YEONGJIN JANG

Assistant Professor
School of Electrical Engineering and Computer Science
Oregon State University
3079 Kelley Engineering Center,
2500 NW Monroe Avenue, Corvallis, OR 97331

Email: yeongjin.jang@oregonstate.edu
Web: http://people.oregonstate.edu/~jangye
☎: +1 (541) 737-2215

RESEARCH INTERESTS

My research focus lies in computer systems security in general and especially in identifying and analyzing emerging attacks to computer systems to build countermeasures to keep systems secure. The following keywords describe my research interests: *trustworthy computing* [4, 5, 9, 17, 19], *vulnerability discovery and analysis* [3, 5, 7, 13, 15, 18], *developing exploit primitives* [5, 6, 8, 12, 16], *jailbreaking* [13, 15, 18], *side-channel attacks* [4, 5, 6, 8, 16], *mobile security* [2, 10, 12, 13, 14, 15, 18], *practical applied cryptography* [1, 14, 19], and *defense mechanisms* [9, 11, 17].

ACADEMIC POSITION

Oregon State University. Corvallis, OR . . . . . Oct 2017 – Current

Assistant Professor of Electrical Engineering and Computer Science

EDUCATION

Georgia Institute of Technology, Atlanta, GA . . . . . Aug 2010 – Aug 2017

Ph.D. in Computer Science

Dissertation Title: *Building Trust in the User I/O in Computer Systems* [20]

Advisors: Prof. Wenke Lee and Prof. Taesoo Kim

M.S. in Computer Science (Specialty: Computing Systems)

Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea. Feb 2010

B.S. in Computer Science

Magna Cum Laude

Dissertation Title: Hardware Implementation of MD5 Brute-force attacker

Advisor: Prof. Seungryoul Maeng

PUBLICATIONS

Summary

11 papers in top-tier security conferences (*USENIX Security, ACM CCS*, and *ISOC NDSS*, 2014-2018)
four papers in a top-tier industry security conference (*Black Hat USA Briefings*, 2013-2016)
three nominations and *one* award by the CSAW Best Applied Research Paper Award

Refereed Journal Articles

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

[2] **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.

Refereed Conference Proceedings

[3] **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.
Acceptance rate: 19.2% (100 of 520).
∗ **Distinguished Paper Award Winner at USENIX Security '18!**

[4] **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**.

[5] **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.
Acceptance rate: 16.3% (85 of 522).

[6] **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.
Acceptance rate: 16.4% (137 of 837).

[7] **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.
Acceptance rate: 15.6% (72 of 463).
∗ **Nominated as one of ten finalists in CSAW Best Applied Research Paper Award 2016.**

[8] **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.

[9] **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.
Acceptance rate: 19.9% (128 of 646).

[10] **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, Col-

orado, October 2015.
Acceptance rate: 19.9% (128 of 646).

[11] **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.
Acceptance rate: 16.9% (51 of 302).
∗ **The third place award by CSAW Best Applied Research Paper Award 2015!**

[12] **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.
Acceptance rate: 19.4% (114 of 585).

[13] **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.
Acceptance rate: 19.1% (67 of 350).

[14] **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.
Acceptance rate: 19.1% (67 of 350).

[15] **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.

[16] **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.

[17] **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.
Acceptance rate: 18.6% (55 of 295).
∗ **Nominated as one of ten finalists in CSAW Best Applied Research Paper Award 2014.**

[18] **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.

Other Published Articles

[19] **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.

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

[21] **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 & AWARDS

Academic Awards

Distinguished Paper Award [3], USENIX Security 2018 ..... Aug 2018

Nominated as a finalist in CSAW Best Applied Research Paper Award [7] ..... Nov 2016

The third place award by CSAW Best Applied Research Paper Award [11] ..... Nov 2015

Nominated as a finalist in CSAW Best Applied Research Paper Award [17] ..... Nov 2014

Nominated as an RSA Security Scholar ..... Oct 2016

People's Choice Award (IDForWeb [21], $2,000 award) by IISP Demo Day Finale ..... Apr 2016

Best Demo Presenter Award [14] by the Marconi Society Young Scholars Symposium ..... Mar 2015

Capture-the-flag (CTF) contests

DEF CON 26 CTF [1], Winner (Team `DEFKOR00t`) ..... Aug 2018

1st place at PNNL, The Department of Energy (DoE) Cyber Defense Competition (CDC) ..... Apr 2018

DEF CON 24 CTF, 3rd place (Team `DEFKOR`) ..... Aug 2016

DARPA Cyber Grand Challenge Finalist (Team `Disekt`) ..... Aug 2016

DEF CON 23 CTF, **Winner** (Team `DEFKOR`) ..... Aug 2015

Qualified for DARPA Cyber Grand Challenge (Team `Disekt`, $750,000 award) ..... Jul 2015

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

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

DEF CON 16 oCTF, 2nd Place (Team `DDUCK`) ..... Aug 2008

Bug Bounties

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

An Integer Overflow Vulnerability in Python zipimport ($1,000), 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

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

PROFESSIONAL ACTIVITIES

Program Committee

World Conference on Information Security Applications (WISA) 2018

ACM Symposium on Information, Computer and Communications Security (ASIACCS) . . . 2018

Reviewer

IEEE Transactions on Information Forensics and Security (TIFS) 2017

External Reviewer

USENIX Annual Technical Conference (ATC) 2018

IEEE Symposium on Security and Privacy (Oakland) 2018

Network and Distributed System Security Symposium (NDSS) . . . . . 2015 – 2017

USENIX Security Symposium (Security) . . . . . 2011, 2015 – 2017

ACM Conference on Computer and Communications Security (CCS) . . . . . 2014 – 2015

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

TEACHING EXPERIENCE

Instructor, Systems Security (CS419/CS519 at OSU, 5.7/5.9) . . . . . Spring 2018

Instructor, Cyber Attacks and Defense (CS419/CS519 at OSU, 6.0/5.9) . . . . . Winter 2018

Teaching Assistant, Network Security (CS6262 at Georgia Tech) . . . . . Spring 2017

Teaching Assistant, Information Security Lab (CS6265 at Georgia Tech) . . . . . Fall 2016

Teaching Assistant, Network Security (CS6262 at Georgia Tech) . . . . . Fall 2016

Teaching Assistant, Introduction to Information Security (CS6260 at Georgia Tech) . . . . . Spring 2016

Teaching Assistant, Information Security Lab (CS6265 at Georgia Tech) . . . . . Fall 2015

Teaching Assistant, Introduction to Computer Programming (CS101 at KAIST) . . . . . Fall 2008

Head Instructor, Information Security Class for Freshmen (KAIST) . . . . . Spring & Fall 2008

MEDIA COVERAGE

Mactans [18]: Injecting Malware Into iOS Devices via Malicious Chargers
Reuters, Forbes, CBSNews, Telegraph, CNN, DailyMail, ZDNet, Ars Technica, PCMagazine, etc.

iOS Botnet [13]: On the Feasibility of Large-Scale Infections of iOS Devices
The Register, Wired, Toms Guide, ComputerWorld, PCWorld, etc.

iOS Jailbreak [15]: Exploiting Unpatched iOS Vulnerabilities for Fun and Profit

International Business Times, ScienceDaily, PCMag, etc.

A11y Attacks [12]: Exploiting Accessibility in Operating Systems
MIT Technology Review

M-Aegis [14]: A Mimicry Privacy Shield
Wired

Gyrus [17]: A Framework for User-Intent Monitoring of Text-based Networked Applications
UPI, ECN, Business Standard, etc.

Reported Security Vulnerabilities (selected list)

IBB-PHP #113268: An Integer Overflow Vulnerability in PHP wordwrap ($500) [7]

IBB-PHP #113120: An Integer Overflow Vulnerability in PHP php_implode ($500) [7]

IBB-PHP #113122: An Integer Overflow Vulnerability in PHP php_str_to_str_ex ($500) [7]

CVE-2016-5636: An Integer Overflow Vulnerability in Python zipimport ($1,000) [7]

US-CERT #VU943167: Voice over LTE implementations contain multiple vulnerabilities [10]

CVE-2015-6614: Elevation of Privilege Vulnerability in Telephony [10]

CVE-2014-4372: Privilege Escalation Vulnerability in iOS 7.1.2 [15]

Invited Presentations

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 [4]

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 [20]

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 [5]

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

Breaking Kernel Address Space Layout Randomization with Intel TSX [6, 8]

Presented at the 23rd ACM CCS 2016 . . . . . Vienna, Austria, Oct 2016 [6].

Presented at the Black Hat USA Briefings 2016 . . . . . Las Vegas, NV, Aug 2016 [8].

Tying Public Key to Person with IDforWeb [21]

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

A11y Attacks: Exploiting Accessibility in Operating Systems [12]

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 [14]

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 [15]

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 [17]

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 [18]

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

John P. Imlay Jr. Professor of Computer Science
Co-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

Catherine M. and James E. Allchin Early Career Assistant 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

KAIST Chair Professor of Electrical Engineering
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

Professor of Computer Science
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