YEONGJIN JANG

Assistant Professor
School of Electrical Engineering and Computer Science
College of Engineering, Oregon State University
2500 NW Monrow Avenue, Corvallis, OR 97331

yeongjin.jang@oregonstate.edu
https://unexploitable.systems
Google Scholar
DBLP

RESEARCH INTERESTS

I am interested in computer systems security, especially in: *secure system design*, *new attack vector discovery*, *automated vulnerability discovery*, *software mitigations and defense*, *side-channel attacks*, *trusted execution environment*, *mobile security*, and *applied cryptography*.

EDUCATION

GEORGIA INSTITUTE OF TECHNOLOGY, Atlanta, GA — August 2017
Ph.D. in Computer Science
Dissertation title: Building Trust in the User I/O in Computer Systems
Advisors: Prof. Wenke Lee and Prof. Taesoo Kim

GEORGIA INSTITUTE OF TECHNOLOGY, Atlanta, GA — August 2016
M.S. in Computer Science
Specialty: *Computer Systems*

KOREA ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY, Daejeon, South Korea — February 2010
B.S. in Computer Science, *Magna Cum Laude*
Thesis title: Hardware Implementation of MD5 Brute-force Attacker
Advisor: Prof. Seungryoul Maeng

WORK EXPERIENCE

OREGON STATE UNIVERSITY, Corvallis, OR, USA — Oct 2017—Current
Assistant Professor of Computer Science

SECURITY AXIOMS, INC., Atlanta, GA, USA — May 2012 — Dec 2014
Chief Engineer — Jan 2013—Dec 2014
Software Engineering Intern — May 2012—Dec 2012

HHC, U.S. ARMY GARRISON YONGSAN (USAG-Y), Seoul, South Korea — Aug 2005—Aug 2007
Sergeant (E-4), military occupational specialty (MOS): 42L (administrative clerk)
Army Commendation Medal (ARCOM)

PUBLICATIONS

REFEREED JOURNAL ARTICLES

[1] Christopher Jelesnianski, Jinwoo Yom, Changwoo Min, and Yeongjin Jang. Securely Sharing Randomized Code that Flies. In *ACM Journal Digital Threats: Research and Practice (DTRAP)*, 2022.

[2] Dongkwan Kim, Eunsoo Kim, Mingeun Kim, Yeongjin Jang, and Yongdae Kim. Enabling the Large-Scale Emulation of Internet of Things Firmware With Heuristic Workarounds. In *IEEE Security & Privacy*, 2021.

[3] Thang Hoang, Muslum Ozgur Ozmen, Yeongjin Jang, and Attila A. Yavuz. Hardware-Supported ORAM in Effect: Practical Oblivious Search and Update on Very Large Dataset. In *Proceedings on Privacy Enhancing Technologies Symposium (PoPETs)*, January 2019.

[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. Towards Engineering a Secure Android Ecosystem: A Survey of Existing Techniques. In *ACM Computing Surveys*, volume 49, pages 38:1–38:47, August 2016.

REFEREED CONFERENCE PROCEEDINGS

[5] Jinhong Choi and Yeongjin Jang. A Survey on Sensor False Data Injection Attacks and Countermeasures in Cyber-physical and Embedded Systems (to appear). In *Proceedings of the 23rd World Conference on Information Security Applications (WISA)*, Jeju, South Korea, August 2022.

[6] Lawrence Roy, Stan Lyakhov, Yeongjin Jang, and Mike Rosulek. Practical Privacy-Preserving Authentication for SSH (to appear). In *Proceedings of the 31st USENIX Security Symposium (Security)*, Boston, MA, August 2022.

[7] Mohannad Ismail, Andrew Quach, Christopher Jelesnianski, Yeongjin Jang, and Changwoo Min. Tightly Seal Your Sensitive Pointers with PACTIGHT (to appear). In *Proceedings of the 31st USENIX Security Symposium (Security)*, Boston, MA, August 2022.

[8] Mohannad Ismail, Jinwoo Yom, Christopher Jelesnianski, Yeongjin Jang, and Changwoo Min. VIP: Safeguard Value Invariant Property for Thwarting Critical Memory Corruption Attacks. In *Proceedings of the 28th ACM Conference on Computer and Communications Security (CCS)*, Seoul, Korea, November 2021.

[9] Mingeun Kim, Dongkwan Kim, Eunsoo Kim, Suryeon Kim, Yeongjin Jang, and Yongdae Kim. FirmAE: Towards Large-Scale Emulation of IoT Firmware for Dynamic Analysis. In *Proceedings of the 2020 Annual Computer Security Applications Conference (ACSAC)*, Austin, TX, December 2020.

[10] Suhwan Song, Chengyu Song, Yeongjin Jang, and Byoungyoung Lee. CrFuzz: Fuzzing Multi-purpose Programs through Input Validation. In *Proceedings of the 2020 ACM Joint European Software Engineering Conference and Symposium (ESEC/FSE)*, Sacramento, CA, November 2020.

[11] Christopher Jelesnianski, Jinwoo Yom, Changwoo Min, and Yeongjin Jang. MARDU : Efficient and Scalable Code Re-randomization. In *Proceedings of the 13th ACM International Systems and Storage Conference (SYSTOR)*, Haifa, Israel, October 2020.

[12] Thang Hoang, Rouzbeh Behnia, Yeongjin Jang, and Attila Yavuz. MOSE: Practical Multi-User Oblivious Storage via Secure Enclaves. In *Proceedings of the 10th ACM Conference on Data and Application Security and Privacy (CODASPY)*, New Orleans, LA, March 2020.

[13] Kyungtae Kim, Dae R. Jeong, Chung Hwan Kim, Yeongjin Jang, Insik Shin, and Byoungyoung Lee. HFL: Hybrid Fuzzing on the Linux Kernel. In *Proceedings of the 2020 Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2020.

[14] Chun Sung Park, Yeongjin Jang, Seungjoo Kim, and Ki Taek Lee. Fuzzing and Exploiting Virtual Channels in Microsoft Remote Desktop Protocol for Fun and Profit. In *Black Hat Europe Briefings 2019*, London, United Kingdom, December 2019. ∗ Received $10,000 from Microsoft Bug Bounty Program (CVE-2019-1108)!

[15] Youngman Jung, Junbum Shin, and Yeongjin Jang. BlueMaster: Bypassing and Fixing Bluetooth-based Proximity Authentication. In *Black Hat Europe Briefings 2019*, London, United Kingdom, December 2019. ∗ Received $3,133.70 from Google's Vulnerability Reward Program!

[16] 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)*, Baltimore, MD, August 2018. ∗ Distinguished Paper Award Winner at USENIX Security '18!

[17] Hyunjun Park, Soyeon Kim, Seungjoo Kim, and Yeongjin Jang. soFrida - Dynamic Analysis Tool for Mobile Apps with Cloud Backend. In *DEF CON 27 Demo Labs*, Las Vegas, NV, August 2019.

[18] 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)*, Shanghai, China, October 2017. ∗ Top scored paper in SysTEX '17.

[19] 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)*, Vancouver, Canada, August 2017.

[20] Yeongjin Jang, Sangho Lee, and Taesoo Kim. Breaking Kernel Address Space Layout Randomization with Intel TSX. In *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)*, Vienna, Austria, October 2016.

[21] 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)*, Austin, TX, August 2016. ∗ Nominated as one of ten finalists in CSAW Best Applied Research Paper Award 2016.

[22] Yeongjin Jang, Sangho Lee, and Taesoo Kim. Breaking Kernel Address Space Layout Randomization with Intel TSX. In *Black Hat USA Briefings 2016*, Las Vegas, NV, August 2016.

[23] 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)*, Denver, Colorado, October 2015.

[24] 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)*, Denver, Colorado, October 2015.

[25] 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 Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2015. ∗ Won the third place award by CSAW Best Applied Research Paper Award 2015!

[26] Yeongjin Jang, Chengyu Song, Simon P. Chung, Tielei Wang, and Wenke Lee. A11y Attacks: Exploiting Accessibility in Operating Systems. In *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*, Scottsdale, Arizona, November 2014.

[27] Tielei Wang, Yeongjin Jang, Yizheng Chen, Pak Ho Chung, Billy Lau, and Wenke Lee. On the Feasibility of Large-Scale Infections of iOS Devices. In *Proceedings of the 23rd USENIX Security Symposium (Security)*, San Diego, CA, August 2014.

[28] Billy Lau, Pak Ho Chung, Chengyu Song, Yeongjin Jang, Wenke Lee, and Alexandra Boldyreva. Mimesis Aegis: A Mimicry Privacy Shield. In *Proceedings of the 23rd USENIX Security Symposium (Security)*, San Diego, CA, August 2014.

[29] Byoungyoung Lee, Yeongjin Jang, Tielei Wang, Chengyu Song, Long Lu, Taesoo Kim, and Wenke Lee. Abusing Performance Optimization Weaknesses to Bypass ASLR. In *Black Hat USA Briefings 2014*, Las Vegas, NV, August 2014.

[30] Yeongjin Jang, Tielei Wang, Byoungyoung Lee, and Billy Lau. Exploiting Unpatched iOS Vulnerabilities for Fun and Profit. In *Black Hat USA Briefings 2014*, Las Vegas, NV, August 2014.

[31] Yeongjin Jang, Simon P. Chung, Bryan D. Payne, and Wenke Lee. Gyrus: A Framework for User-Intent Monitoring of Text-based Networked Applications. In *Proceedings of the 2014 Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2014. ∗ Nominated as one of ten finalists in CSAW Best Applied Research Paper Award 2014.

[32] Billy Lau, Yeongjin Jang, Chengyu Song, Tielei Wang, Pak Ho Chung, and Paul Royal. Mactans: Injecting Malware Into iOS Devices via Malicious Chargers. In *Black Hat USA Briefings 2013*, Las Vegas, NV, August 2013.

PREPRINTS AND OTHERS

[33] Lawrence Roy, Stanislav Lyakhov, Yeongjin Jang, and Mike Rosulek. Practical privacy-preserving authentication for ssh. 2022. https://eprint.iacr.org/2022/740.

[34] Mohannad Ismail, Andrew Quach, Christopher Jelesnianski, Yeongjin Jang, and Changwoo Min. Tightly seal your sensitive pointers with pactight. arXiv, 2022. arXiv:2203.15121 [cs.CR], https://arxiv.org/abs/2203.15121.

[35] Christopher Jelesnianski, Jinwoo Yom, Changwoo Min, and Yeongjin Jang. Making Code Re-randomization Practical with MARDU. September 2019. arXiv:1909.09294 [cs.CR], https://arxiv.org/abs/1909.09294.

[36] Hsuan-Chi Kuo, Akshith Gunasekaran, Yeongjin Jang, Sibin Mohan, Rakesh B. Bobba, David Lie, and Jesse Walker. MultiK: A Framework for Orchestrating Multiple Specialized Kernels. March 2019. arXiv:1903.06889 [cs.OS], https://arxiv.org/abs/1903.06889.

[37] Thang Hoang, Muslum Ozgur Ozmen, Yeongjin Jang, and Attila A. Yavuz. Hardware-Supported ORAM in Effect: Practical Oblivious Search and Update on Very Large Dataset. March 2018. Cryptology ePrint Archive, Report 2018/247, https://eprint.iacr.org/2018/247.

[38] Yeongjin Jang. Building Trust in the User I/O in Computer Systems. *Ph.D. Thesis*, Georgia Institute of Technology, August, 2017.

GRANTED PATENTS

[39] Simon Pak Ho Chung, Wenke Lee, and Yeongjin Jang. Systems and Methods for Using Video for User and Message Authentication. September 2017. *U.S. Patent*, US20170279815A1.

TEACHING EXPERIENCE

The following is the list of courses that I taught as the head instructor, followed by the official teaching evaluation score of each. The score represented by the median of Q1/Q2 (6.0 as max), where:

Q1: The course as a whole was.
Q2: The instructor's contribution to the course was.

Operating Systems II (CS444/544 at OSU, 203 students, 5.8/5.9) ..... Fall 2021
Cyber Attacks and Defense (CS499/579 at OSU, 26 students, 5.9/5.8) ..... Fall 2021
Cyber Attacks and Defense (CS499/579 at OSU, 32 students, remote delivery, 5.9/5.9) ..... Spring 2021
Operating Systems II (CS444/544 at OSU, 199 students, remote delivery, 5.3/5.8) ..... Fall 2020
Operating Systems II (CS444/544 at OSU, 204 students, remote delivery, not evaluated) ..... Spring 2020
Cyber Security Seminar (CS 505 at OSU, 6 students, 6.0/6.0) ..... Winter 2020
Systems Security (CS419/579 at OSU, 22 students, 6.0/6.0) ..... Fall 2019
Cyber Attacks and Defense (CS419/579 at OSU, 40 students, 5.9/5.9) ..... Fall 2019
Operating Systems II (CS444/544 at OSU, 136 students, 5.8/5.9) ..... Spring 2019
Advanced Operating Systems (CS519 at OSU, 7 students, 5.8/5.8) ..... Winter 2019
Cyber Attacks and Defense (CS419/519 at OSU, 25 students, 5.7/5.9) ..... Fall 2018
Systems Security (CS419/519 at OSU, 18 students, 5.7/5.9) ..... Spring 2018
Cyber Attacks and Defense (CS419/519 at OSU, 19 students, 6.0/5.9) ..... Winter 2018

Please refer to my public teaching review scores at **RateMyProfessor.com**.

The followings are student testimonials extracted from the course evaluation reports:

> *"This was by far one of the best courses I have taken at OSU. The course content was technically very challenging, but the lecture videos, lab tutorials, and round-the-clock help from Professor Jang and the TAs allowed me to excel in the course and actually learn the material. You can tell that he cares about his students success and understanding of the course concepts. "* [CS444/544 Operating Systems II F2020]

"... the professor was kind, interactive and extremely helpful to our learning (as opposed to give-away-answers helpful). He ensured that each student succeeded. As the lectures had to be digital, he made video lectures, and released them to the class – these were as educational and helpful as possible, given the circumstances. " [CS444/544 Operating Systems II S2020]

"Dr. Jang has a great skill to explain complicated things in a simple way, so I was able to understand most of the material. The course covered a lot of material, so the knowledge we acquired was rather broad than deep, but still, I believe that the way Dr. Jang explained content was very effective, and covered many details." [CS419/579 Systems Security F2019]

"I definitely enjoyed the gamified course. Instant feedback. I would love a part 2 of the course with more advanced binary exploitation concepts." [CS419/579 Cyber Attacks and Defense F2019]

"This was easily the hardest course I took in my time at Oregon State, but with that being said I cannot understate how amazing Yeongjin was. I would take any class taught by Yeongjin due to how much you can tell he cares. It is rare for a teacher to offer a hard class and still get an ovation during the last class period." [CS419/579 Cyber Attacks and Defense F2019]

"The professor had great lectures that complemented the labs well. The course redesign definitely made the OS curriculum more cohesive ... Expectations were clear and students were given plenty of opportunities to excel." [CS444/544 Operating Systems II S2019]

"Help (in the form of asking questions and resolving code issues) from Professor Jang was quicker and more accessible more than any other professor I've had. He is very interested in his students learning." [CS444/544 Operating Systems II S2019]

"... His curriculum is meticulous and approachable, despite being incredibly challenging. I found myself accomplishing things I did not believe I could. Yeongjin is more than an amazing professor, he is also incredibly personable and is a friend to his students." [CS419/519 Advanced Operating Systems W2019]

HONORS AND AWARDS

Academic Awards

Austin Paul Engineering Faculty Award, Oregon State University	Sep 2020
2018–2019 EECS Innovative Teaching Award, Oregon State University	Jun 2019
Distinguished Paper Award [16], USENIX Security 2018	Aug 2018
Nominated as a finalist in CSAW Best Applied Research Paper Award [21]	Nov 2016
The third place award by CSAW Best Applied Research Paper Award [25]	Nov 2015
Nominated as a finalist in CSAW Best Applied Research Paper Award [31]	Nov 2014
Nominated as an RSA Security Scholar	Oct 2016
People's Choice Award (IDForWeb [39], $2,000 award) by IISP Demo Day Finale	Apr 2016
Best Demo Presenter Award [28] by the Marconi Society Young Scholars Symposium	Mar 2015

Capture-the-flag (CTF) contests

The DARPA Cyber Grand Challenge

DARPA Cyber Grand Challenge Finalist, Team `Disekt`	Aug 2016
Qualified for DARPA Cyber Grand Challenge, Team `Disekt`, $750,000 award	Jul 2015

DEF CON CTF

Qualified for DEF CON 30 CTF, Team `OSUSEC`	May 2022
6th place, DEF CON 28 CTF, Team `Samurai`	Aug 2020
8th place, DEF CON 27 CTF, Team `r00timentary`	Aug 2019
Winner DEF CON 26 CTF [1], Team `DEFKOR00t`	Aug 2018
3rd place, DEF CON 24 CTF, Team `DEFKOR`	Aug 2016
Winner, DEF CON 23 CTF, Team `DEFKOR`	Aug 2015

[1] DEF CON CTF (Capture The Flag) is the most competitive hacking contest in the world, where world best hackers are competing each other.

3rd place, DEF CON 18 CTF, Team `KAIST&POSTECH`) Aug 2010

6th place, DEF CON 17 CTF, Team `Song of Freedom`) Aug 2009

2nd place, DEF CON 16 oCTF, Team `DDUCK`) Aug 2008

NSA Codebreaker Challenge

3rd place, The 2021 NSA Codebreaker Challenge (Oregon State University) Jan 2022

3rd place, The 2020 NSA Codebreaker Challenge (Oregon State University) Jan 2021

3rd place, The 2019 NSA Codebreaker Challenge (Oregon State University) Jan 2020

Winner, The 2018 NSA Codebreaker Challenge (Oregon State University) Jan 2019

DoE CyberForce Competition

7th national, The Department of Energy Cyberforce Competition Nov 2021

1st at PNNL, 6th national, The Department of Energy Cyberforce Competition Nov 2019

1st at PNNL, 3rd national, The Department of Energy Cyberforce Competition Dec 2018

1st at PNNL, 4th national, The Department of Energy Cyber Defense Competition Apr 2018

Bug Bounties

Authentication Bypass in Android Smart Lock ($3,133.70) [15], Google May 2019

Information leak in Microsoft Remote Desktop Protocol ($10,000) [14], Microsoft Apr 2019

Three integer overflow vulnerabilities in PHP ($1,500) [21], the Internet Bug Bounty Jun 2016

An Integer Overflow Vulnerability in Python zipimport ($1,000) [21], the Internet Bug Bounty Apr 2016

Automatic URL redirection vulnerability ($500), Facebook Mar 2014

Scholarships

Scholarship for Doctoral Study, The Kwanjeong Educational Foundation 2010 – 2015

KAIST Undergraduate Research Program Scholarship 2008

Scholarship for Undergraduate Study, Korea Science and Engineering Foundation 2003 – 2009

PROFESSIONAL ACTIVITIES

Program Committee Member

Annual Computer Security Applications Conference (ACSAC) 2022

USENIX Security Symposium 2021

Black Hat Asia Review Board 2021, 2022

ACM ASIA Conference on Computer and Communications Security (ASIACCS) 2018, 2019, 2020, 2021

World Conference on Information Security Applications (WISA) 2018, 2019, 2020, 2022

Organizing Committee Member

Registration Chair, ACM Computer and Communications Security (CCS) 2022

Web Chair, ACM Computer and Communications Security (CCS) 2021

Journal Reviewer

ACM Transactions on Privacy and Security (TOPS) 2021

IEEE Transactions on Dependable and Secure Computing (TDSC) 2020
IEEE Transactions on Cloud Computing (TCC) 2019
IEEE Transactions on Information Forensics and Security (TIFS) 2017

NSF Panel Reviewer

NSF Secure and Trustworthy Computing (SaTC) panel 2022
NSF Secure and Trustworthy Computing (SaTC) panel 2020

External Reviewer

USENIX Annual Technical Conference (ATC) 2018
IEEE Symposium on Security and Privacy (Oakland) 2018
Network and Distributed System Security Symposium (NDSS) 2015, 2016, 2017
USENIX Security Symposium (Security) 2011, 2015, 2016, 2017
ACM Conference on Computer and Communications Security (CCS) 2014, 2015, 2016
IEEE European Symposium on Security and Privacy (EuroS&P) 2016
The Workshop on System Software for Trusted Execution (SysTEX) 2016
European Symposium on Research in Computer Security (ESORICS) 2014, 2015
ACM Symposium On Usable Privacy and Security (SOUPS) 2014

INVITED TALKS

Confidential and Private Computing using ORAM and TEE [3, 12]

Presented at National Security Research Institute Daejeon, South Korea (online), Apr 2021.
Presented at POSTECH Pohang, South Korea (online), Apr 2021.
Presented at Samsung Security Tech Forum Seoul, South Korea (online), Aug 2020.

Efficient and Scalable Code Randomization [35]

Presented at Samsung Research Seoul, South Korea, Dec 2019.
Presented at National Security Research Institute Daejeon, South Korea, Dec 2019.

Myths and Facts in Encryption

Presented at the 2019 Economic Summit by FI-TEAM Tigard, OR, Jan 2019.

Myths and Facts in User Authentication

Presented at the 2018 Economic Summit by FI-TEAM Tigard, OR, Mar 2018.

SGX-Bomb: Locking Down the Processor via Rowhammer Attack [18]

Presented at the PoC conference Seoul, South Korea, Nov 2017.
Presented at the 2nd SysTEX Workshop Shanghai, China, Oct 2017.

Dynamic Malware Analysis Framework

Presented in Intel ISTC-ARSA Retreat at Georgia Tech Atlanta, GA, Jun 2017.

Protecting Computing System Interactions [38]

Seminar at the University of Virginia Charlottesville, VA, Mar 2017.
Seminar at the University of Southern California Los Angeles, CA, Mar 2017.

Seminar at the Pennsylvania State University — State College, PA, Mar 2017.
Seminar at Texas A&M University — College Station, TX, Mar 2017.
Seminar at Oregon State University — Corvallis, OR, Mar 2017.
Seminar at the University of Oregon — Eugene, OR, Mar 2017.
Seminar at the University of Georgia — Athens, GA, Feb 2017.
IISP Seminar at the Georgia Institute of Technology — Atlanta, GA, Feb 2017.

Hacking in Darkness: Return-oriented Programming against Secure Enclaves [19]

Seminar at Intel Labs — Hillsboro, OR, Feb 2017.

Breaking Kernel Address Space Layout Randomization with Intel TSX [20, 22]

Presented at the 23rd ACM CCS 2016 [20] — Vienna, Austria, Oct 2016.
Presented at the Black Hat USA Briefings 2016 [22] — Las Vegas, NV, Aug 2016.

Tying Public Key to Person with IDforWeb [39]

Presented at the IISP Demo Day Finale 2016 — Atlanta, GA, Apr 2016.

A11y Attacks: Exploiting Accessibility in Operating Systems [26]

Information Security Seminar at Samsung Electronics — Suwon, South Korea, Dec 2014.
Presented at the 21st ACM CCS 2014 — Scottsdale, AZ, Nov 2014.

Security Overlay (Mimesis Aegis): A Mimicry Privacy Shield [28]

Information Security Seminar at NCC Group — Atlanta, GA, Mar 2015.
Demonstrated at the Marconi Society Young Scholars Symposium — Atlanta, GA, Mar 2015.
Information Security Seminar at Yonsei Univesity — Seoul, South Korea, Dec 2014.

Exploiting Unpatched iOS Vulnerabilities for Fun and Profit [30]

IEEE Seminar at Georgia State University — Atlanta, GA, Sep 2014.
Presented at the Black Hat USA Briefings 2014 — Las Vegas, NV, Aug 2014.
Information Security Seminar at Korea University — Seoul, South Korea, Jul 2014.
Information Security Seminar at KAIST — Daejeon, South Korea, Jul 2014.
Information Security Seminar at Yonsei University — Seoul, South Korea, Jul 2014.

Gyrus: A Framework for User-Intent Monitoring of Text-based Networked Applications [31]

Presented at the 21st NDSS — San Diego, CA, Feb 2014.
Information Security Seminar at Korea University — Seoul, South Korea, Dec 2013.
Information Security Seminar at KAIST — Daejeon, South Korea, Dec 2013.

Mactans: Injecting Malware Into iOS Devices via Malicious Chargers [32]

Information Security Seminar at Korea University — Seoul, South Korea, Dec 2013.
Information Security Seminar at KAIST — Daejeon, South Korea, Dec 2013.
Presented at the Black Hat USA Briefings 2013 — Las Vegas, NV, Aug 2013.

CloudCapsule: Protecting Confidential Data Using VM Check-pointing and Restore

Presented at the 2013 DoD ASD Cyber Security SBIR Workshop — Arlington, VA, Jul 2012.

LIST OF REFERENCES

Dr. Wenke Lee, Ph.D.

John P. Imlay Jr. Chair Professor of Computer Science
Executive Director, Institute for Information Security and Privacy (IISP)
Georgia Institute of Technology, Atlanta, GA
Homepage : http://wenke.gtisc.gatech.edu
Phone : 404-385-2879
Email : wenke@cc.gatech.edu

Dr. Taesoo Kim, Ph.D.

Professor of Computer Science
Director, Georgia Tech System Software and Security (GTS3) Center
Georgia Institute of Technology, Atlanta, GA
Homepage : https://taesoo.kim
Phone : 404-385-2934
Email : taesoo@gatech.edu

Dr. Yongdae Kim, Ph.D.

Professor of Electrical Engineering
Professor of Graduate School of Information Security
Director, KAIST Cyber Security Research Center
Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea
Homepage : http://syssec.kaist.ac.kr/~yongdaek/
Phone : +82-42-350-7430
Email : yongdaek@kaist.ac.kr

Dr. Kang Li, Ph.D.

Director, Institute for Cybersecurity and Privacy (ICSP)
University of Georgia, Athens, GA
Homepage : http://cobweb.cs.uga.edu/~kangli/
Phone : 706-583-0395
Email : kangli@cs.uga.edu

Last updated: July 6, 2022