symposium (Security 2019),* Santa Clara, CA, August 2019.
Hacker News

[41] Soyeon Park, Sangho Lee, Wen Xu, Hyungon Moon, and Taesoo Kim. libmpk: Software Abstraction for Intel Memory Protection Keys (Intel MPK). *In Proceedings of the 2019 USENIX Annual Technical Conference (ATC 2019),* Renton, WA, July 2019. (acceptance rate: 19.9% = 71/356)

[42] Wen Xu, Hyungon Moon, Sanidhya Kashyap, Po-Ning Tseng, and Taesoo Kim. Fuzzing File Systems via Two-Dimensional Input Space Exploration. *In Proceedings of the 40th IEEE Symposium on Security and Privacy (S&P 2019),* San Francisco, CA, May 2019.
CVE-2018-1092, CVE-2018-1093, CVE-2018-1094, CVE-2018-1095, CVE-2018-10840, CVE-2018-10876, CVE-2018-10877, CVE-2018-10878, CVE-2018-10879, CVE-2018-10880, CVE-2018-10881, CVE-2018-10882, CVE-2018-10883, ... (32 CVEs)

[43] Hong Hu, Chenxiong Qian, Carter Yagemann, Simon P. Chung, Bill Harris, Taesoo Kim, and Wenke Lee. Enforcing Unique Code Target Property for Control-Flow Integrity. *In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS 2018),* Toronto, Canada, October 2018. (acceptance rate: 16.6% = 134/809)

[44] Insu Yun, Sangho Lee, Meng Xu, Yeongjin Jang, and Taesoo Kim. QSYM: A Practical Concolic Execution Engine Tailored for Hybrid Fuzzing. *In Proceedings of the 27th USENIX Security Symposium (Security 2018),* Baltimore, MD, August 2018. (acceptance rate: 19.1% = 100/524)
Distinguished Paper Award
CVE-2017-6836, CVE-2017-8891, CVE-2017-12878, CVE-2017-17080, CVE-2017-17081, ...

[45] Yang Ji, Sangho Lee, Mattia Fazzini, Joey Allen, Evan Downing, Taesoo Kim, Alessandro Orso, and Wenke Lee. Efficient Data Flow Tagging and Tracking for Refinable Cross-host Attack Investigation. *In Proceedings of the 27th USENIX Security Symposium (Security 2018),* Baltimore, MD, August 2018. (acceptance rate: 19.1% = 100/524)

[46] Sanidhya Kashyap, Changwoo Min, and Taesoo Kim. Scaling Guest OS Critical Sections with eCS. *In Proceedings of the 2018 USENIX Annual Technical Conference (ATC 2018),* Boston, MA, July 2018. (acceptance rate: 20.1% = 76/378)

[47] Meng Xu, Chenxiong Qian, Kangjie Lu, Michael Backes, and Taesoo Kim. Precise and Scalable Detection of Double-Fetch Bugs in OS Kernels. *In Proceedings of the 39th IEEE Symposium on Security and Privacy (S&P 2018),* San Francisco, CA, May 2018. (acceptance rate: 11.5% = 63/549)
CVE-2017-15037

[48] Sanidhya Kashyap, Changwoo Min, Kangnyeon Kim, and Taesoo Kim. A Scalable Ordering Primitive for Multicore Machines. *In Proceedings of the 13rd ACM European Conference on Computer Systems (EuroSys 2018),* Porto, Portugal, April, 2018. (acceptance rate: 16.4% = 43/262)

[49] Changwoo Min, Woon-Hak Kang, Mohan Kumar Sanidhya Kashyap, Steffen Maass, Heeseung Jo, and Taesoo Kim. SOLROS: A Data-Centric Operating System Architecture for Heterogeneous Computing. *In Proceedings of the 13rd ACM European Conference on Computer Systems (EuroSys 2018),* Porto, Portugal, April, 2018. (acceptance rate: 16.4% = 43/262)

[50] Mohan Kumar, Steffen Maass, Sanidhya Kashyap, Jan Vesely, Zi Yan, Taesoo Kim, Abhishek Bhattacharjee, and Tushar Krishna. LATR: Lazy Translation Coherence. *In Proceedings of the 23rd ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2018),* Williamsburg, VA, March, 2018. (acceptance rate: 17.6% = 56/319)

[51] Wen Xu, Sanidhya Kashyap, Changwoo Min, and Taesoo Kim. Designing New Operating Primitives to Improve Fuzzing Performance. *In Proceedings of the 23th ACM Conference on Computer and Communications Security (CCS 2017),* Dallas, TX, October 2017. (acceptance rate: 18.1% = 151/836)
Mozilla Research

[52] Yang Ji, Sangho Lee, Evan Downing, Weiren Wang, Mattia Fazzini, Taesoo Kim, Alex Orso, and Wenke Lee. RAIN: Refinable Attack Investigation with On-demand Inter-Process Information Flow Tracking. *In Proceedings of the 23th ACM Conference on Computer and Communications Security (CCS 2017),* Dallas, TX, October 2017. (acceptance rate: 18.1% = 151/836)
GT News Horizons

[53] Ruian Duan, Ashish Bijlani, Meng Xu, Taesoo Kim, and Wenke Lee. Checking Open-Source License Violation and 1-day Security Risk at Large Scale. *In Proceedings of the 23th ACM Conference on Computer and Communications Security (CCS 2017),* Dallas, TX, October 2017. (acceptance rate: 18.1% = 151/836)

[54] Yeongjin Jang, Jaehyuk Lee, Sangho Lee, and Taesoo Kim. SGX-Bomb: Locking Down the Processor via Rowhammer Attack. *In Proceedings of the 2nd Workshop on System Software for Trusted Execution (SysTEX 2017),* Shanghai, China, October 2017.
Hacker News

[55] Heeseung Jo, Woonhak Kang, Changwoo Min, and Taesoo Kim. FLSCHED: A Lockless and Lightweight Approach to OS Scheduler for Xeon Phi. *In Proceedings of the 8th Asia-Pacific Workshop on Systems (APSys 2017),* Mumbai, India, September 2017.

[56] Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado. Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing. *In Proceedings of the 26th USENIX Security Symposium (Security 2017),* Vancouver, Canada, August 2017. (acceptance rate: 16.3% = 85/522)
Intel SGX Research

[57] Jaehyuk Lee, Jinsoo Jang, Yeongjin Jang, Nohyun Kwak, Yeseul Choi, Changho Choi, Taesoo Kim, Marcus Peinado, and Brent B. Kang. Hacking in Darkness: Return-oriented Programming against Secure Enclaves. *In Proceedings of the 26th USENIX Security Symposium (Security 2017),* Vancouver, Canada, August 2017. (acceptance rate: 16.3% = 85/522)
Intel SGX Research

[58] Ren Ding, Chenxiong Qian, Chengyu Song, Bill Harris, Taesoo Kim, and Wenke Lee. Efficient Protection of Path-Sensitive Control Security. *In Proceedings of the 26th USENIX Security Symposium (Security 2017),* Vancouver, Canada, August 2017. (acceptance rate: 16.3% = 85/522)

[59] Meng Xu and Taesoo Kim. PlatPal: Detecting Malicious Documents with Platform Diversity. *In Proceedings of the 26th USENIX Security Symposium (Security 2017),* Vancouver, Canada, August 2017. (acceptance rate: 16.3% = 85/522)

[60] Sanidhya Kashyap, Changwoo Min, and Taesoo Kim. Scalable NUMA-aware Blocking Synchronization Primitives. *In Proceedings of the 2017 USENIX Annual Technical Conference (ATC 2017),* Santa Clara, CA, July 2017. (acceptance rate: 21.2% = 60/283)

[61] Su Yong Kim, Sangho Lee, Insu Yun, Wen Xu, Byoungyoung Lee, Youngtae Yun, and Taesoo Kim. CAB-Fuzz: Practical Concolic Testing Techniques for COTS Operating Systems. *In Proceedings of the 2017 USENIX Annual Technical Conference (ATC 2017),* Santa Clara, CA, July 2017. (acceptance rate: 21.2% = 60/283)
CVE-2015-6098, CVE-2016-0040, CVE-2016-7219

[62] Meng Xu, Kangjie Lu, Taesoo Kim, and Wenke Lee. Bunshin: Compositing Security Mechanisms through Diversification. *In Proceedings of the 2017 USENIX Annual Technical Conference (ATC 2017),* Santa Clara, CA, July 2017. (acceptance rate: 21.2% = 60/283)

[63] Steffen Maass, Changwoo Min, Sanidhya Kashyap, Woonhak Kang, Mohan Kumar, and Taesoo Kim. Mosaic: Processing a Trillion-Edge Graph on a Single Machine. *In Proceedings of the 12st ACM European Conference on Computer Systems (EuroSys 2017),* Belgrade, Serbia, April, 2017. (acceptance rate: 20.5% = 41/200)
Best Student Paper Award
The Next Platform, Hacker News 1/2, GT News, The morning paper

[64] Seongmin Kim, Juhyeng Han, Jaehyeong Ha, Taesoo Kim, and Dongsu Han. Enhancing Security and Privacy of Tor's Ecosystem by using Trusted Execution Environments. *In Proceedings of the 14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 2017),* Boston, MA, March 2017. (acceptance rate: 18.2% = 46/253)
Intel SGX Research

[65] Jaebaek Seo, Byoungyoung Lee, Sungmin Kim, Ming-Wei Shih, Insik Shin, Dongsu Han, and Taesoo Kim. SGX-Shield: Enabling Address Space Layout Randomization for SGX Programs. *In Proceedings of the 2017 Network and Distributed System Security Symposium (NDSS 2017),* San Diego, CA, February 2017. (acceptance rate: 16.1% = 68/423)
Intel SGX Research

[66] Ming-Wei Shih, Sangho Lee, Taesoo Kim, and Marcus Peinado. T-SGX: Eradicating Controlled-Channel Attacks Against Enclave Programs. *In Proceedings of the 2017 Network and Distributed System Security Symposium (NDSS 2017),* San Diego, CA, February 2017. (acceptance rate: 16.1% = 68/423)
Intel SGX Research

[67] Ketan Bhardwaj, Ming-Wei Shih, Pragya Agarwal, Ada Gavrilovska, Taesoo Kim, and Karsten Schwan. Fast, Scalable and Secure Onloading of Edge Functions using AirBox. *In Proceedings of the 1st IEEE/ACM Symposium on Edge Computing (SEC 2017),* Washington, DC, October 2016.
Patent: WO2018026841A1

[68] Kangjie Lu, Chengyu Song, Taesoo Kim, and Wenke Lee. UniSan: Proactive Kernel Memory Initialization to Eliminate Data Leakages. *In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS 2016),* Vienna, Austria, October 2016. (acceptance rate: 16.5% = 137/831)
CVE-2016-5243, CVE-2016-5244, CVE-2016-4569, CVE-2016-4578, CVE-2016-4569, CVE-2016-4485, CVE-2016-4486, CVE-2016-4482, AndroidID-28620568, AndroidID-28619338, AndroidID-28620324, AndroidID-28673002, AndroidID-28672819, AndroidID-28672560, AndroidID-28616963, ...

[69] Yeongjin Jang, Sangho Lee, and Taesoo Kim. Breaking Kernel Address Space Layout Randomization with Intel TSX. *In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS 2016),* Vienna, Austria, October 2016. (acceptance rate: 16.5% = 137/831)
Hacker News, LWN, Attacking Windows 10 by IOActive, Google Project Zero, Microsoft

[70] Alexandra Boldyreva, Taesoo Kim, Richard J. Lipton, and Bogdan Warinschi. Provably-Secure Remote Memory Attestation for Heap Overflow Protection. *In Proceedings of the 10th Conference on Security and Cryptography for Networks (SCN 2016),* Amalfi, Italy, August, 2016.

[71] Insu Yun, Changwoo Min, Xujie Si, Yeongjin Jang, Taesoo Kim, and Mayur Naik. APISan: Sanitizing API Usages through Semantic Cross-checking. *In Proceedings of the 25th USENIX Security Symposium (Security 2016),* Austin, TX, August, 2016. (acceptance rate: 15.6% = 72/463)
Top 10 Finalists, CSAW16
TGC/News, CVE-2016-5636

[72] Changwoo Min, Sanidhya Kashyap, Steffen Maass, Woonhak Kang, and Taesoo Kim. Understanding Manycore Scalability of File Systems. *In Proceedings of the 2016 USENIX Annual Technical Conference (ATC 2016),* Denver, CO, June 2016. (acceptance rate: 19.0% = 47/248)

[73] Sanidhya Kashyap, Changwoo Min, Byoungyoung Lee, Taesoo Kim, and Pavel Emelyanov. Instant OS Updates via Userspace Checkpoint-and-Restart. *In Proceedings of the 2016 USENIX Annual Technical Conference (ATC 2016),* Denver, CO, June 2016. (acceptance rate: 19.0% = 47/248)
Linux Plumbers Conference 2015, CRIU

[74] Chengyu Song, Hyungon Moon, Monjur Alam, Insu Yun, Byoungyoung Lee, Taesoo Kim, Wenke Lee, and Yunheung Paek. HDFI: Hardware-Assisted Data-flow Isolation. *In Proceedings of the 37th IEEE Symposium on Security and Privacy (S&P 2016),* San Jose, CA, May 2016. (acceptance rate: 13.3% = 55/413)

[75] Ming-Wei Shih, Mohan Kumar, Taesoo Kim, Ada Gavrilovska. S-NFV: Securing NFV States by using SGX. *In Proceedings of the 1st ACM International Workshop on Security in SDN and NFV,* New Orleans, LA, March 2016.
Best paper, invited to present at the NFV World Congress
Intel SGX Research

[76] Prerit Jain, Soham Desai, Seongmin Kim, Ming-Wei Shih, JaeHyuk Lee, Changho Choi, Youjung Shin, Taesoo Kim, Brent B. Kang and Dongsu Han. OpenSGX: An Open Platform for SGX Research. *In Proceedings of the 2016 Network and Distributed System Security Symposium (NDSS 2016),* San Diego, CA, February 2016. (acceptance rate: 15.4% = 60/389)
Wikipedia: Software Guard Extensions, Intel SGX Research

[77] Chengyu Song, Byoungyoung Lee, Kangjie Lu, William R. Harris, Taesoo Kim and Wenke Lee. Enforcing Kernel Security Invariants with Data Flow Integrity. *In Proceedings of the 2016 Network and Distributed System Security Symposium (NDSS 2016),* San Diego, CA, February 2016. (acceptance rate: 15.4% = 60/389)

[78] Jaebaek Seo, Daehyeok Kim, Donghyun Cho, Taesoo Kim and Insik Shin. FlexDroid: Enforcing In-App Privilege Separation in Android. *In Proceedings of the 2016 Network and Distributed System Security Symposium (NDSS 2016),* San Diego, CA, February 2016. (acceptance rate: 15.4% = 60/389)

[79] Seongmin Kim, Youjung Shin, Jaehyung Ha, Taesoo Kim, and Dongsu Han. A First Step Towards Leveraging Commodity Trusted Execution Environments for Network Applications. *In Proceedings of the 14th ACM Workshop on Hot Topics in Networks (HotNets 2015),* Philadelphia, PA, November 2015. (acceptance rate: 18.6% = 26/140)

[80] Meng Xu, Yeongjin Jang, Xinyu Xing, Taesoo Kim, and Wenke Lee. UCognito: Private Browsing without Tears. *In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS 2015),* Denver, CO, October 2015. (acceptance rate: 19.8% = 128/646)
Observer Innovation

[81] Kangjie Lu, Chengyu Song, Byoungyoung Lee, Simon P. Chung, Taesoo Kim, and Wenke Lee. ASLR-Guard: Stopping Address Space Leakage for Code Reuse Attacks. *In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS 2015),* Denver, CO, October 2015. (acceptance rate: 19.8% = 128/646)
Dagstuhl Seminar

[82] Hongil Kim, Dongkwan Kim, Minhee Kwon, Hyungseok Han, Yeongjin Jang, Dongsu Han, Taesoo Kim, and Yongdae Kim. Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations. *In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS 2015),* Denver, CO, October 2015. (acceptance rate: 19.8% = 128/646)
Android Security, CERT, Networkworld, Softpedia, pocketnow, VoIPshield, VU#943167, CVE-2015-6614

[83] Changwoo Min, Sanidhya Kashyap, Byoungyoung Lee, Chengyu Song, and Taesoo Kim. Cross-checking Semantic Correctness: The Case of Finding File System Bugs. *In Proceedings of the 25th ACM Symposium on Operating Systems Principles (SOSP 2015),* Monterey, CA, October 2015. (acceptance rate: 16.1% = 30/186)
Bug Report

[84] Byoungyoung Lee, Chengyu Song, Taesoo Kim, and Wenke Lee. Type Casting Verification: Stopping an Emerging Attack Vector. *In Proceedings of the 24th USENIX Security Symposium (Security 2015),* Washington, DC, August 2015. (acceptance rate: 15.7% = 67/426)
2015 Internet Defense Prize ($100k Prize)
Top 10 Finalists, CSAW15
Internet Defense Prize, USENIX Update, Facebook, ZDNet, We Live Security, Science 2.0, hys.org, Scientific Computing, IT Pro Portal, Laboratory Equipment, Gizbot, Science Codex, Business Standard, ECN magazine, The Times of India, CanIndia News, New Indian Express, InfoSec, Social Times, The Register, CTV News, Threat Post, TNW News, The Security Ledger, Georgia Tech News Center, ScienceDaily, Milton Security, ACM TECHNEWS, Gadget 360, SC Magazine, IHS Engineering 360, CVE-2014-1594, . . .

[85] Sanidhya Kashyap, Changwoo Min, and Taesoo Kim. Scalability in the Clouds! A Myth or Reality? *In Proceedings of the 6th Asia-Pacific Workshop on Systems (APSys 2015),* Tokyo, Japan, July 2015. (acceptance rate: 29.4% = 20/68)
Best paper, nominated to Operating Systems Review (OSR)
LWN: qspinlock in Linux

[86] Changwoo Min, Woon-Hak Kang, Taesoo Kim, Sang-Won Lee, and Young Ik Eom. Lightweight Application-Level Crash Consistency on Transactional Flash Storage. *In Proceedings of the 2015 USENIX Annual Technical Conference (ATC 2015),* Santa Clara, CA, July 2015. (acceptance rate: 15.8% = 35/221)

[87] Seungyeop Han, Haichen Shen, Taesoo Kim, Arvind Krishnamurthy, Thomas Anderson, and David Wetherall. MetaSync: File Synchronization Across Multiple Untrusted Storage Services. *In Proceedings of the 2015 USENIX Annual Technical Conference (ATC 2015),* Santa Clara, CA, July 2015. (acceptance rate: 15.8% = 35/221)

[88] Byoungyoung Lee, Chengyu Song, Yeongjin Jang, Tielei Wang, Taesoo Kim, Long Lu, and Wenke Lee. Preventing Use-after-free with Dangling Pointers Nullification. *In Proceedings of the 2015 Network and Distributed System Security Symposium (NDSS 2015),* San Diego, CA, February 2015. (acceptance rate: 16.9% = 51/302)
Best Applied Security Research Paper (CSAW15)

[89] Amir Yazdanbakhsh, Gennady Pekhimenko, Bradley Thwaites, Hadi Esmaeilzadeh, Taesoo Kim, Onur Mutlu, and Todd C Mowry. RFVP: Rollback-Free Value Prediction with Safe-to-Approximate Loads. *SCS Technical Report GT-CS-15-01, Georgia Institute of Technology,* Atlanta, GA, January 2015.

[90] Haogang Chen, Taesoo Kim, Xi Wang, M. Frans Kaashoek, and Nickolai Zeldovich. Identifying Information Disclosure in Web Applications with Retroactive Auditing. *In Proceedings of the 11th Symposium on Operating Systems Design and Implementation (OSDI 2014),* Broomfield, CO, October 2014. (acceptance rate: 18.4% = 42/228)

[91] Seungyeop Han, Haichen Shen, Taesoon Kim, Arvind Krishnamurthy, Thomas Anderson, and David Wetherall. MetaSync: File Synchronization Across Multiple Untrusted Storage Services. *Technical Report UW-CSE-14-05-02, University of Washington Computer Science and Engineering,* Seattle, WA, May 2014.

[92] Byoungyoung Lee, Long Lu, Tielei Wang, Taesoo Kim, and Wenke Lee. From Zygote to Morula: Fortifying Weakened ASLR on Android. *In Proceedings of the 35th IEEE Symposium on Security and Privacy (S&P 2014),* San Jose, CA, May 2014. (acceptance rate: 13.2% = 44/334)
LWN, Copperhead

[93] Ramesh Chandra, Taesoo Kim, and Nickolai Zeldovich. Asynchronous Intrusion Recovery for Interconnected Web Services. *In Proceedings of the 24th ACM Symposium on Operating Systems Principles (SOSP 2013),* Farmington, PA, November 2013. (acceptance rate: 18.8% = 30/160)

[94] Taesoo Kim, Ramesh Chandra, and Nickolai Zeldovich. Optimizing Unit Test Execution in Large Software Programs using Dependency Analysis. *In Proceedings of the 4th Asia-Pacific Workshop on Systems (APSys 2013),* Singapore, July 2013. (acceptance rate: 27.4% = 20/73)

[95] Haogang Chen, Cody Cutler, Taesoo Kim, Yandong Mao, Xi Wang, Nickolai Zeldovich, and M. Frans Kaashoek. Security Bugs in Embedded Interpreters. *In Proceedings of the 4th Asia-Pacific Workshop on Systems (APSys 2013),* Singapore, July 2013. (acceptance rate: 27.4% = 20/73)

[96] Taesoo Kim and Nickolai Zeldovich. Practical and Effective Sandboxing for Non-root Users. *In Proceedings of the 2013 USENIX Annual Technical Conference (ATC 2013),* San Jose, CA, June 2013. (acceptance rate: 14.2% = 33/233)
Hacker News, Wikipedia: seccomp, Coders Grid, AlternativeTo, TorProject

[97] Taesoo Kim, Ramesh Chandra, and Nickolai Zeldovich. Efficient Patch-based Auditing for Web Application Vulnerabilities. *In Proceedings of the 10th Symposium on Operating Systems Design and Implementation (OSDI 2012),* Hollywood, CA, October 2012. (acceptance rate: 11.6% = 25/215)

[98] Taesoo Kim, Marcus Peinado, and Gloria Mainar-Ruiz. System-Level Protection Against Cache-based Side Channel Attacks in the Cloud. *In Proceedings of the 21st USENIX Security Symposium (Security 2012),* Bellevue, WA, August 2012. (acceptance rate: 19.4% = 43/222)

[99] Taesoo Kim, Ramesh Chandra, and Nickolai Zeldovich. Recovering from Intrusions in Distributed Systems with Dare. *In Proceedings of the 3rd Asia-Pacific Workshop on Systems (APSys 2012),* Seoul, South Korea, July 2012. (acceptance rate: 35.6% = 16/45)

[100] Ramesh Chandra, Taesoo Kim, Meelap Shah, Neha Narula, and Nickolai Zeldovich. Intrusion Recovery for Database-backed Web Applications. *In Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP 2011),* Cascais, Portugal, October 2011. (acceptance rate: 18.3% = 28/153)

[101] Taesoo Kim, Xi Wang, Nickolai Zeldovich, and M. Frans Kaashoek. Intrusion Recovery using Selective Re-execution. *In Proceedings of the 9th Symposium on Operating Systems Design and Implementation (OSDI 2010),* Vancouver, Canada, October 2010. (acceptance rate: 16.1% = 32/199)
Network World

[102] Taesoo Kim and Nickolai Zeldovich. Making Linux Protection Mechanisms Egalitarian with UserFS. *In Proceedings of the 19th USENIX Security Symposium (Security 2010),* Washington, DC, August 2010. (acceptance rate: 14.9% = 30/202)

[103] Taesoo Kim and Sungho Jo. Simulation of Human Locomotion using a Musculoskeletal Model. *International Conference on Control, Automation and Systems,* Seoul, South Korea, October 2008.

B.4. Other Refereed Material

[1] Yonghwi Jin, Jungwon Lim, Insu Yun, and Taesoo Kim. Compromising the macOS kernel through Safari by chaining six vulnerabilities. *BlackHat USA 2020,* Las Vegas, NV, August 2020.
Pwn2Own, CVE-2020-9850, CVE-2020-9839, CVE-2020-9856, CVE-2020-9801

[2] Jinho Jung, Chanil Jeon, Max Wolotsky, Insu Yun, and Taesoo Kim. AVPASS: Leaking and Bypassing Antivirus Detection Model Automatically. *BlackHat USA 2017,* Las Vegas, NV, August 2017.
DARK Reading 1/2/3, WIRED

[3] Yeongjin Jang, Sangho Lee, and Taesoo Kim. Breaking Kernel Address Space Layout Randomization (KASLR) with Intel TSX. *BlackHat USA 2016,* Las Vegas, NV, August 2016.
Hacker News, LWN, Attacking Windows 10 by IOActive, Google Project Zero, Microsoft

[4] Byoungyoung Lee, Yeongjin Jang, Tielei Wang, Chengyu Song, Long Lu, Taesoo Kim, and Wenke Lee. Abusing Performance Optimization Weaknesses to Bypass ASLR. *BlackHat USA 2014,* Las Vegas, NV, August 2014.
Phrack, ISS Source, IT Researches, Embedded

C. Other Publications and Creative Products

C.1. Patents

[1] Yang Ji, Joey Allen, Evan Downing, Mattia Fazzini, Taesoo Kim, Sangho Lee, Wenke Lee, and Alex Orso, **Enabling Cross-Host Refinable Attack Investigation with Efficient Data flow Tagging and Tracking** (patent pending).

[2] Ruian Duan, Ashish Bijlani, Taesoo Kim, and Wenke Lee, **Devices, Systems, And Methods Of Program Identification, Isolation, And Profile Attachment**, US20200065074A1.

[3] Marcus Peinado and Taesoo Kim, **System and Method for Providing Stealth Memory**, US20120159103.

[4] Ketan Bhardwaj, Ada Gavrilovska and Taesoo Kim, **Methods and systems for providing secure mobile edge computing ecosystems**, WO2018026841A1.

C.2. Hardware and Software Artifacts

All of our software artifacts from research are publicly available on GitHub and GTS3. Some of them include:

[1] **QSYM**, A practical concolic execution engine tailored for hybrid fuzzing, 08/2018
`https://github.com/sslab-gatech/qsym`.

[2] **AVPass**, A tool for leaking and bypassing Android malware detection system, 07/2017
`https://github.com/sslab-gatech/avpass`.

[3] **Mosaic**, A trillion-edge graph processing engine, 06/2017
`https://github.com/sslab-gatech/mosaic`.

[4] **HDFI**, Hardware-assisted data-flow isolation, 06/2017
`https://github.com/sslab-gatech/hdfi`.

[5] **T-SGX**, A compiler-based tool that protects Intel SGX applications against controlled-channel attacks, 03/2017
`https://github.com/sslab-gatech/t-sgx`.

[6] **CST-Lock**, A scalable blocking synchronization mechanism, 05/2017
`https://github.com/sslab-gatech/cst-locks`.

[7] **Unisan**, A tool to eliminate data leakages via uninitialization vulnerabilities, 12/2016
`https://github.com/sslab-gatech/unisan`.

[8] **DrK**, A PoC to attack KASLR via TSX, 12/2016
`https://github.com/sslab-gatech/DrK`.

[9] **fakeroot-p**, A scalable implementation of fakeroot, 06/2016
`https://github.com/sslab-gatech/fakeroot-p`.

[10] **SGX-Shield**, A tool to enable ASLR for SGX programs, 07/2016
`https://github.com/jaebaek/SGX-Shield`.

[11] **FxMark**, Benchmark to measure filesystem multicore scalability, 06/2016
`https://github.com/sslab-gatech/fxmark`.

[12] **Kenali**, A modified Linux kernel for Nexus 9, 03/2016
`https://github.com/sslab-gatech/kenali-kernel`.

[13] **ASLR-Guard**, A compiler to enhance the security of the ASLR mechanism, 02/2016
`https://github.com/sslab-gatech/kenali-kernel`.

[14] **Juxta**, A tool to find filesystem-specific semantic bugs, 12/2015
`https://github.com/sslab-gatech/juxta`.

[15] **Ucognito**, Universal private browsing, 10/2015
`https://github.com/sslab-gatech/ucognito`.

[16] **CaVer**, A bad-casting verifier, 10/2015
`https://github.com/sslab-gatech/caver`.

[17] **OpenSGX**, A QEMU Emulator for SGX instructions, 01/2016
`https://github.com/sslab-gatech/opensgx`.

[18] **Die**, A latex paper template, 09/2014
`https://github.com/tsgates/die`.

[19] **Rust.ko**, A minimal Linux kernel module written in rust, 09/2014
`https://github.com/tsgates/rust.ko`.

[20] **MBox**, A sandbox tool for Linux by interpositioning on system calls, for non-root users, 12/2012
`https://github.com/tsgates/mbox`.

[21] **lab-submit**, Course labs/HW submission system used for MIT 6.824/6.858/6.888/6.932, 09/2012.

[22] **emacsbook**, A free/online book about Lisp and Emacs (in Korean), 10/2011
`https://github.com/tsgates/emacsbook`.

[23] **gtklookup**, An Emacs mode provides a search interface for GTK manual, 10/2009
`https://github.com/tsgates/gtklookup`.

[24] **pylookup**, An Emacs mode provides a search interface for Python reference manual, 07/2009
`https://github.com/tsgates/pylookup`.

[25] **cclookup**, An Emacs mode provides a search interface for C++ reference manual, 06/2009
`https://github.com/tsgates/cclookup`.

[26] **git-emacs**, An Emacs major mode provides a VCS interface to git, 03/2009
`https://github.com/tsgates/git-emacs`.

[27] **django-html-mode**, An Emacs major mode renders Django html templates, 12/2007.

As byproducts of our research, we've directly contributed to popular opensource projects, including Linux, FreeBSD, Android, Microsoft Windows, Chrome, Safari, Firefox, IE, PHP, OpenSSL, Python, Rust, etc (see CVEs summarized in our web site).

D. PRESENTATIONS (SELECTED)

[1] **Are we done yet? Our journey to fight against memory-safety bugs**
CTF Cybersecurity Symposium (ASU)

[2] **Are we done yet? Our journey to fight against memory-safety bugs**
Keynote at CCS'21

[3] **Building Trustworthy Software Foundation with Hardware Security Mechanisms**
Keynote at Samsung Security Tech Forum 2018

[4] **Attacks and Defenses for Intel SGX**
The 7th Technion Summer School on Cyber and Computer Security

[5] **Scaling Security Practices: Automated Approaches to Eliminate Security Vulnerabilities**
University of Pennsylvania (04/2018), Columbia University (04/2018), MIT (04/2018), University of Michigan (04/2018), Princeton University (04/2018)

[6] **SGX Security and Privacy (Invited Tutorial)**
CCS'17 Tutorial (11/2018)

[7] **Security and AI**
Microsoft Faculty Summit 2017: The Edge of AI (07/2017)

[8] **Attacking Intel SGX**
Intel Science and Technology Center (ISTC) for Adversary-Resilient Security Analytics (06/2017), Seoul National University (05/2017), Korea University (05/2017), Zer0con: Conference for Exploit Developers & Bug Hunters (04/2017)

[9] **Bless and curse of a new hardware feature: the case of Intel TSX**
POSTECH (12/2016), KAIST (12/2016), National Security Research Institute (NSRI) (12/2016)

[10] **Cross-checking Semantic Correctness: The Case of Finding File System Bugs**
Yonsei University (12/2016), KAIST (03/2016), Sungkyungkwan University (12/2015)

[11] **MLsploit: Framework for Evaluating and Improving ML in Security Applications**
Intel Adversary-Resilient Security Analytics (08/2016)

[12] **DrK: Breaking Kernel Address Space Layout Randomization with Intel TSX**
Intel SGX Team (08/2016)

[13] **Understanding Manycore Scalability of File Systems**
KCC 2016 (06/2016)

[14] **Mitigating DDoS Attacks with Resource-oriented Reconfiguration**
DARPA/XD3 Kick-off (04/2016)

[15] **Emerging Security Concerns on Cloud Computing**
National Security Research Institute (NSRI) (03/2016)

[16] **Recent Trends and Techniques to prevent Code-Reuse Attacks**
Samsung R&D Center (12/2015)

[17] **Scalability in the Clouds! A Myth or Reality?**
ETRI, Electronics and Telecommunications Research Institute (12/2015)

[18] **Rebootless Operating System Update**
2015 US-Korea Conference on Science, Technology and Entrepreneurship (08/2015)

[19] **ASLR-Guard: Stopping Code Address Leakages for Code Reuse Attacks**
Dagstuhl Seminar: The Continuing Arms Race: Code-Reuse Attacks and Defenses (07/2015)

[20] **Automatic Intrusion Recovery with System-wide History**
Seoul National University (07/2015), KAIST (07/2015), Kyungpook National University (07/2015)

[21] **Study on Manycore Scalabiliy of Next-generation OSes**
Electronics and Telecommunications Research Institute (ETRI) (07/2015)

[22] **BFT++: Attack-tolerant Systems**
ASD-R&E: Kick-off Meeting (ICS) (06/2015), ONR/NSWC: Attack-resilient Industrial Control Systems (ICS) (03/2015), ONR Workshop, University of California, Santa Barbara (01/2015)

[23] **Efficient Patch-based Auditing for Web Application Vulnerabilities**
Software Engineering Seminar (03/2015), KAIST (08/2013), Seoul National University (08/2013), OSDI'12 (10/2012)

[24] **MetaSync: File Synchronization Across Multiple Untrusted Storage Services**
CERCS, Georgia Institute of Technology (10/2014)

[25] **BlackNet: Surveillance System with Automotive Black Boxes (EDR)**
NSF: US/Korea Workshopon SDN/NFV for Smart Cities (08/2014)

[26] **Automatic Intrusion Recovery with System-wide History**
Georgia Institute of Technology (04/2014), Microsoft Research, Mountain View, CA (04/2014), University of Texas at Austin (03/2014), University of Washington (03/2014), University of Maryland (03/2014), Cornell University (03/2014), Microsoft Research, Redmond, WA (02/2014), University of Southern California (02/2014), Purdue University (02/2014)

[27] **Asynchronous Intrusion Recovery for Interconnected Web Services**
SOSP'13 (11/2013)

[28] **Optimizing Unit Test Execution in Large Software Programs using Dependency Analysis**
APSys'13 (07/2013)

[29] **Practical and Effective Sandboxing for Non-root Users**
ATC'13 (06/2013)

[30] **Poirot: Auditing Web Application Vulnerability with Security Patches (poster)**
DARPA/CRASH PI Meeting

[31] **System-Level Protection Against Cache-based Side Channel Attacks in the Cloud**
USENIX Security'12 (08/2012), Sungkyungkwan University (12/2012)

[32] **Recovering from Intrusions in Distributed Systems with Dare**
APSys'12 (07/2012)

[33] **Intrusion Recovery Using Selective Re-execution**
POSTECH (06/2011), KAIST (05/2011)

[34] **Preventing Side-channel Attacks Exploiting Memory Latency for Cloud Computing**
MIT CSAIL Security Seminar (10/2010)

[35] **A new protection mechanism against cache-based side-channel attacks in the Cloud**
Microsoft Research XCG, (08/2010)

[36] **Making Linux Protection Mechanisms Egalitarian with UserFS**
USENIX Security'10 (08/2010), MIT CSAIL Security Seminar (07/2010), Microsoft Research (07/2010)

[37] **Program Binary Obfuscation**
MIT CSAIL Security Seminar, (03/2010)

[38] **Playing with Beehive: Design a Hardware Locking in Verilog**
IAP: Multicore research with Beehive (01/2010)

[39] **Simulation of Human Locomotion using a Musculoskeletal Model**
Int. Conference on Control, Automation and Systems (10/2008)

E. Grants and Contracts

$47.6 million is awarded in total, out of which my share is **$18.4 million**.

E.1. As Principal Investigator

[1] **Title of Project: Extending Use-After-Free Vulnerabilities Detection to Userspace Applications and Language Runtime.**
Agency/Company: National Security Research Institute (NSRI),
Total Dollar Amount: $85,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 08/2022–07/2023
Share: 100%

[2] **Title of Project: Pioneering the Software Development Paradigm with Rust**
Agency/Company: ONR
Total Dollar Amount: $825,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 01/2023–12/2027
Share: 100%

[3] **Title of Project: EdgeShield: Defeating Next-generation Cyber Threats on the Edge Environment**
Agency/Company: Cisco
Total Dollar Amount: $154,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 11/2022–10/2023
Share: 100%

[4] **Title of Project: Research on Detection of Use-After-Free Vulnerabilities with Function Summarization**
Agency/Company: National Security Research Institute (NSRI),
Total Dollar Amount: $85,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 08/2021–07/2022
Share: 100%

[5] **Title of Project: MetaFuzz: A Dynamic Approach to Schedule Existing Fuzzers for Better Performance**
Agency/Company: Cisco
Total Dollar Amount: $150,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 08/2021–04/2023
Share: 100%

[6] **Title of Project: Enhancing Security of Systems Software**
Agency/Company: Technology Innovation Institute, Abu Dhabi, UAE
Total Dollar Amount: $1,800,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 03/01/2021–03/01/2023
Share: 100%

[7] **Title of Project: D3: Debloating, Dialecting and Diversification for Attack Resilient Software with Real-time Constraints**
Agency/Company: Technology Innovation Institute, Abu Dhabi, UAE
Total Dollar Amount: $1,575,000
Role: PI
Collaborators: Taesoo Kim (PI), Wenke Lee (co-PI)
Period of Contract: 09/01/2020–08/31/2023
Share: 50%

[8] **Title of Project: Research on Automatic Generation of Security Model**
Agency/Company: National Security Research Institute (NSRI),
Total Dollar Amount: $85,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 08/2020–07/2021
Share: 100%

[9] **Title of Project: Google Research Award (Gift)**
Agency/Company: Google
Total Dollar Amount: $63,026

Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 03/2019
Share: 100%

[10] **Title of Project: VMware Early Career Faculty Grants (Gift)**
Agency/Company: VMware
Total Dollar Amount: $35,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 08/2018
Share: 100%

[11] **Title of Project: Exploring Security Hardening Techniques for Trustworthy Cloud Platforms**
Agency/Company: KAIST
Total Dollar Amount: $32,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 07/19/2019–06/31/2021
Share: 100%

[12] **Title of Project: RUST as Automotive Programming Language: Security, Safety and Performance**
Agency/Company: Ford
Total Dollar Amount: $200,000
Role: PI
Collaborators: Taesoo Kim (PI) and Vivek Sarkar (co-PI)
Period of Contract: 05/2019–05/2021
Share: 50%

[13] **Title of Project: Toward Autonomous Reasoning of Weird Machines in The Presence of Memory-safety Issues (DARPA AIMEE)**
Agency/Company: Defense Advanced Research Projects Agency (DARPA)
Total Dollar Amount: $805,070
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 01/2020–06/2021
Share: 100%

[14] **Title of Project: Exploring Potential Privacy and Security Threats on Emerging IoT Protocol Stacks**
Agency/Company: Samsung
Total Dollar Amount: $100,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 11/2018–11/2019
Share: 100%

[15] **Title of Project: SGX101: Example-based, Security-focused Educational Modules for Learning SGX (Gift)**
Agency/Company: Intel
Total Dollar Amount: $15,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 08/2019–08/2020
Share: 100%

[16] **Title of Project: PRIDWEN: New Software and Hardware Abstractions to Address Side-channel Attacks against Intel SGX (Gift)**
Agency/Company: Intel
Total Dollar Amount: $300,000
Role: PI
Collaborators: Taesoo Kim (PI)

Period of Contract: 01/2019–01/2022
Share: 100%

[17] **Title of Project: Interactive Editing Techniques for Subsetting and Dialeting Network Protocol**
Agency/Company: ONR
Total Dollar Amount: $5,080,580
Role: PI
Collaborators: Taesoo Kim (PI), Brendan Saltaformaggio, William Harris, Santosh Pande, Alessandro Orso and Wenke Lee
Period of Contract: 04/2018–10/2023
Share: 63%

[18] **Title of Project: MuPDF License Violation (Gift)**
Agency/Company: Artifex
Total Dollar Amount: $22,500
Role: PI
Collaborators: Taesoo Kim (PI), Wenke Lee
Period of Contract: 01/2018–04/2018
Share: 50%

[19] **Title of Project: CAREER: System Techniques to Improve Fuzzing Performance**
Agency/Company: NSF
Total Dollar Amount: $500,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 03/2018–02/2024
Share: 100%

[20] **Title of Project: PRIDWEN: A Composable, Compiler-Based Framework for Protecting SGX Programs against Side-Channel Attacks (Gift)**
Agency/Company: Intel
Total Dollar Amount: $270,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 12/2017–11/2020
Share: 100%

[21] **Title of Project: HOSEA: Hardware-Oriented Secure Edge Analytics for IoT**
Agency/Company: Samsung
Total Dollar Amount: $100,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 10/2017–09/2018
Share: 100%

[22] **Title of Project: Diversity and Integrity for Cyber Resilience of Legacy Industrial Control & Combat Systems**
Agency/Company: Boeing/ONR
Total Dollar Amount: $750,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 02/2017–08/2020
Share: 100%

[23] **Title of Project: Designing New Operating Primitives to Improve Fuzzing Performance (Gift)**
Agency/Company: Mozilla
Total Dollar Amount: $60,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 06/01/2017–06/01/2018
Share: 100%

[24] **Title of Project: Designing Secure Cloud Storage Service by using SGX**
Agency/Company: Mirae Technology Research Foundation (MTRF)
Total Dollar Amount: $50,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 09/2016–08/2017
Share: 100%

[25] **Title of Project: CI-P: Collaborative: Planning for a Community-Driven Open Research Infrastructure to Support Secure Computing Research involving Intel SGX**
Agency/Company: National Science Foundation (NSF)
Total Dollar Amount: $100,000
Role: PI
Collaborators: Taesoo Kim (PI) and Zhiqiang Lin
Period of Contract: 08/2016–08/2017
Share: 50%

[26] **Title of Project: Virtualized Infrastructure for Information Security**
Agency/Company: Georgia Tech
Total Dollar Amount: $60,665
Role: PI
Collaborators: Taesoo Kim (PI), Manos Antonakakis, Wenke Lee, and Mustaque Ahamad
Period of Contract: 08/2016
Share: 25%

[27] **Title of Project: TWC: Medium: Collaborative: Systems, Tools, and Techniques for Executing, Managing, and Securing SGX Programs**
Agency/Company: National Science Foundation (NSF)
Total Dollar Amount: $1,199,999
Role: PI
Collaborators: Taesoo Kim (PI) and Zhiqiang Lin
Period of Contract: 06/2016–04/2020
Share: 56%

[28] **Title of Project: Python Bug Bounty: CVE-2016-5636 (Gift)**
Agency/Company: Internet Bug Bounty
Total Dollar Amount: $1,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 06/2016
Share: 100%

[29] **Title of Project: PHP Bug Bounty (Gift)**
Agency/Company: Internet Bug Bounty
Total Dollar Amount: $1,500
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 05/2016
Share: 100%

[30] **Title of Project: Microsoft Azure Research Award CRM:00290117 (Gift)**
Agency/Company: Microsoft
Total Dollar Amount: $20,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 01/2016
Share: 100%

[31] **Title of Project: Mitigating DDoS Attacks at the Endpoint with Resource-Oriented Reconfiguration**
Agency/Company: Defense Advanced Research Projects Agency (DARPA)

Total Dollar Amount: $1,187,200
Role: PI
Collaborators: Taesoo Kim (PI), William R. Harris, Wenke Lee
Period of Contract: 05/2016–09/2017
Share: 51%

[32] **Title of Project: SaTC-EDU: EAGER: Big Data and Security: Educating The Next-Generation Security Analysts**
Agency/Company: National Science Foundation (NSF)
Total Dollar Amount: $300,000
Role: PI
Collaborators: Taesoo Kim (PI), Manos Antonakakis, Mayur Naik, Wenke Lee
Period of Contract: 06/2015–05/2017
Share: 65%

[33] **Title of Project: Educating the Next Generation Computer Scientists: Curriculum Development for Secure Big Data Processing**
Agency/Company: GT-FIRE: Transformative Research and Education Annual Awards
Total Dollar Amount: $7,000
Role: PI
Collaborators: Taesoo Kim (PI), Hadi Esmaeilzadeh
Period of Contract: 02/2015–01/2016
Share: 50%

[34] **Title of Project: Research on Concolic Testing Techniques Applicable to Real-world Software**
Agency/Company: National Security Research Institute (NSRI),
Total Dollar Amount: $89,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 07/2015–06/2016
Share: 100%

[35] **Title of Project: BFT++: Attack Tolerance in Hard Real-Time Systems**
Agency/Company: Office of Naval Research (ONR)
Total Dollar Amount: $1,245,719
Role: PI
Collaborators: Taesoo Kim (PI), Wenke Lee, Tielei Wang
Period of Contract: 04/2015–03/2018
Share: 48%

[36] **Title of Project: Xilinx Education Equipment Donation (14260178) (Gift)**
Agency/Company: Xilinx
Total Dollar Amount: $12,564
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 10/2015
Share: 100%

[37] **Title of Project: Georgia Power Professor of Excellence Award (Gift)**
Agency/Company: Georgia Power
Total Dollar Amount: $1000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 10/2015
Share: 100%

[38] **Title of Project: The Best Applied Security Research Paper (Gift)**
Agency/Company: Cyber Security Awareness Week 2015 (CSAW)
Total Dollar Amount: $500
Role: PI

Collaborators: Taesoo Kim (PI), Wenke Lee
Period of Contract: 11/2015
Share: 100%

[39] **Title of Project: 2015 Internet Defense Prize (Gift)**
Agency/Company: Facebook
Total Dollar Amount: $100,000
Role: PI
Collaborators: Taesoo Kim (PI) and Wenke Lee
Period of Contract: 08/2015
Share: 100%

[40] **Title of Project: Xilinx Education Equipment Donation (14260178) (Gift)**
Agency/Company: Xilinx
Total Dollar Amount: $6,990
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 02/2015
Share: 100%

[41] **Title of Project: Xilinx Education Equipment Donation (14260178) (Gift)**
Agency/Company: Xilinx
Total Dollar Amount: $4,635
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 01/2015
Share: 100%

[42] **Title of Project: Mozilla Foundation Security Advisory: CVE-2014-89 (Gift)**
Agency/Company: Mozilla
Total Dollar Amount: $3,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 12/2014
Share: 100%

[43] **Title of Project: Study on Manycore Scalabiliy of the Next-generation Operating Systems**
Agency/Company: Electronics and Telecommunications Research Institute (ETRI)
Total Dollar Amount: $1,098,000
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 11/2014–02/2018
Share: 100%

[44] **Title of Project: Intel Equipment Donation (16826535) (Gift)**
Agency/Company: Intel
Total Dollar Amount: $34,578
Role: PI
Collaborators: Taesoo Kim (PI)
Period of Contract: 10/2014
Share: 100%

E.2. As Co-Principal Investigator

[1] **Title of Project: AI-Assisted Prevention of Supply Chain Attacks on Programming Language Packages**
Agency/Company: Defense Advanced Research Projects Agency (DARPA)
Total Dollar Amount: $1,000,000
Role: co-PI
Collaborators: Brendan Saltaformaggio (PI), Wenke Lee (co-PI) and Taesoo Kim (co-PI)
Period of Contract: 06/2021–11/2022
Share: 31%

[2] **Title of Project: Proof-driven Refinement of Infrastructure Software Modules (PRISM)**
Agency/Company: Defense Advanced Research Projects Agency (DARPA)
Total Dollar Amount: $10,600,000
Role: co-PI
Collaborators: Brendan Saltaformaggio (PI), Wenke Lee (co-PI), Taesoo Kim (co-PI), Alessandro Orso (co-PI), Qirun Zhang (co-PI)
Period of Contract: 04/2021–04/2025
Share: 15%

[3] **Title of Project: AUTOMPHC: Automating Massively Parallel Heterogeneous Computing (DARPA PAPPA)**
Agency/Company: Defense Advanced Research Projects Agency (DARPA)
Total Dollar Amount: $1,000,000
Role: co-PI
Collaborators: Vivek Sarkar (PI), Taesoo Kim (co-PI) and Sukarno Mertoguno (co-PI)
Period of Contract: 01/2020–06/2021
Share: 20%

[4] **Title of Project: SaTC: CORE: Medium: Understanding and Fortifying Machine Learning Based Security Analytics**
Agency/Company: NSF
Total Dollar Amount: $1,000,000
Role: co-PI
Collaborators: Polo Chau (PI), Taesoo Kim, Wenke Lee and Le Song
Period of Contract: 08/2017–08/2020
Share: 25%

[5] **Title of Project: Comprehensive System Debloating via Path-Based Learning and Late-Stage OS Composition**
Agency/Company: ONR
Total Dollar Amount: $4,500,000
Role: co-PI
Collaborators: William Harris (PI), Taesoo Kim, Wenke Lee, Alessandro Orso, and Santosh Pande
Period of Contract: 09/2017–08/2020
Share: 20%

[6] **Title of Project: The Malware Lab: A Collaborative Malware Analysis and Experimentation Framework**
Agency/Company: Lockheed Martin
Total Dollar Amount: $100,000
Role: co-PI
Collaborators: Wenke Lee (PI) and Taesoo Kim
Period of Contract: 06/2017–05/2018
Share: 50%

[7] **Title of Project: Georgia Tech's Scholarship-for-Service (SFS) Program**
Agency/Company: National Science Foundation (NSF)
Total Dollar Amount: $4,999,196
Role: co-PI
Collaborators: Mustaque Ahamad (PI), Wenke Lee, Taesoo Kim, Seymour Goodman, and Emmanouil K. Antonakakis
Period of Contract: 09/2016–09/2020
Share: 2%

[8] **Title of Project: Intel Adversary-Resilient Security Analytics (Gift)**
Agency/Company: Intel
Total Dollar Amount: $1,500,000
Role: co-PI
Collaborators: Wenke Lee (PI), Polo Chau, Taesoo Kim, and Le Song
Period of Contract: 08/2016–08/2019
Share: 15%

[9] **Title of Project: Transparent Computing, THEIA: Tagging and Tracking of Multi-level Host Events for Transparent Computing and Information Assurance**

Agency/Company: Defense Advanced Research Projects Agency (DARPA)
Total Dollar Amount: $4,253,126
Role: co-PI
Collaborators: Wenke Lee (PI), Taesoo Kim, Alessandro Orso, Simon Chung, Albert Brezecko.
Period of Contract: 07/2015–06/2019
Share: 20%

F. Other Scholarly and Creative Accomplishments

[1] **Leading NSA Codebreaker Competition, 2015-2020**: Students in CS6265, which I designed and offered in 2015-2020, participated together in NSA Codebreaker Challenges and ranked in top 3 in the competition a seven-year streak.

[2] **TKCTF, 2018-**: We have been organizing TKCTF at GT since 2018.

[3] **Finalist to the DARPA Cyber Grand Challenge, 2016**: The Disekt team proceeded to the final round of the DARPA Cyber Grand Challenge, and resulted in $750,000 award.

[4] **Start-up**: A group of PhD students (two from MIT and one from Stanford) with our advisor at MIT co-found a start-up, Nerati (now Compass), whose underlying techniques are based on my thesis. We got two million dollars initial investment from Bain Capital Ventures (2012).

G. Societal And Policy Impacts

G.1. Research Coverage in the News

[1] *Georgia Tech Takes Second in NSA Codebreaker Challenge to Extend to a Seven-Year Streak*:
GT School of Cybersecurity and Privacy (03/2021)

[2] *Team of Georgia Tech Students Win World Hacking Competition*:
GT CoC News Letter (08/2018)

[3] *Assistant Professor Taesoo Kim Wins NSF CAREER Award for Fuzzing Research*:
GT CoC News Letter (03/2018)

[4] *Georgia Tech Professor Taesoo Kim Named Allchin Professor*:
GT CoC News Letter (11/2017)

[5] *Georgia Tech Students Sweep NSA Hacking Contest*:
GT Institute for Information Security and Privacy (03/2017)

[6] *College of Computing's Taesoo Kim Has a Passion For the Nitty-Gritty Details of Internet Security*:
School of Computer Science (12/2016)

[7] *BFT++: Attack Tolerance in Hard Real-Time Systems*:
Georgia Tech News Center (06/2015), Atlanta Business Chronicle (06/2015)

[8] *Mitigating DDoS Attacks at the Endpoint with Resource-Oriented Reconfiguration*:
GovInfoSecurity (05/2016), Cyber War Desk (05/2016), FierceITSecurity (05/2016)

[9] *Rudra: Finding Memory Safety Bugs in Rust at the Ecosystem Scale*:
Distinguished Artifact Award

[10] *Finding Consensus Bugs in Ethereum via Multi-transaction Differential Fuzzing*:
Coindesk, Yahoo Fiance

[11] *FREEDOM: Engineering a State-of-the-Art DOM Fuzzer*:
CVE-2019-6212, CVE-2019-8596, CVE-2019-8609, CVE-2019-8720, CVE-2020-9803, CVE-2020-9806, CVE-2020-9807, CVE-2020-9895, CVE-2019-5806, CVE-2019-5817

[12] *Compromising the macOS kernel through Safari by chaining six vulnerabilities*:
Pwn2Own, CVE-2020-9850, CVE-2020-9839, CVE-2020-9856, CVE-2020-9801

[13] *Fuzzing JavaScript Engines with Aspect-preserving Mutation*:
CVE-2020-6382, CVE-2019-13730, CVE-2019-13764, CVE-2019-8811, CVE-2019-8816, ... (12 CVEs)

[14] *MLsploit: A Framework for Interactive Experimentation with Adversarial Machine Learning Research*:
BlackHat Asia/Arsenal

[15] *Breaking Turtles All the Way Down: An Exploitation Chain to Break out of VMware ESXi*:
CVE-2018-6981, CVE-2018-6982

[16] *Fuzzification: Anti-Fuzzing Techniques*:
Hacker News

[17] *Fuzzing File Systems via Two-Dimensional Input Space Exploration*:
CVE-2018-1092, CVE-2018-1093, CVE-2018-1094, CVE-2018-1095, CVE-2018-10840, CVE-2018-10876, CVE-2018-10877, CVE-2018-10878, CVE-2018-10879, CVE-2018-10880, CVE-2018-10881, CVE-2018-10882, CVE-2018-10883, ... (32 CVEs)

[18] *QSYM: A Practical Concolic Execution Engine Tailored for Hybrid Fuzzing*:
CVE-2017-6836, CVE-2017-8891, CVE-2017-12878, CVE-2017-17080, CVE-2017-17081, ...

[19] *Precise and Scalable Detection of Double-Fetch Bugs in OS Kernels*:
CVE-2017-15037

[20] *Designing New Operating Primitives to Improve Fuzzing Performance*:
Mozilla Research

[21] *RAIN: Refinable Attack Investigation with On-demand Inter-Process Information Flow Tracking*:
GT News Horizons

[22] *SGX-Bomb: Locking Down the Processor via Rowhammer Attack*:
Hacker News

[23] *Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing*:
Intel SGX Research

[24] *Hacking in Darkness: Return-oriented Programming against Secure Enclaves*:
Intel SGX Research

[25] *AVPASS: Leaking and Bypassing Antivirus Detection Model Automatically*:
DARK Reading 1/2/3, WIRED

[26] *CAB-Fuzz: Practical Concolic Testing Techniques for COTS Operating Systems*:
CVE-2015-6098, CVE-2016-0040, CVE-2016-7219

[27] *Mosaic: Processing a Trillion-Edge Graph on a Single Machine*:
The Next Platform, Hacker News 1/2, GT News, The morning paper

[28] *Enhancing Security and Privacy of Tor's Ecosystem by using Trusted Execution Environments*:
Intel SGX Research

[29] *SGX-Shield: Enabling Address Space Layout Randomization for SGX Programs*:
Intel SGX Research

[30] *T-SGX: Eradicating Controlled-Channel Attacks Against Enclave Programs*:
Intel SGX Research

[31] *Fast, Scalable and Secure Onloading of Edge Functions using AirBox*:
Patent: WO2018026841A1

[32] *UniSan: Proactive Kernel Memory Initialization to Eliminate Data Leakages*:
CVE-2016-5243, CVE-2016-5244, CVE-2016-4569, CVE-2016-4578, CVE-2016-4569, CVE-2016-4485, CVE-2016-4486, CVE-2016-4482, AndroidID-28620568, AndroidID-28619338, AndroidID-28620324, AndroidID-28673002, AndroidID-28672819, AndroidID-28672560, AndroidID-28616963, ...

[33] *Breaking Kernel Address Space Layout Randomization with Intel TSX*:
Hacker News, LWN, Attacking Windows 10 by IOActive, Google Project Zero, Microsoft

[34] *APISan: Sanitizing API Usages through Semantic Cross-checking*:
TGC/News, CVE-2016-5636

[35] *Breaking Kernel Address Space Layout Randomization (KASLR) with Intel TSX*:
Hacker News, LWN, Attacking Windows 10 by IOActive, Google Project Zero, Microsoft

[36] *Instant OS Updates via Userspace Checkpoint-and-Restart*:
Linux Plumbers Conference 2015, CRIU

[37] *S-NFV: Securing NFV States by using SGX*:
Intel SGX Research

[38] *OpenSGX: An Open Platform for SGX Research*:
Wikipedia: Software Guard Extensions, Intel SGX Research

[39] *Opportunistic Spinlocks: Achieving Virtual Machine Scalability in the Clouds*:
LWN: qspinlock in Linux

[40] *UCognito: Private Browsing without Tears*:
Observer Innovation

[41] *ASLR-Guard: Stopping Address Space Leakage for Code Reuse Attacks*:
Dagstuhl Seminar

[42] *Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations*:
Android Security, CERT, Networkworld, Softpedia, pocketnow, VoIPshield, VU#943167, CVE-2015-6614

[43] *Cross-checking Semantic Correctness: The Case of Finding File System Bugs*:
Bug Report

[44] *Type Casting Verification: Stopping an Emerging Attack Vector*:
Internet Defense Prize, USENIX Update, Facebook, ZDNet, We Live Security, Science 2.0, hys.org, Scientific Computing, IT Pro Portal, Laboratory Equipment, Gizbot, Science Codex, Business Standard, ECN magazine, The Times of India, CanIndia News, New Indian Express, InfoSec, Social Times, The Register, CTV News, Threat Post, TNW News, The Security Ledger, Georgia Tech News Center, ScienceDaily, Milton Security, ACM TECHNEWS, Gadget 360, SC Magazine, IHS Engineering 360, CVE-2014-1594, ...

[45] *Scalability in the Clouds! A Myth or Reality?*:
LWN: qspinlock in Linux

[46] *Abusing Performance Optimization Weaknesses to Bypass ASLR*:
Phrack, ISS Source, IT Researches, Embedded

[47] *From Zygote to Morula: Fortifying Weakened ASLR on Android*:
LWN, Copperhead

[48] *Practical and Effective Sandboxing for Non-root Users*:
Hacker News, Wikipedia: seccomp, Coders Grid, AlternativeTo, TorProject

[49] *Intrusion Recovery using Selective Re-execution*:
Network World

H. Other Professional Activities

[1] Visiting Scholar at University of Washington (CSE, 06/2014–08/2014).

V. Education

A. Courses Taught

Semester	Course Number	Course Title	Enrollment	CIOS Score (5.0)
Fall 2023	CS 6365	Information Security Lab (link)	48	N/A
Spring 2023	CS 8803	Exploiting Smart Contracts and DeFi (link)	40	N/A
Fall 2020	CS 6265 A/O01/OCY	Information Security Lab (link)	25/16/36	4.9/5.0/4.58
Spring 2020	CS 3210 A	Design Operating Systems (link)	61	N/A (due to COVID)
Fall 2019	CS 6265 A/O01/OCY	Information Security Lab (link)	33/36/5	4.7/4.6/5.0
Fall 2018	CS 6265 A (8803)	Information Security Lab (link)	31	4.6
Fall 2017	CS 6265 A (8803)	Information Security Lab (link)	21	4.7
Fall 2016	CS 6265 A	Information Security Lab (link)	24	4.7
Spring 2016	CS 3210 A/GR1	Design Operating Systems (link)	40/1	4.8/5.0 (100%)
Fall 2015	CS 6265 E	Information Security Lab (link)	21	4.2
Fall 2014	CS 8803 BSS	Special Topics: Building Secure Systems (link)	16	4.8

- *"The best and hardest class I have ever taken."* — in CS 6265, Fall 2017
- *"I have found Taesoo to be an asset in addressing challenges and problems in class as well as during my acquaintanceship with him over the past two years. I look forward to following his professional success over the coming years."* — in CS 6265, Fall 2017
- *"The bevy of knowledge I've gained really is remarkable."* — in CS 6265, Fall 2016
- *"Tech is fortunate to have Prof. Kim!"* — in CS 6265, Fall 2016
- *"Probably one of the best profs at Tech."* — in CS 3210, Spring 2016
- *"He is extremely knowledgeable about any topics that I had questions about in lecture. He also covered interesting research topics in class, keeps a very good and comprehensible pace. Another great feature is live code demos. Almost all of my sysarch professors thus far keep lectures extremely theoretical with no application."* — in CS 3210, Spring 2016
- *"the sheer brilliance. good grasp on each concepts. effective communication in transferring knowledge. Atleast I got inspired to study harder. Although I struggled way too much, it was fun."* — in CS 6265, Fall 2015
- *"The best course I have taken in my entire degree at Georgia Tech. I gained more knowledge from this course than I gained from all of my other security courses combined."* — in CS 6265, Fall 2015
- *"He exceeds all you can imagine in this field. Though tough to follow, it is good to make your shoes wet"* — in CS 8803, Fall 2014
- *"Prof Taesoo's strength is his incredible dedication to be practical and get his hands dirty. This is very impressive because not many profs are able to display such technical ability and it definitely help students see/learn how things are done in reality."* — in CS 8803, Fall 2014

B. Individual Student Guidance

B.1. Ph.D. Students

[1] **Soyeon Park**
Spring 2017-present
Publications: [4], [24], [24], [25], [30], [41]
Status: Post-Qualifier

[2] **Fan Sang**
Fall 2018-present
Publications: [12], [17]
Status: Post-Qualifier

[3] **Seulbae Kim**
Fall 2018-present
Publications: [8], [3], [33]
Status: Post-Qualifier

[4] **Hanqing Zhao**
Summer 2018-present
Publications: [29], [38]
Status: Pre-Qualifier

[5] **Sujin Park**
Fall 2019-present
Publications: [13], [22]
Status: Pre-Qualifier

[6] **Mansour Alharthi**
Fall 2019-present
Publications: N/A
Status: Pre-Qualifier

[7] **Ammar Askar**
Fall 2019-present
Publications: [5], [10], [19]
Status: Post-Qualifier

[8] **Kevin Stevens**
Fall 2020-present
Publications: N/A
Status: Pre-Qualifier

[9] **Mingyu Guan**
Spring 2020-present
Publications: [14]
Status: Post-Qualifier

[10] **Yu-Fu Fu**
Fall 2020-present
Publications: [3]
Status: Pre-Qualifier

[11] **Mingyi Liu**
Spring 2021-present
Publications: N/A
Status: Pre-Qualifier

[12] **Fabian Fleischer**
Fall 2021-present
Publications: N/A
Status: Pre-Qualifier

[13] **Kuilin Li**
Fall 2021-present
Publications: N/A
Status: Pre-Qualifier

[14] **Xiang Cheng**
Fall 2021-present
Publications: [1]
Status: Pre-Qualifier

[15] **Chuhong Yuan**
Fall 2022-present
Publications: N/A
Status: Pre-Qualifier

[16] **Gyejin Lee**
Fall 2022-present
Publications: N/A
Status: Pre-Qualifier

[17] **Jungwon Lim**
Fall 2020-present
Publications: [19], [20], [23], [1]
Status: Pre-Qualifier (on-leave)

[18] **Yonghwi Jin**
Fall 2020-present
Publications: [23], [1]
Status: Pre-Qualifier (on-leave)

[19] **Yechan Bae**
Fall 2019-present
Publications: [19]
Status: Pre-Qualifier (on-leave)

[20] **Wen Xu**
Fall 2016-Summer 2021
Publications: [17], [25], [3], [30], [31], [33], [41], [42], [51], [61]
Thesis: *An IR-based Fuzzing Approach for Finding Context-Aware Bugs in API-based systems*
Status: PhD'22
First Employment: **Postdoc at Georgia Tech**

[21] **Ren Ding**
Spring 2017-Spring 2021
Publications: [17], [31], [58]
Thesis: *Performant Software Hardening under Hardware Support*
Status: PhD'22
First Employment: **Facebook**

[22] **Jinho Jung**
Fall 2016-Spring 2021
Publications: [23], [27], [32], [40], [2]
Thesis: *Practical Systems for Strengthening and Weakening Binary Analysis Frameworks*
Status: PhD'21
First Employment: **ROK Army**

[23] **Insu Yun**
Fall 2016-Winter 2020
Publications: [9], [10], [18], [20], [28], [1], [30], [44], [2], [61], [71], [74]
Thesis: *Concolic Execution Tailored for Hybrid Fuzzing*
Status: PhD'20
Pwn2Own20
Distinguished Paper Award
First Employment: **Assistant Professor at KAIST**

[24] **Sanidhya Kashyap**
Fall 2014-Summer 2020
Publications: [13], [20], [22], [3], [29], [33], [34], [35], [36], [42], [46], [48], [49], [50], [51], [60], [63], [72], [73], [9], [83], [85]
Thesis: *Scaling Synchronization Primitives*

Status: PhD'20
The Best Student Paper Award at EuroSys'17
Best Paper at APSys'15
First Employment: **Assistant Professor at EPFL**

[25] **Meng Xu**
Fall 2014-Summer 2020
Publications: [3], [29], [33], [4], [44], [47], [6], [53], [59], [62], [7], [80]
Thesis: *Finding Race Conditions in Kernels: the Symbolic Way and the Fuzzy Way*
Status: PhD'20
First Employment: **Assistant Professor at the University of Waterloo**

[26] **Ming-wei Shih**
Fall 2014-Summer 2019
Publications: [12], [56], [65], [66], [67], [7], [75], [76]
Thesis: *Securing Intel SGX against Side-Channel Attacks via Load-Time Synthesis*
Status: PhD'20
First Employment: **Microsoft**

[27] **Mohan Kumar**
Fall 2014-present
Publications: [2], [49], [50], [63], [75]
The Best Student Paper Award at EuroSys'17
First Employment: **Facebook**

[28] **Steffen Maass**
Fall 2015-present
Publications: [2], [49], [50], [63], [72]
The Best Student Paper Award at EuroSys'17
First Employment: **Google**

[29] **YeongJin Jang**
Fall 2014-Summer 2017
Publications: [44], [54], [57], [69], [7], [71], [3], [80], [82], [88], [4]
Thesis: *Building Trust in the User I/O in Computer Systems*
Status: PhD'17 (Co-advised by Wenke Lee)
First Employment: **Assistant Professor at Oregon State University**

[30] **Kangjie Lu**
Fall 2014-Summer 2017
Publications: [4], [47], [62], [68], [7], [77], [81]
Thesis: *Securing Software Systems by Preventing Information Leaks*
Status: PhD'17 (Co-advised by Wenke Lee)
First Employment: **Assistant Professor at the University of Minnesota**

[31] **Chengyu Song**
Fall 2014-Spring 2016
Publications: [4], [58], [68], [7], [74], [77], [81], [83], [84], [88], [4]
Thesis: *Preventing Exploits against Memory Corruption Vulnerabilities*
Status: PhD'16 (Co-advised by Wenke Lee)
2015 Internet Defense Prize
First Employment: **Assistant Professor at UC Riverside**

[32] **Byoungyoung Lee**
Fall 2014-Spring 2016
Publications: [61], [65], [7], [73], [74], [77], [81], [83], [84], [88], [4], [92]
Thesis: *Protecting Computer Systems through Eliminating or Analyzing Vulnerabilities*
Status: PhD'16 (Co-advised by Wenke Lee)
2015 Internet Defense Prize
First Employment: **Assistant Professor at Purdue**

B.2. M.S. Students

[1] **Jeffrey Forster**
Spring 2016-Fall 2017
Publications: N/A
Thesis: *Using Intel SGX Technologies to Secure Large Scale Systems in Public Cloud Environments*
Status: Thesis Track
First Employment: **Sandia National Laboratories**

[2] **Kevin Flansburg**
Fall 2014-Spring 2016
Publications: N/A
Thesis: *A Framework for Automated Management of Exploit Testing Environments*
Status: MS'16
First Employment: **PhD at Georgia Tech (ECE)**

[3] **Prerit Jain**
Fall 2014-Spring 2015
Publications: [76]
Status: MS'15
First Employment: **Oracle**

[4] **Soham Desai**
Fall 2014-Spring 2015
Publications: [76]
Status: MS'15
First Employment: **Intel**

B.3. Undergraduate Students

[1] **Stephen Tong**
Fall 2018-Fall 2021
Publications: [10], [23]
Status: UROP: Machine Learning Approches in Fuzzing

[2] **David Heavern**
Fall 2016-Fall 2017
Publications: N/A
Status: UROP: Adversarial Machine Learning

[3] **Alex Epifano**
Spring 2017-Fall 2017
Publications: N/A
Status: UROP: Auditing Security Issues in Linux Kernel

B.4. Service on Thesis or Dissertation Committees

[1] Dominic Chen (CMU), *"Mitigating Memory-Safety Bugs with Efficient Out-of-Process Integrity Checking"*, 05/2021.

[2] Wen Xu, *"An IR-based Fuzzing Approach for Finding Context-Aware Bugs in API-based systems"*, 05/2021.

[3] Ren Ding, *"Performant Software Hardening under Hardware Support"*, 05/2021.

[4] Jinho Jung, *"Practical Systems for Strengthening and Weakening Binary Analysis Frameworks"*, 05/2021.

[5] Chenxiong Qian, *"Reducing Software's Attack Surface with Code Debloating"*, 04/2021.

[6] Jaehyuk Lee (KAIST), *"Unintended consequences of system design: unpremeditated usage of benign system components devastates security"*, 11/2020.

[7] Alexander Merritt, *"Efficient Programming of Massive-Memory Machines"*, 07/2017.

[8] Wei Meng, *"Identifying and Mitigating Threats from Embedding Third-party Content"*, 07/2017.

[9] Abhinav Narain, *"Near-Field Deniable Communication"*, 07/2017.

[10] Jian Huang, *"Exploiting Intrinsic Flash Properties to Enhance Modern Storage Systems"*, 06/2017.

[11] Jaebaek Seo, *"Redesigning Software-based Defenses against Privileged Attackers on Trusted Computing"*, 03/2017.

[12] Ketan Bhardwaj, *"Frame, Rods and Beads of the Edge Computing ABACUS"*, 11/2016.

[13] Seungwoo Jung, *"Optimization of SiGe HBT BiCMOS Analog Building Blocks for Operation in Extreme Environments"*, 10/2015.

[14] Wei Jin, *"Automated Support for Reproducing and Debugging Field Failures"*, 05/2015.

[15] Kevin Flansburg, *"A Framework for Automated Management of Exploit Testing Environments"*, 12/2015.

B.5. Mentorship of Postdoctoral Fellows or Visiting Scholars

[1] **Hang Zhang**
Fall 2021-present
Publications: N/A

[2] **Wen Xu**
Fall 2021-present
Publications: [17], [25], [3], [30], [31], [33], [41], [42], [51], [61]

[3] **Sangdon Park**
Fall 2021-present
Publications: [2]

[4] **JaeHyuk Lee**
Spring 2022-present
Publications: [3], [54], [57], [76]

[5] **HyungSeok Han**
Spring 2023-present
Publications: [82]

[6] **Xiaokuan Zhang**
Fall 2021-Summer 2022
Publications: [12]
First Employment: **Assistant Professor at George Mason University**

[7] **Hyungjoon Koo**
Fall 2019-Winter 2020
Publications: [24], [24], [26]
First Employment: **Assistant Professor at Sungkyunkwan University**

[8] **Daehee Jang**
Spring 2019-Winter 2020
Publications: [10], [20], [30]
First Employment: **Assistant Professor at Sungshin Women's University**

[9] **Hong Hu**
Spring 2017-Summer 2020
Publications: [20], [23], [27], [31], [39], [40], [43]
Status: Co-advised by Wenke Lee
First Employment: **Assistant Professor at the Pennsylvania State University**

[10] **Sangho Lee**
Fall 2015-Spring 2019
Publications: [4], [12], [41], [44], [45], [6], [52], [54], [56], [61], [66], [69], [7], [3]
Status: Co-advised by Wenke Lee
Post Doctorate Scholarship from National Research Foundation of Korea, 2017-2018
First Employment: **Researcher at Microsoft Research**

[11] **Hyungon Moon**
Summer 2017-Fall 2018
Publications: [41], [42], [74]
First Employment: **Assistant Professor at UNIST (Ulsan National Institute of Science and Technology)**

[12] **Woonhak Kang**
Spring 2016-Fall 2017
Publications: [27], [49], [55], [63], [72], [86]
Post-doctoral Research Fellowship from Sungkyunkwan University
The Best Student Paper Award at EuroSys'17
First Employment: **eBay**

[13] **Changwoo Min**
Fall 2014-Fall 2017
Publications: [34], [46], [48], [49], [51], [55], [60], [63], [71], [72], [73], [9], [83], [85], [86]
Outstanding Post Doctorate Researcher Award, 2016
Post Doctorate Scholarship from National Research Foundation of Korea, 2015-2016
The Best Student Paper Award at EuroSys'17
Best Paper at APSys'15
First Employment: **Assistant Professor at Virginia Tech**

[14] **Euiseong Seo**
Spring 2018-present
Publications: N/A
Status: Professor at Sungkyunkwan University

[15] **Heeseung Jo**
Spring 2016-Spring 2017
Publications: [49], [55]
Status: Professor at Chonbuk National University

[16] **Su Yong Kim**
Spring 2015-Spring 2016
Publications: [61]
Status: Researcher at National Security Research Institute

C. Educational Innovations and Other Contributions

[1] **Mentoring GreyH@t Hacking Club**. GreyH@t is an undergraduate hacking club at Georgia Tech. We regularly introduce our research projects to the club members, and provide guidance on CTF problems. We also provide lab and course materials for CTF practices.

VI. Service

A. Professional Contributions

A.1. Conference Committee Activities

[1] Program Committee, *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2020

[2] Program Committee, *ACM Symposium on Operating Systems Principles (SOSP)*, 2019, 2021

[3] Program Committee, *International Workshop on Speculative Side Channel Analysis (WoSSCA)*, 2019

[4] Program Committee, *IEEE Symposium on Security and Privacy (Oakland)*, 2019, 2021, 2022

[5] Program Committee, *Workshop on Software Debloating and Delayering (SALAD)*, 2018

[6] Program Committee, *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, 2018

[7] Program Committee, *The Network and Distributed System Security Symposium (NDSS)*, 2018, 2019, 2020

[8] Program Committee, *The Workshop on Binary Analysis Research (BAR)*, 2018, 2019

[9] Program Committee, *USENIX Security Symposium (Security)*, 2015, 2018, 2021, 2022, 2024

[10] Program Committee, *ACM European Conference on Computer Systems (EuroSys)*, 2018

[11] Program Committee, *USENIX Annual Technical Conference (ATC)*, 2017, 2018, 2019

[12] Workshop Co-chair, *ACM Conference on Computer and Communications Security (CCS)*, 2017

[13] Program Committee, *ACM Conference on Computer and Communications Security (CCS)*, 2015, 2016, 2017, 2018, 2019, 2023

[14] Program Committee, *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2016, 2017

[15] Program Committee, *Workshop on Multicore and Rack-scale Systems (MaRS)*, 2016

[16] Program Committee, *ACM Asia-Pacific Workshop on Systems (APSys)*, 2015, 2016, 2018

[17] Program Co-chair, *ACM Asia-Pacific Workshop on Systems (APSys)*, 2020

[18] Program Committee, *USENIX Workshop on Hot Topics in Storage and File Systems (HotStorage)*, 2016

[19] Program Committee, *ACM International Systems and Storage Conference (SYSTOR)*, 2016

[20] Program Committee, *World Conference on Information Security Applications (WISA)*, 2013

[21] Web Admin, *European Conference on Computer Systems (EuroSys)*, 2012

[22] Program Committee, *IEEE Secure Development Conference (SecDev)*, 2017

[23] Program Co-chair, *IEEE Secure Development Conference (SecDev)*, 2020

[24] Steering Committee, *IEEE Secure Development Conference (SecDev)*, 2021, 2022

[25] Program Co-chair, *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2018

[26] Program Committee, *ACM/IFIP/USENIX Middleware (Middleware)*, 2017

[27] Program Committee, *Design Automation Conference (DAC)*, 2017

[28] Program Co-chair, *World Conference on Information Security Applications (WISA)*, 2017

[29] Program Committee, *International World Wide Web Conference (WWW)*, 2017

[30] Program Committee, *Workshop on System Software for Trusted Execution (SysTEX)*, 2016, 2017, 2019

[31] Program Co-chair, *Workshop on Forming an Ecosystem Around Software Transformation (FEAST)*, 2017

[32] Program Committee, *Workshop on Forming an Ecosystem Around Software Transformation (FEAST)*, 2016, 2018, 2019

[33] Advisory, *Silicon Valley Cybersecurity Institute (SVCSI)*, 2022-present

[34] Advisory, *TII*, 2021-present

[35] Academic Advisor, *PwnedNoMore*, 2022-present

[36] Academic Advisor, *Zellic*, 2022-present

A.2. Journal Reviewing Activities

[1] *ACM Transactions on Computer Systems (TOCS)*, 2018

[2] *Security and Communication Networks (SCN)*, 2014

[3] *IBM Journal of Research and Development (IBM)*, 2015

[4] *ACM Transactions on Information and System Security (TISSEC)*, 2014, 2015

[5] *IEEE/ACM Transactions on Networking (ToN)*, 2013

[6] *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2014

A.3. Funding Agency Panel Activities

[1] *NSF*, 2015

A.4. Memberships and Activities in Professional Societies

[1] Member, Association for Computing Machinery (ACM)

[2] Member, The Advanced Computing Systems Association (USENIX)

[3] Member, Institute of Electrical and Electronics Engineers (IEEE)

B. Public and Community Service

[1] *Hungry Hungry Hackers (H3), Designing Challenges for the Hacking Competition*, 2016

C. Institute Contributions

[1] *Faculty Senate*, 09/2019–12/2021

[2] *School of Computer Science Dean Search Committee*, 08/2019–04/2020

[3] *TSO Advisory Committee*, 04/2015–12/2017

[4] *Mentoring GreyH@t*, 08/2016–present

[5] *SCS Faculty Senate*, Fall 2019

[6] *SCS Faculty Recruiting Committee*, Spring 2016, Spring 2018

[7] *SCP Faculty Recruiting Committee*, Spring 2022, Spring 2023

[8] *SCP School Advisory Committee*, Spring 2022-present

[9] *SCS Faculty Recruiting Effectiveness Committee*, Fall 2016