TAESOO KIM

CATHERINE M. AND JAMES E. ALLCHIN EARLY CAREER ASSISTANT PROFESSOR

SCHOOL OF COMPUTER SCIENCE
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

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–present*
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. Distinguished Paper Award at USENIX Security'18, 2018
2. DEFKOR00T won DEF CON CTF'18, 2018
3. VMware Early Career Faculty Grants ($35k), 2018
4. The Lockheed Martin Inspirational Young Faculty, 2018
5. NSF CAREER Award, 2018
6. 100 Future Technologies and Leaders, The National Academy of Engineering of Korea (NAEK), 2017
7. The Catherine M. and James E. Allchin Early Career Professorship, 2017
8. Mozilla Research Award ($60k), 2017
9. James D. Lester III Family Award, 2017
10. Best Student Paper at EuroSys, 2017
11. The Lockheed Excellence in Teaching Award, 2017
12. CTL/BP Junior Faculty Teaching Excellence Award, 2017
13. Class of 1969 Teaching Fellows Award, 2016
14. Microsoft Azure Research Award ($20k), 2016
15. Best Paper at SDN/NFV workshop (invited for NFV World Congress), 2016
16. Best Applied Security Research Paper (CSAW15), 2015
17. Georgia Power Professor of Excellence ($1,000), 2015
18. Best Paper at APSys15 (invited for OSR), 2015
19. 2015 Internet Defense Prize ($100k), 2015
20. Finalist to DARPA Cyber Grand Challenge ($750k, Disekt), 2015
21. GT-FIRE: Transformative Research and Education Annual Awards ($7,000), 2015
22. Samsung Scholarship ($250k for 5 years), 09/2009–06/2014
23. Korea Presidential Science Scholarship ($40k for 4 years), 03/2003–09/2008
24. 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**, The Emacs Book (Korean), `http://tsgates.github.io/emacsbook/`, 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] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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
2019	1			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	

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

[2] Wen Xu, Hyungon Moon, Sanidhya Kashyap, Po-Ning Tseng, and Taesoo Kim. Fuzzing File Systems via Two-Dimensional Input Space Exploration (to appear). *In Proceedings of the 40th IEEE Symposium on Security and Privacy (S&P 2019),* San Francisco, CA, May 2019.

[3] 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)

[4] 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, ...

[5] 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)

[6] 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)

[7] 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

[8] 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)

[9] 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)

[10] 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)

[11] 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

[12] 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

[13] 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)

[14] 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

[15] 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.

[16] 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

[17] 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

[18] 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)

[19] 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)

[20] 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)

[21] 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

[22] 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)

[23] 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

[24] 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

[25] 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

[26] 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

[27] 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

[28] 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, ...

[29] 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

[30] 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.

[31] 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

[32] 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)

[33] 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

[34] 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)

[35] 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

[36] 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

[37] 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)

[38] 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)

[39] 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)

[40] 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

[41] 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

[42] 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

[43] 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

[44] 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, . . .

[45] 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

[46] 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)

[47] 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)

[48] 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)

[49] 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.

[50] 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)

[51] 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.

[52] 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

[53] 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)

[54] 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)

[55] 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)

[56] 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

[57] 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)

[58] 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)

[59] 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)

[60] 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)

[61] 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

[62] 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)

[63] 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] 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, Auguest 2017.
DARK Reading 1/2/3, WIRED

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

[3] 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, Auguest 2014.
Phrack, ISS Source, IT Researches, Embedded

C. Other Publications and Creative Products

C.1. Patents

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

[2] 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 are hosted in Github: `https://github.com/sslab-gatech`.

[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, Android, Microsoft Windows, Chrome, Firefox, IE, PHP, OpenSSL, Python, etc. Some of recent, critical security vulnerabilities are: CVE-2016-5636, CVE-2016-5243, CVE-2016-5244, AndroidID-28620568, AndroidID-28619338, AndroidID-28620324, AndroidID-28673002, AndroidID-28673002, AndroidID-28672819, AndroidID-28672560, AndroidID-28616963, AndroidID-28616963, AndroidID-28616963, CVE-2016-4578, CVE-2016-4569, CVE-2016-4485, CVE-2016-4486, CVE-2016-4482, CVE-2016-0040 (MS16-014), IBB-PHP #113122, IBB-PHP #113120, IBB-PHP #113268, CVE-2015-6614, VU#943167, and CVE-2014-1594,

D. PRESENTATIONS (SELECTED)

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

[2] **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)

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

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

[5] **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)

[6] **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)

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

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

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

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

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

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

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

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

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

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

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

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

[19] **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)

[20] **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)

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

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

[23] **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)

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

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

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

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

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

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

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

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

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

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

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

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

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

E. Grants and Contracts

$29.1 million is awarded in total, out of which my share is **$11.3 million**.

E.1. As Principal Investigator

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

[2] **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%

[3] **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%

[4] **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%

[5] **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%

[6] **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%

[7] **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: 03/2018–02/2023
Share: 100%

[8] **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%

[9] **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%

[10] **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%

[11] **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%

[12] **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%

[13] **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%

[14] **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%

[15] **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%

[16] **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%

[17] **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%

[18] **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%

[19] **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%

[20] **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%

[21] **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%

[22] **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%

[23] **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%

[24] **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%

[25] **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%

[26] **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%

[27] **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%

[28] **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%

[29] **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%

[30] **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%

[31] **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%

[32] **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: 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%

[2] **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%

[3] **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%

[4] **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%

[5] **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%

[6] **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] **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).

[2] **Leading NSA Codebreaker Competition, 2015**: Students in CS6265, which I designed and offered in 2015, participated together in NSA Codebreaker Challenges and ranked the 1st (out of 329 universities) in the competition.

[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.

G. Societal And Policy Impacts

G.1. Research Coverage in the News

[1] *Team of Georgia Tech Students Win World Hacking Competition*:
GT CoC News Letter

[2] *Assistant Professor Taesoo Kim Wins NSF CAREER Award for Fuzzing Research*:
GT CoC News Letter

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

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

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

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

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

[8] *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, ...

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

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

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

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

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

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

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

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

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

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

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

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

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

[22] *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, ...

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

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

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

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

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

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

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

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

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

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

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

[34] *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, ...

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

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

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

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

[39] *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. Teaching

A. Courses Taught

Semester Year	Course Number	Course Title	Enrollment	CIOS Score (Participation)
Fall 2017	CS 6265 A (8803)	Information Security Lab (link)	21	4.7/5.0 (100%)
Fall 2016	CS 6265 A	Information Security Lab (link)	24	4.7/5.0 (96%)
Spring 2016	CS 3210 A	Design Operating Systems (link)	40	4.8/5.0 (100%)
Spring 2016	CS 3210 GR1	Design Operating Systems (link)	1	5.0/5.0 (100%)
Fall 2015	CS 6265 E	Information Security Lab (link)	21	4.2/5.0 (90%)
Fall 2014	CS 8803 BSS	Special Topics: Building Secure Systems (link)	16	4.8/5.0 (88%)

- *"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] **Sanidhya Kashyap**
Fall 2014-present
Publications: [2], [6], [8], [9], [10], [11], [20], [23], [32], [33], [6], [43], [45]
Status: Post-Qualifier
The Best Student Paper Award at EuroSys'17
Best Paper at APSys'15

[2] **Meng Xu**
Fall 2014-present
Publications: [1], [4], [7], [3], [13], [19], [22], [4], [40]
Status: Post-Qualifier

[3] **Mohan Kumar**
Fall 2014-present
Publications: [9], [10], [23], [35]
Status: Post-Qualifier
The Best Student Paper Award at EuroSys'17

[4] **Steffen Maass**
Fall 2015-present
Publications: [9], [10], [23], [32]
Status: Post-Qualifier
The Best Student Paper Award at EuroSys'17

[5] **Ming-wei Shih**
Fall 2014-present
Publications: [16], [25], [26], [27], [4], [35], [36]
Status: Post-Qualifier

[6] **Insu Yun**
Fall 2016-present
Publications: [4], [1], [21], [31], [34]
Status: Post-Qualifier

[7] **Wen Xu**
Fall 2016-present
Publications: [2], [11], [21]
Status: Pre-Qualifier

[8] **Jinho Jung**
Fall 2016-present
Publications: [1], [1]
Status: Pre-Qualifier

[9] **Ren Ding**
Spring 2017-present
Publications: [18]
Status: Pre-Qualifier

[10] **ChangSeok Oh**
Spring 2017-present
Publications: N/A
Status: Pre-Qualifier

[11] **Soyeon Park**
Spring 2017-present
Publications: N/A
Status: Pre-Qualifier

[12] **Fan Sang**
Fall 2018-present
Publications: N/A
Status: Pre-Qualifier

[13] **Seulbae Kim**
Fall 2018-present
Publications: N/A
Status: Pre-Qualifier

[14] **Max Wolotsky**
Fall 2016-Spring 2018
Publications: [1]
Status: Pre-Qualifier

[15] **Ashish Bijlani**
Fall 2016-Spring 2017
Publications: [13]
Status: PhD at Georgia Tech

[16] **YeongJin Jang**
Fall 2014-Summer 2017
Publications: [4], [14], [17], [29], [4], [31], [2], [40], [42], [48], [3]
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**

[17] **Kangjie Lu**
Fall 2014-Summer 2017
Publications: [1], [7], [22], [28], [4], [37], [41]
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**

[18] **Chengyu Song**
Fall 2014-Spring 2016
Publications: [1], [18], [28], [4], [34], [37], [41], [43], [44], [48], [3]
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**

[19] **Byoungyoung Lee**
Fall 2014-Spring 2016
Publications: [21], [25], [4], [33], [34], [37], [41], [43], [44], [48], [3], [52]
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: [36]
Status: MS'15
First Employment: **Oracle**

[4] **Soham Desai**
Fall 2014-Spring 2015
Publications: [36]
Status: MS'15
First Employment: **Intel**

B.3. Undergraduate Students

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

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

[2] Yeongjin Jang, *"Building Trust in the User I/O in Computer Systems"*, 07/2017.

[3] Kangjie Lu, *"Seucring Modern Systems by Preventing Information Leaks"*, 07/2017.

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

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

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

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

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

[9] Chengyu Song, *"Preventing Exploits against Memory Corruption Vulnerabilities"*, 07/2016.

[10] Byoungyoung Lee, *"Protecting Computer Systems through Eliminating or Analyzing Vulnerabilities"*, 07/2016.

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

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

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

B.5. Mentorship of Postdoctoral Fellows or Visiting Scholars

[1] **Sangho Lee**
Fall 2015-present
Publications: [4], [5], [3], [12], [14], [16], [21], [26], [29], [4], [2]
Status: Co-advised by Wenke Lee
Post Doctorate Scholarship from National Research Foundation of Korea, 2017-2018

[2] **Hong Hu**
Spring 2017-present
Publications: [1], [3]
Status: Co-advised by Wenke Lee

[3] **Hyungon Moon**
Summer 2017-Fall 2018
Publications: [2], [34]
First Employment: **Assistant Professor at UNIST (Ulsan National Institute of Science and Technology)**

[4] **Woonhak Kang**
Spring 2016-Fall 2017
Publications: [9], [15], [23], [32], [46]
Post-doctoral Research Fellowship from Sungkyunkwan University
The Best Student Paper Award at EuroSys'17
First Employment: **eBay**

[5] **Changwoo Min**
Fall 2014-Fall 2017
Publications: [6], [8], [9], [11], [15], [20], [23], [31], [32], [33], [6], [43], [45], [46]
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**

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

[7] **Heeseung Jo**
Spring 2016-Spring 2017
Publications: [9], [15]
Status: Professor at Chonbuk National University

[8] **Su Yong Kim**
Spring 2015-Spring 2016
Publications: [21]
Status: Researcher at National Security Research Institute

C. Other Teaching Activities

[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

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

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

[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

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

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

[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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[4] *SCS Faculty Recruiting Effectiveness Committee*, Fall 2016, Fall 2019