

# YEONGJIN JANG, PH.D.

Staff Research Scientist  
Google DeepMind  
2000 N. Shoreline Blvd, Mountain View, CA, 94043

✉ [dr.yeongjin.jang@gmail.com](mailto:dr.yeongjin.jang@gmail.com)  
🌐 <https://www.unexploitable.systems>  
🔖 [Google Scholar](#)  
🔖 [LinkedIn](#)

## RESEARCH INTERESTS

---

I am interested in using Generative AI to advance autonomous vulnerability detection and patching, overcoming limitations of traditional static/dynamic analysis techniques such as symbolic execution, fuzzing, and concolic testing. I also work on developing novel cyber-attack methodologies, exploit mitigation strategies, secure systems design, trusted execution environments, crypto-system co-design, architectural side-channel attacks, and mobile security.

## ACHIEVEMENT SUMMARY

---

- The DARPA/ARPA-H AI Cyber Challenge (AIXCC) Champion (Team Atlanta, \$4M and \$2M awards)
  - Focusing on AI-driven vulnerability detection and mitigation
- The DARPA Cyber Grand Challenge Finalist (Disekt, \$750K award)
  - Focusing on dynamic program analysis such as fuzzing and concolic execution
- The champion of the DEF CON CTF (2x Winner, DEFKOR in 2015 and DEFKOR00T in 2018)
  - Focusing on vulnerability research, exploit development, and patching
- Served as PI or Co-PI on over \$8M research grants
  - Focusing on program analysis, and security testing of RTOS, Drone/UAS, Nuclear facility, etc.
- Six Black Hat USA/Europe Briefings presentations
- 18 top-tier academic conference proceedings (USENIX Security, ACM CCS, NDSS, FSE, and ASPLOS)
- Pwned iPhone twice (charger attack in 2013 [7] and rooting in 2014 [5])
- Pwned Intel CPU twice (DrK attack in 2016 [17] and SGX-Bomb in 2017 [15])
- Pwned iOS, Android, Microsoft Windows, GNOME in Linux at once via a11y attack [22])
- Winner of the 2018 NSA Codebreaker Challenge (OSUSEC)
- The USENIX Security 2018 Distinguished Paper Award (QSYM [14], top-cited performant concolic executor)
- The Frontier of Science Award (\$25,000) in 2023 [14].

## EDUCATION

---

GEORGIA INSTITUTE OF TECHNOLOGY, Atlanta, GA	Aug 2010 — Aug 2017
Ph.D. in Computer Science (Advisors: Prof. Wenke Lee and Prof. Taesoo Kim)	August 2017
Dissertation Title: Building Trust in the User I/O in Computer Systems	
M.S. in Computer Science (Specialty: <i>Computer Systems</i> )	August 2016
KOREA ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY, Daejeon, South Korea	Mar 2003 — Feb 2010
B.S. in Computer Science, <i>Magna Cum Laude</i>	
Thesis Title: Hardware Implementation of MD5 Brute-force Attacker (on FPGA)	

## WORK EXPERIENCE

---

- Google DeepMind**, Mountain View, CA, USA *Oct 2025 – Present*  
*Staff Research Scientist*
- Samsung Research America**, Mountain View, CA, USA *Aug 2023 – Oct 2025*  
*Principal Software Engineer, Vulnerability Research*
- Conduct autonomous vulnerability research by combining traditional static/dynamic analysis with large-language models (LLMs) on production environments (large open-source Java projects, e.g., apache commons, Jenkins, Spring, etc.).
  - Developed techniques in reachability analysis, concolic execution, hybrid fuzzing, and LLM-based techniques, as part of the DARPA/H-ARPA-H AI Cyber Challenge (Team Atlanta).
- Oregon State University**, Corvallis, OR, USA *Jul 2017 – Aug 2024*  
*Courtesy Appointment* *Jun 2023 – Aug 2024*  
*Tenure-track Assistant Professor, Computer Science* *Oct 2017 – Jun 2023*  
*Courtesy Appointment* *Jul 2017 – Oct 2017*
- Directed externally funded research projects in cybersecurity, managing over \$8M in grants.
  - Advised 15 graduate students, six undergraduate researchers, and two government professionals.
  - Specialized in secure system design, automated vulnerability discovery, exploit mitigation, trusted execution environments, and crypto-system co-design.
- Georgia Institute of Technology**, Atlanta, GA, USA
- Graduate Research Assistant* *Jan 2015 – Aug 2017*  
*Graduate Research Assistant* *Aug 2010 – May 2012*
- Security Axioms, Inc.**, Atlanta, GA, USA *May 2012 – Dec 2014*  
*Chief Engineer* *Jan 2013 – Dec 2014*  
*Software Engineering Intern* *May 2012 – Dec 2012*
- Developed secure storage solutions for virtual machine and iOS sandbox environments.
  - Led projects funded by the Army Research Office (ARO) through SBIR Phase I and II.
- Independent Cybersecurity Contractor**, Daejeon, South Korea *Jan 2008 – Aug 2010*
- Executed penetration tests and security assessments for South Korean government and financial institutions.
  - Identified and reported over 100 security vulnerabilities across more than 400 systems.
- HHC, U.S. Army Garrison Yongsan (USAG-Y)**, Seoul, South Korea *Aug 2005 – Aug 2007*
- Completed mandatory military service as a Korean Augmentation to the U.S. Army (KATUSA).

## PUBLICATIONS

---

18 papers in top-tier conferences (*USENIX Security, CCS, NDSS, ASPLOS, FSE*)

6 presentations in *Black Hat USA/Europe Briefings*

### REFEREED INDUSTRY CONFERENCE ARTICLES

- [1] **Fuzzing and Exploiting Virtual Channels in Microsoft Remote Desktop Protocol for Fun and Profit.**  
Chun Sung Park, Yeongjin Jang, Seungjoo Kim, and Ki Taek Lee.  
In *Black Hat Europe Briefings 2019*, London, United Kingdom, December 2019.  
\* [Received \\$10,000 from Microsoft Bug Bounty Program \(CVE-2019-1108\)](#)!
- [2] **BlueMaster: Bypassing and Fixing Bluetooth-based Proximity Authentication.**  
Youngman Jung, Junbum Shin, and Yeongjin Jang.  
In *Black Hat Europe Briefings 2019*, London, United Kingdom, December 2019.  
\* [Received \\$3,133.70 from Google's Vulnerability Reward Program](#)!
- [3] **soFrida - Dynamic Analysis Tool for Mobile Apps with Cloud Backend.**  
Hyunjun Park, Soyeon Kim, Seungjoo Kim, and Yeongjin Jang.  
In *DEF CON 27 Demo Labs*, Las Vegas, NV, August 2019.
- [4] **Breaking Kernel Address Space Layout Randomization with Intel TSX.**  
Yeongjin Jang, Sangho Lee, and Taesoo Kim.  
In *Black Hat USA Briefings 2016*, Las Vegas, NV, August 2016.
- [5] **Exploiting Unpatched iOS Vulnerabilities for Fun and Profit.**  
Yeongjin Jang, Tielei Wang, Byoungyoung Lee, and Billy Lau.  
In *Black Hat USA Briefings 2014*, Las Vegas, NV, August 2014.  
\* [Acknowledged as CVE-2014-4372](#)!
- [6] **Abusing Performance Optimization Weaknesses to Bypass ASLR.**  
Byoungyoung Lee, Yeongjin Jang, Tielei Wang, Chengyu Song, Long Lu, Taesoo Kim, and Wenke Lee.  
In *Black Hat USA Briefings 2014*, Las Vegas, NV, August 2014.
- [7] **Mactans: Injecting Malware Into iOS Devices via Malicious Chargers.**  
Billy Lau, Yeongjin Jang, Chengyu Song, Tielei Wang, Pak Ho Chung, and Paul Royal.  
In *Black Hat USA Briefings 2013*, Las Vegas, NV, August 2013.

### REFEREED CONFERENCE PROCEEDINGS

- [1] **Enforcing C/C++ Type and Scope at Runtime for Control-Flow and Data-Flow Integrity.**  
Mohannad Ismail, Christopher Jelesnianski, Yeongjin Jang, Changwoo Min, and Wenjie Xiong.  
In *Proceedings of the 29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, La Jolla, CA, April 2024.
- [2] **GENESIS: A Generalizable, Efficient, and Secure Intra-kernel Privilege Separation.**  
Seongman Lee, Seoye Kim, Chihyun Song, Byeongsu Woo, Eunyeong Ahn, Junsu Lee, Yeongjin Jang, Jinsoo Jang, Hojoon Lee, and Brent ByungHoon Kang.  
In *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing (SAC)*, Avila, Spain, April 2024.
- [3] **SGX-USB: Secure USB I/O Path for Secure Enclaves.**  
Yeongjin Jang and Sejin Keem.  
In *Proceedings of the 57th Hawaii International Conference on System Sciences (HICSS)*, Waikiki, HI, January 2024.
- [4] **Protect the System Call, Protect (most of) the World with BASTION.**  
Christopher Jelesnianski, Mohannad Ismail, Yeongjin Jang, Dan Williams, and Changwoo Min.  
In *Proceedings of the 28th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, Vancouver, Canada, March 2023.

- [5] **A Survey on Sensor False Data Injection Attacks and Countermeasures in Cyber-physical and Embedded Systems.**  
Jinhong Choi and **Yeongjin Jang**.  
In *Proceedings of the 23rd World Conference on Information Security Applications (WISA)*, Jeju, South Korea, August 2022.
- [6] **Practical Privacy-Preserving Authentication for SSH.**  
Lawrence Roy, Stan Lyakhov, **Yeongjin Jang**, and Mike Rosulek.  
In *Proceedings of the 31st USENIX Security Symposium (Security)*, Boston, MA, August 2022.
- [7] **Tightly Seal Your Sensitive Pointers with PACTIGHT.**  
Mohannad Ismail, Andrew Quach, Christopher Jelesnianski, **Yeongjin Jang**, and Changwoo Min.  
In *Proceedings of the 31st USENIX Security Symposium (Security)*, Boston, MA, August 2022.
- [8] **VIP: Safeguard Value Invariant Property for Thwarting Critical Memory Corruption Attacks.**  
Mohannad Ismail, Jinwoo Yom, Christopher Jelesnianski, **Yeongjin Jang**, and Changwoo Min.  
In *Proceedings of the 28th ACM Conference on Computer and Communications Security (CCS)*, Seoul, Korea, November 2021.
- [9] **FirmAE: Towards Large-Scale Emulation of IoT Firmware for Dynamic Analysis.**  
Mingeun Kim, Dongkwan Kim, Eunsoo Kim, Suryeon Kim, **Yeongjin Jang**, and Yongdae Kim.  
In *Proceedings of the 2020 Annual Computer Security Applications Conference (ACSAC)*, Austin, TX, December 2020.
- [10] **CrFuzz: Fuzzing Multi-purpose Programs through Input Validation.**  
Suhwan Song, Chengyu Song, **Yeongjin Jang**, and Byoungyoung Lee.  
In *Proceedings of the 2020 ACM Joint European Software Engineering Conference and Symposium (ESEC/FSE)*, Sacramento, CA, November 2020.
- [11] **MARDU : Efficient and Scalable Code Re-randomization.**  
Christopher Jelesnianski, Jinwoo Yom, Changwoo Min, and **Yeongjin Jang**.  
In *Proceedings of the 13th ACM International Systems and Storage Conference (SYSTOR)*, Haifa, Israel, October 2020.
- [12] **MOSE: Practical Multi-User Oblivious Storage via Secure Enclaves.**  
Thang Hoang, Rouzbeh Behnia, **Yeongjin Jang**, and Attila Yavuz.  
In *Proceedings of the 10th ACM Conference on Data and Application Security and Privacy (CODASPY)*, New Orleans, LA, March 2020.
- [13] **HFL: Hybrid Fuzzing on the Linux Kernel.**  
Kyungtae Kim, Dae R. Jeong, Chung Hwan Kim, **Yeongjin Jang**, Insik Shin, and Byoungyoung Lee.  
In *Proceedings of the 2020 Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2020.
- [14] **QSYM: A Practical Concolic Execution Engine Tailored for Hybrid Fuzzing.**  
Insu Yun, Sangho Lee, Meng Xu, **Yeongjin Jang**, and Taesoo Kim.  
In *Proceedings of the 27th USENIX Security Symposium (Security)*, Baltimore, MD, August 2018.  
\* [Distinguished Paper Award Winner at USENIX Security '18!](#)
- [15] **SGX-Bomb: Locking Down the Processor via Rowhammer Attack.**  
**Yeongjin Jang**, Jaehyuk Lee, Sangho Lee, and Taesoo Kim.  
In *Proceedings of the 2nd Workshop on System Software for Trusted Execution (SysTEX)*, Shanghai, China, October 2017.  
\* [Top scored paper in SysTEX '17.](#)
- [16] **Hacking in Darkness: Return-oriented Programming against Secure Enclaves.**  
Jaehyuk Lee, Jinsoo Jang, **Yeongjin Jang**, Nohyun Kwak, Yeseul Choi, Changho Choi, Taesoo Kim, Marcus Peinado, and Brent B. Kang.  
In *Proceedings of the 26th USENIX Security Symposium (Security)*, Vancouver, Canada, August 2017.
- [17] **Breaking Kernel Address Space Layout Randomization with Intel TSX.**  
**Yeongjin Jang**, Sangho Lee, and Taesoo Kim.  
In *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)*, Vienna, Austria, October 2016.
- [18] **APISAN: Sanitizing API Usages through Semantic Cross-checking.**

Insu Yun, Changwoo Min, Xujie Si, **Yeongjin Jang**, Taesoo Kim, and Mayur Naik.  
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.](#)

- [19] **UCognito: Private Browsing without Tears.**  
Meng Xu, **Yeongjin Jang**, Xinyu Xing, Taesoo Kim, and Wenke Lee.  
In *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, Denver, Colorado, October 2015.
- [20] **Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations.**  
Hongil Kim, Dongkwan Kim, Minhee Kwon, Hyungseok Han, **Yeongjin Jang**, Dongsu Han, Taesoo Kim, and Yongdae Kim.  
In *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, Denver, Colorado, October 2015.
- [21] **Preventing Use-after-free with Dangling Pointers Nullification.**  
Byoungyoung Lee, Chengyu Song, **Yeongjin Jang**, Tielei Wang, Taesoo Kim, Long Lu, and Wenke Lee.  
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!](#)
- [22] **A11y Attacks: Exploiting Accessibility in Operating Systems.**  
**Yeongjin Jang**, Chengyu Song, Simon P. Chung, Tielei Wang, and Wenke Lee.  
In *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*, Scottsdale, Arizona, November 2014.
- [23] **On the Feasibility of Large-Scale Infections of iOS Devices.**  
Tielei Wang, **Yeongjin Jang**, Yizheng Chen, Pak Ho Chung, Billy Lau, and Wenke Lee.  
In *Proceedings of the 23rd USENIX Security Symposium (Security)*, San Diego, CA, August 2014.
- [24] **Mimesis Aegis: A Mimicry Privacy Shield.**  
Billy Lau, Pak Ho Chung, Chengyu Song, **Yeongjin Jang**, Wenke Lee, and Alexandra Boldyreva.  
In *Proceedings of the 23rd USENIX Security Symposium (Security)*, San Diego, CA, August 2014.
- [25] **Gyrus: A Framework for User-Intent Monitoring of Text-based Networked Applications.**  
**Yeongjin Jang**, Simon P. Chung, Bryan D. Payne, and Wenke Lee.  
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.](#)

## REFEREED JOURNAL ARTICLES

- [1] **Securely Sharing Randomized Code that Flies.**  
Christopher Jelesnianski, Jinwoo Yom, Changwoo Min, and **Yeongjin Jang**.  
In *ACM Journal Digital Threats: Research and Practice (DTRAP)*, 2022.
- [2] **Enabling the Large-Scale Emulation of Internet of Things Firmware With Heuristic Workarounds.**  
Dongkwan Kim, Eunsoo Kim, Mingeun Kim, **Yeongjin Jang**, and Yongdae Kim.  
In *IEEE Security & Privacy*, 2021.
- [3] **Hardware-Supported ORAM in Effect: Practical Oblivious Search and Update on Very Large Dataset.**  
Thang Hoang, Muslum Ozgur Ozmen, **Yeongjin Jang**, and Attila A. Yavuz.  
In *Proceedings on Privacy Enhancing Technologies Symposium (PoPETs)*, January 2019.
- [4] **Towards Engineering a Secure Android Ecosystem: A Survey of Existing Techniques.**  
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.  
In *ACM Computing Surveys*, volume 49, pages 38:1–38:47, August 2016.

## PREPRINTS AND OTHERS

- [1] **A Comprehensive Survey of Unmanned Aerial Systems' Risks and Mitigation Strategies.**  
Sharad Shrestha, Mohammed Ababneh, Satyajayant Misra, Jr. Henry M. Cathey, Roopa Vishwanathan, Matt Jansen, Jinhong Choi, Rakesh Bobba, and Yeongjin Jang. 2025. URL <https://arxiv.org/abs/2506.10327>.
- [2] **Tightly seal your sensitive pointers with pactight.**  
Mohannad Ismail, Andrew Quach, Christopher Jelesnianski, Yeongjin Jang, and Changwoo Min. arXiv, March 2022. doi: 10.48550/ARXIV.2203.15121. URL <https://arxiv.org/abs/2203.15121>.
- [3] **Practical privacy-preserving authentication for ssh.**  
Lawrence Roy, Stanislav Lyakhov, Yeongjin Jang, and Mike Rosulek. June 2022. URL <https://eprint.iacr.org/2022/740>.
- [4] **Making Code Re-randomization Practical with MARDU.**  
Christopher Jelesnianski, Jinwoo Yom, Changwoo Min, and Yeongjin Jang. September 2019. arXiv:1909.09294 [cs.CR], <https://arxiv.org/abs/1909.09294>.
- [5] **MultiK: A Framework for Orchestrating Multiple Specialized Kernels.**  
Hsuan-Chi Kuo, Akshith Gunasekaran, Yeongjin Jang, Sibin Mohan, Rakesh B. Bobba, David Lie, and Jesse Walker. March 2019. arXiv:1903.06889 [cs.OS], <https://arxiv.org/abs/1903.06889>.
- [6] **Hardware-Supported ORAM in Effect: Practical Oblivious Search and Update on Very Large Dataset.**  
Thang Hoang, Muslum Ozgur Ozmen, Yeongjin Jang, and Attila A. Yavuz. March 2018. Cryptology ePrint Archive, Report 2018/247, <https://eprint.iacr.org/2018/247>.
- [7] **Building Trust in the User I/O in Computer Systems.**  
Yeongjin Jang and Ph.D. Thesis.  
Georgia Institute of Technology, August, 2017.

## GRANTED PATENTS

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

## HONORS AND AWARDS

---

### Academic Awards

Frontier of Science Award [14], International Congress of Basic Science (\$25,000 award)	Jul 2023
Austin Paul Engineering Faculty Award, Oregon State University	Sep 2020
2018–2019 EECS Innovative Teaching Award, Oregon State University	Jun 2019
Distinguished Paper Award [14], USENIX Security 2018	Aug 2018
Nominated as a finalist in CSAW Best Applied Research Paper Award [18]	Nov 2016
The third place award by CSAW Best Applied Research Paper Award [21]	Nov 2015
Nominated as a finalist in CSAW Best Applied Research Paper Award [25]	Nov 2014
Nominated as an RSA Security Scholar	Oct 2016
People's Choice Award (IDForWeb [1], \$2,000 award) by IISP Demo Day Finale	Apr 2016
Best Demo Presenter Award [24] by the Marconi Society Young Scholars Symposium	Mar 2015

### Capture-the-flag (CTF) contests

### *The DARPA/ARPA-H AI Cyber Challenge (AIxCC)*

The winner of the AI Cyber Challenge Final Competition, Team Atlanta \$4,000,000 award Aug 2025  
Qualified for the AI Cyber Challenge Final Competition, Team Atlanta, \$2,000,000 award Aug 2024

### *The DARPA Cyber Grand Challenge*

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

### *DEF CON CTF*

16th place, DEF CON 30 CTF, Team OSUSEC Aug 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 <sup>1</sup>, Team DEFKOR00t Aug 2018  
3rd place, DEF CON 24 CTF, Team DEFKOR Aug 2016  
**Winner**, DEF CON 23 CTF, Team DEFKOR Aug 2015  
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*

2nd place, The 2022 NSA Codebreaker Challenge (Oregon State University) Jan 2023  
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  
**Winner**, The 2016 NSA Codebreaker Challenge (Georgia Institute of Technology) Jan 2017

### *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) [2], Google May 2019  
Information leak in Microsoft Remote Desktop Protocol (\$10,000) [1], Microsoft Apr 2019  
Three integer overflow vulnerabilities in PHP (\$1,500) [18], the Internet Bug Bounty Jun 2016

---

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

An Integer Overflow Vulnerability in Python zipimport (\$1,000) [18], the Internet Bug Bounty	Apr 2016
Automatic URL redirection vulnerability (\$500), Facebook	Mar 2014

### Scholarships

Scholarship for Doctoral Study, The Kwanjeong Educational Foundation (\$25,000/year for 5 years)	2010 – 2015
KAIST Undergraduate Research Program Scholarship	2008
Scholarship for Undergraduate Study, Korea Science and Engineering Foundation	2003 – 2009

## PROFESSIONAL ACTIVITIES

---

### Program Committee Member

USENIX WOOT Conference on Offensive Technologies (WOOT)	2024
Annual Computer Security Applications Conference (ACSAC)	2022
USENIX Security Symposium (Security)	2021
Black Hat Asia Review Board	2021, 2022, 2023
ACM ASIA Conference on Computer and Communications Security (ASIACCS)	2018, 2019, 2020, 2021
World Conference on Information Security Applications (WISA)	2018, 2019, 2020, 2022
IEEE Silicon Valley Cybersecurity Conference (SVCC)	2023

### 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, 2023
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

---

### **Panel discussion at Samsung Security Tech Forum**

Presented at Samsung Security Tech Forum Seoul, South Korea, Sep 2024.

### **How Hackers Drive Security Innovation**

Presented at Samsung Security Tech Forum Seoul, South Korea, Aug 2023.

### **Defeating Emerging Attacks with State-of-the-art Technologies [6, 7]**

Presented at Samsung Research Seoul, South Korea, Sep 2022.

### **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.

Keynote Speech at Samsung Security Tech Forum Seoul, South Korea (online), Aug 2020.

### **Efficient and Scalable Code Randomization [4]**

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 [15]**

Keynote Speech 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 [7]**

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 [16]**  
Seminar at Intel Labs Hillsboro, OR, Feb 2017.
- Breaking Kernel Address Space Layout Randomization with Intel TSX [17, 4]**  
Presented at the 23rd ACM CCS 2016 [17] Vienna, Austria, Oct 2016.  
Presented at the Black Hat USA Briefings 2016 [4] Las Vegas, NV, Aug 2016.
- Tying Public Key to Person with IDforWeb [1]**  
Presented at the IISP Demo Day Finale 2016 Atlanta, GA, Apr 2016.
- A11y Attacks: Exploiting Accessibility in Operating Systems [22]**  
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 [24]**  
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 [5]**  
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 [25]**  
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 [7]**  
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.

## MANAGED RESEARCH GRANTS

---

Funding Totals: **\$8,892,640**, My Share: **\$1,115,573**.

**1. Study on Security/Reliability Test and Evaluation Method for Secure Real-time Operating System**

Collaborators: Yeongjin Jang (**PI**) and Byoungyoung Lee.

Agency: Agency for Defense Development of South Korea

Total U.S. Dollar Amount: **\$449,920** (My share: **\$288,692**)

Period of Contract: 08/2018—12/2020

**2. Research on Binary Static Analysis Technique via Concolic Testing**

Collaborators: Yeongjin Jang (**PI**).

Agency: National Security Research Institute of South Korea

Total U.S. Dollar Amount: **\$85,000** (My share: **\$85,000**)

Period of Contract: 03/2019—02/2020

**3. Thwarting Memory Safety Violation by Stack Layout Randomization**

Collaborators: Yeongjin Jang (**PI**).

Agency: KAIST

Total U.S. Dollar Amount: **\$29,484** (My share: **\$29,484**)

Period of Contract: 01/2020—06/2021

**4. A38 A11L.UAS.78: UAS Cyber Security and Safety Lit Review**

Collaborators: Rakesh Bobba (**PI**), Yeongjin Jang (**Co-PI**), and Houssam Abbas

Agency: Federal Aviation Administration (FAA)

Total U.S. Dollar Amount: **\$200,000** (My share: **\$61,568**)

Period of Contract: 08/2020—07/2021

**5. Dynamic Risk Assessment for Nuclear Cybersecurity**

Collaborators: Camille Palmer (**PI**), Rakesh Bobba, and Yeongjin Jang (**Co-PI**)

Agency: Nuclear Regulatory Commission (NRC)

Total U.S. Dollar Amount: **\$500,000** (My share: **\$131,075**)

Period of Contract: 04/2021—03/2024

**6. A51 Best Engineering Practices for Automated Systems**

Collaborators: Houssam Abbas (**PI**), Rakesh Bobba, Yeongjin Jang (**Co-PI**), Jinsub Kim, and Arun Natarajan

Agency: Federal Aviation Administration (FAA)

Total U.S. Dollar Amount: **\$1,782,450** (My share: **\$233,735**)

Period of Contract: 08/2021—08/2024

**7. Thwarting Memory Safety Violation by Stack Layout Randomization**

Collaborators: Yeongjin Jang (**PI**)

Agency: KAIST

Total U.S. Dollar Amount: **\$33,777** (My share: **\$33,777**)

Period of Contract: 05/2021—04/2022

**8. Cybersecurity and STEM Research Experiences for Navy ROTC**

Collaborators: Rakesh Bobba (**PI**), Dave Nevin, and Yeongjin Jang (**Co-PI**)

Agency: Office of Naval Research (ONR)  
Total U.S. Dollar Amount: **\$200,000** (My share: **\$45,748**)  
Period of Contract: 09/2021—09/2022

**9. A58 Illustrate the Need for UAS Cybersecurity Oversight and Risk Management**

Collaborators: Rakesh Bobba (**PI**), Yeongjin Jang (**Co-PI**), and Houssam Abbas  
Agency: Federal Aviation Administration (FAA)  
Total U.S. Dollar Amount: **\$812,302** (My share: **\$182,066**)  
Period of Contract: 09/2021—09/2022

**10. CyberCorps Scholarship for Service: A Clinical Rotation Approach to Professional Cybersecurity Workforce Development**

Collaborators: Rakesh Bobba (**PI**), Dave Nevin, Yeongjin Jang (**Co-PI**), and Sanghyun Hong  
Agency: National Science Foundation (NSF)  
Total U.S. Dollar Amount: **\$4,799,707** (My share: **\$24,428**)  
Period of Contract: 01/2023—01/2028

## STUDENTS ADVISED

---

### Ph.D. Students

Akshith Gunasekaran (Co-advised with Prof. Rakesh Bobba)	Aug 2018 – Jun 2023
Ping-Jui Liao (graduated with MS degree, first job: Software Engineer at Google)	Aug 2018 – Jun 2023
Jinhong Choi (transferred to other advisor)	Apr 2019 – Jun 2023

### M.S. Students

Ping-Jui Liao (First job: Software Engineer at Google)	Aug 2018 — Jun 2024
Jonathan Keller (First job: Senior Engineer at Infineon)	Sep 2022 – Jun 2024
Lucas Ball	Sep 2022 – Jun 2024
Philiph Lee (returned to the Ministry of the Interior and Safety)	Jan 2021 — Dec 2022
Ryan Kennedy (First job: Security Consultant at NETSPI)	Sep 2020 – Aug 2022
Andrew Quach (degree not awarded)	Jun 2019 – Mar 2022
Cody Holliday (First job: Software Engineer at Jedox)	Sep 2019 – Dec 2021
Phillip Mestas III (First job: Software Engineer at Google)	Sep 2019 – Jun 2021
Hadi Rahal-Arabi (First job: Software Engineer at Intel)	Jan 2019 – Aug 2021

### B.S. Students

Casey Colley	Sep 2022 – Jun 2023
Rudy Peralta	Mar 2022 – Dec 2022
Lyell Read (First job: Security Engineer at PPLSI)	Jun 2019 — Mar 2022
Zander Nead-Work (advanced to graduate study at Georgetown)	Jun 2019 – Jun 2021
Khuong Luu	Apr 2019 – Dec 2020

### Resaerchers

Kihwan Kim (Ph.D. student intern from KAIST)	Jan 2022 – Jun 2022
Changil Lim (Ph.D. student intern from KAIST)	Jan 2022 – Jun 2022
Taehyun Kim (Ph.D. student intern from KAIST)	Jan 2022 – Jun 2022

Jangha Kim (Senior Researcher at NSRI)  
Sera Lee (Ph.D. student intern from KAIST)  
Travis Whitehead (Infrastructure Engineer at Tag1 Consulting)

Mar 2019 – Mar 2020  
Jan 2019 – Jun 2019  
Sep 2019 – Jun 2020

## 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.

Cyber Attacks and Defense (CS499/579 at OSU, 50 students, 6.0/6.0) ..... Winter 2023  
Introduction to Security (CS370 at OSU, 89 students, 5.9/6.0) ..... Fall 2022  
Operating Systems II (CS444/544 at OSU, 193 students, 5.8/5.9) ..... Fall 2022  
Operating Systems II (CS444/544 at OSU, 203 students, 5.9/5.8) ..... Fall 2021  
Cyber Attacks and Defense (CS499/579 at OSU, 26 students, 5.8/5.9) ..... 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](https://www.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]*

## LIST OF REFERENCES

---

**Prof. Wenke Lee, Ph.D. (main doctoral dissertation advisor)**

Regents' Professor and 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>  
LinkedIn : <https://www.linkedin.com/in/wenke-lee-1b8109/>  
Phone : 404-385-2879  
Email : wenke@cc.gatech.edu

**Dr. Kang Li, Ph.D. (worked @ Disekt; CTF/Cyber Grand Challenge)**

Chief Technology Officer (CTO)  
CertiK  
LinkedIn : <https://www.linkedin.com/in/kangoli/>  
Email : kang.li@certik.com

**Dr. Changwoo Min, Ph.D. (Research collaborator)**

Software Engineer  
Igalia, LLC.  
Blog : <https://blogs.igalia.com/changwoo>  
LinkedIn: <https://www.linkedin.com/in/changwoo-min-7545121/>

Last updated: October 13, 2025