SANGHO LEE

Senior Researcher
Microsoft Research
99/3230, 14820 NE 36th St, Redmond, WA 98052

Sangho.Lee@microsoft.com
https://sangho2.github.io
https://scholar.google.com/citations?user=kjPZ8VcAAAAJ
https://www.microsoft.com/en-us/research/people/sanghle/

EDUCATION

Pohang University of Science and Technology (POSTECH), Pohang, South Korea ..... February 2013
Ph.D. in Computer Science and Engineering
Dissertation: Detection of Web Security Attacks Exploiting URL Redirection (Advisor: Prof. Jong Kim)

POSTECH, Pohang, South Korea ..... February 2008
M.S. in Computer Science and Engineering
Thesis: Redistributing Time-based Rights for Content Sharing in DRM (Advisor: Prof. Jong Kim)

Hongik University, Seoul, South Korea ..... February 2006
B.S. in Computer Engineering

WORK EXPERIENCE

Senior Researcher, Microsoft Research, Redmond, WA, USA ..... November 2018–Current
Cloud and Infrastructure Security Group

Postdoctoral Fellow, Georgia Institute of Technology, Atlanta, GA, USA ..... November 2015–October 2018
Hosts: Prof. Taesoo Kim and Prof. Wenke Lee

Post-doctoral Research Associate, POSTECH ..... March 2013–October 2015
Host: Prof. Jong Kim

RESEARCH INTERESTS

Interested in all aspects of computer security including hardware, systems, and web security

PUBLICATIONS

Conference Proceedings

[1] **Hacksaw: Hardware-Centric Kernel Debloating via Device Inventory and Dependency Analysis**.
Zhenghao Hu, **Sangho Lee**, and Marcus Peinado.
In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, November 2023.

[2] **Rethinking System Audit Architectures for High Event Coverage and Synchronous Log Availability**.
Varun Gandhi*, Sarbartha Banerjee*, Aniket Agrawal, Adil Ahmad, **Sangho Lee**, and Marcus Peinado.
In *Proceedings of the USENIX Security Symposium (Security)*, August 2023.
* **Co-lead authors**.

[3] **APRON: Authenticated and Progressive System Image Renovation**.
Sangho Lee.
In *Proceedings of the USENIX Annual Technical Conference (ATC)*, July 2023.

[4] **Spacelord: Private and Secure Smart Space Sharing**.
Yechan Bae, Sarbartha Banerjee, **Sangho Lee**, and Marcus Peinado*.
In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, December 2022.
* **Alphabetically ordered**.

[5] **DeView: Confining Progressive Web Applications by Debloating Web APIs**.
ChangSeok Oh, **Sangho Lee**, Chenxiong Qian, Hyungjoon Koo, and Wenke Lee.
In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, December 2022.

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

[7] **HardLog: Practical Tamper-Proof System Auditing Using a Novel Audit Device**.
Adil Ahmad, **Sangho Lee**, and Marcus Peinado.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2022.

[8] **KARD: Lightweight Data Race Detection with Per-Thread Memory Protection**.
Adil Ahmad, **Sangho Lee**, Pedro Fonceca, and Byoungyoung Lee.
In *Proceedings of the ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, April 2021.

[9] **All Your Clicks Belong to Me: Investigating Click Interception on the Web**.
Mingxue Zhang, Wei Meng, **Sangho Lee**, Byoungyoung Lee, and Xinyu Xing.
In *Proceedings of the USENIX Security Symposium (Security)*, August 2019.

[10] **libmpk: Software Abstraction for Intel Memory Protection Keys (Intel MPK)**.
Soyeon Park, **Sangho Lee**, Wen Xu, Hyungon Moon, and Taesoo Kim.
In *Proceedings of the USENIX Annual Technical Conference (ATC)*, July 2019.

[11] **Dominance as a New Trusted Computing Primitive for the Internet of Things**.
Meng Xu, Manuel Huber, Zhichuang Sun, Paul England, Marcus Peinado, **Sangho Lee**, Andrey Marochko, Dennis Matoon, Rob Spiger, and Stefan Thom.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2019.

[12] **DIFT Games: Dynamic Information Flow Tracking Games for Advanced Persistent Threats**.
Dinuka Sahabandu, Baicen Xiao, Andrew Clark, **Sangho Lee**, Wenke Lee, and Radha Poovendran.
In *Proceedings of the 57th IEEE Conference on Decision and Control (CDC)*, December 2018.

[13] **Multi-Stage Dynamic Information Flow Tracking Game**.
Shana Moothedath, Dinuka Sahabandu, Andrew Clark, **Sangho Lee**, Wenke Lee, and Radha Poovendran.
In *Proceedings of the 9th Conference on Decision and Game Theory for Security (GameSec)*, October 2018.

[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 USENIX Security Symposium (Security)*, August 2018.
* **Distinguished Paper Award, Frontiers of Science Award**.

[15] **Enabling Refinable Cross-host Attack Investigation with Efficient Data Flow Tagging and Tracking**.
Yang Ji, **Sangho Lee**, Mattia Fazzini, Joey Allen, Evan Downing, Taesoo Kim, Alessandro Orso, and Wenke Lee.
In *Proceedings of the USENIX Security Symposium (Security)*, August 2018.
* GT.

[16] **RAIN: Refinable Attack Investigation with On-demand Inter-Process Information Flow Tracking**.
Yang Ji, **Sangho Lee**, Evan Downing, Weiren Wang, Mattia Fazzini, Taesoo Kim, Alessandro Orso, and Wenke Lee.
In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, October–November 2017.
* AAU, Research Horizons, E&T Magazine, IT Governance USA, Cybersecurity Insiders.

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

[18] **Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing**.
Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado.
In *Proceedings of the USENIX Security Symposium (Security)*, August 2017.

* Intel SGX Academic Research.

[19] **CAB-Fuzz: Practical Concolic Testing Techniques for COTS Operating Systems**.
Su Yong Kim, **Sangho Lee**, Insu Yun, Wen Xu, Byoungyoung Lee, Youngtae Yun, and Taesoo Kim.
In *Proceedings of the USENIX Annual Technical Conference (ATC)*, July 2017.
* CVE-2016-7219, CVE-2016-0040, CVE-2015-6098.

[20] **FACT: Functionality-centric Access Control System for IoT Programming Frameworks**.
Sanghak Lee, Jiwon Choi, Jihun Kim, Beumjin Cho, **Sangho Lee**, Hanjun Kim, and Jong Kim.
In *Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT)*, June 2017.

[21] **T-SGX: Eradicating Controlled-Channel Attacks Against Enclave Programs**.
Ming-Wei Shih*, **Sangho Lee***, Taesoo Kim, and Marcus Peinado.
In *Proceedings of the Annual Network and Distributed System Security Symposium (NDSS)*, February–March 2017.
* **Co-lead authors**, Intel SGX Academic Research.

[22] **Inferring Browser Activity and Status Through Remote Monitoring of Storage Usage**.
Hyungsub Kim, **Sangho Lee**, and Jong Kim.
In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, December 2016.

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

[24] **RecProv: Towards Provenance-aware User-space Record and Replay**.
Yang Ji, **Sangho Lee**, and Wenke Lee.
In *Proceedings of the 6th International Provenance and Annotation Workshop (IPAW)*, June 2016.

[25] **CrowdTarget: Target-based Detection of Crowdturfing in Online Social Networks**.
Jonghyuk Song, **Sangho Lee**, and Jong Kim.
In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, October 2015.

[26] **Identifying Cross-origin Resource Status Using Application Cache**.
Sangho Lee, Hyungsub Kim, and Jong Kim.
In *Proceedings of the Annual Network and Distributed System Security Symposium (NDSS)*, February 2015.

[27] **Exploring and Mitigating Privacy Threats of HTML5 Geolocation API**.
Hyungsub Kim, **Sangho Lee**, and Jong Kim.
In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, December 2014.

[28] **Stealing Webpages Rendered on Your Browser by Exploiting GPU Vulnerabilities**.
Sangho Lee, Youngsok Kim, Jangwoo Kim, and Jong Kim.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2014.
* Reddit.

[29] **Punobot: Mobile Botnet using Push Notification Service in Android**.
Hayoung Lee, Taeho Kang, **Sangho Lee**, Jong Kim, and Yoonho Kim.
In *Proceedings of the International Workshop on Information Security Applications (WISA)*, August 2013.

[30] **I Know the Shortened URLs You Clicked on Twitter: Inference Attack using Public Click Analytics and Twitter Metadata**.
Jonghyuk Song, **Sangho Lee**, and Jong Kim.
In *Proceedings of the International World Wide Web Conference (WWW)*, May 2013.

[31] **WarningBird: Detecting Suspicious URLs in Twitter Stream**.
Sangho Lee and Jong Kim.
In *Proceedings of the Annual Network and Distributed System Security Symposium (NDSS)*, February 2012.

[32] **Spam Filtering in Twitter using Sender-receiver Relationship**.
Jonghyuk Song, **Sangho Lee**, and Jong Kim.
In *Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID)*, September 2011.

[33] **A Batch Rekeying Time Decision Algorithm for IPTV Systems**.
Sangho Lee and Jong Kim.
In *Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC)*, January 2011.

[34] **A Secure and Mutual-profitable DRM Interoperability Scheme**.
Sangho Lee, Heejin Park, and Jong Kim.
In *Proceedings of the IEEE Symposium on Computers and Communications (ISCC)*, June 2010.

[35] **Reducing IPTV Channel Zapping Time based on Viewer's Surfing Behavior and Preference**.
Yuna Kim, Jae Keun Park, Hong Jun Choi, **Sangho Lee**, Heejin Park, Jong Kim, Zino Lee, and Kwangil Ko.
In *Proceedings of the IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, March-April 2008.

Journal/Magazine Articles

[36] **Memory Protection Keys: facts, key extension perspectives, and discussions**.
Soyeon Park, **Sangho Lee**, and Taesoo Kim.
IEEE Security & Privacy, 21(3), May-June 2023.

[37] **Prevention of Cross-update Privacy Leaks on Android**.
Beumjin Cho, **Sangho Lee**, Meng Xu, Sangwoo Ji, Taesoo Kim, and Jong Kim.
Computer Science and Information Systems, 15(1):111–137, January 2018.

[38] **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.
ACM Computing Surveys, 49(2), August 2016.

[39] **Inference Attack on Browsing History of Twitter Users using Public Click Analytics and Twitter Metadata**.
Jonghyuk Song, **Sangho Lee**, and Jong Kim.
IEEE Transactions on Dependable and Secure Computing, 13(3):340–354, May-June 2016.

[40] **Preserving Source- and Sink-location Privacy in Sensor Networks**.
Sangho Lee, Jong Kim, and Yoonho Kim.
Computer Science and Information Systems, 13(1):115–130, January 2016.

[41] **Early filtering of ephemeral malicious accounts on Twitter**.
Sangho Lee and Jong Kim.
Computer Communications, 54:48–57, December 2014.

[42] **WarningBird: A Near Real-time Detection System for Suspicious URLs in Twitter Stream**.
Sangho Lee and Jong Kim.
IEEE Transactions on Dependable and Secure Computing, 10(3):183–195, May-June 2013.

[43] **Fluxing botnet command and control channels with URL shortening services**.
Sangho Lee and Jong Kim.
Computer Communications, 36(3):320–332, February 2013.

[44] **Distance Bounding with Delayed Responses**.
Sangho Lee, Jin Seok Kim, Sung Je Hong, and Jong Kim.
IEEE Communications Letters, 16(9):1478–1481, September 2012.

[45] **DRMFS: A file system layer for transparent access semantics of DRM-protected contents**.
Sangho Lee, Hay-Rim Lee, Seungkwang Lee, and Jong Kim.
Journal of Systems and Software, 85(5):1058–1066, May 2012.

[46] **Redistributing time-based rights between consumer devices for content sharing in DRM system**.
Sangho Lee, Jong Kim, and Sung Je Hong.
International Journal of Information Security, 8(4):263–273, August 2009.

[47] **Security weakness of Tseng's fault-tolerant conference-key agreement protocol**.
Sangho Lee, Jong Kim, and Sung Je Hong.
Journal of Systems and Software, 82(7):1163–1167, July 2009.

Granted Patents

[48] **Data race detection with per-thread memory protection**.

Sangho Lee and Adil Ahmad.
US 11,556,395, January 2023.

[49] **Selective boot sequence controller for resilient storage memory**.
Stefan Thom, Paul England, Robert Karl Spiger, Brian Telfer, **Sangho Lee**, and Marcus Peinado.
US 11,520,596, December 2022.

[50] **Methods and apparatuses for providing DRM interoperability**.
Jong Kim, **Sangho Lee**, and Heejin Park.
US 8,386,799, February 2013.

[51] **Method of distributing time of using contents between personal devices and system based on the same**.
Sangho Lee and Jong Kim.
Korea 10-0951792, April 2010.

[52] **Method and apparatus for rights-preserving interoperability in DRM**.
Heejin Park, **Sangho Lee**, and Jong Kim.
Korea 10-0942992, February 2010.

Honors and Awards

Frontiers of Science Award, 1st International Congress of Basic Science ($25,000)	2023
Distinguished Paper Award, 27th USENIX Security Symposium	2018
Postdoctoral Research Fellowship, National Research Foundation of Korea ($35,000)	2017–2018
Runner-up Prize, Evaluation of ITRC Support Program ($1,000)	2013

Professional Activities

Program Committee Member

USENIX Security Symposium	2021–2022
Annual Computer Security Applications Conference (ACSAC)	2016–2023
Workshop on Artificial Intelligence System with Confidential Computing (AISCC)	2024
IEEE Silicon Valley Cybersecurity Conference (SVCC)	2023
ACM SIGOPS Asia-Pacific Workshop on Systems (APSys)	2020
ACM Asia Conference on Computer and Communications Security (AsiaCCS)	2018
World Conference on Information Security Applications (WISA)	2018

External Reviewer

USENIX Annual Technical Conference (ATC)	2018
USENIX Security Symposium	2017
IEEE Transactions on Information Forensics and Security (TIFS)	2018
IEEE Transactions on Computational Social Systems (TCSS)	2017
ACM Transactions on Privacy and Security (TOPS)	2016
Journal of Computing Science and Engineering (JCSE)	2015
IEEE Communications Letters	2013
Security and Communication Networks (SCN)	2011
IEEE Transactions on Dependable and Secure Computing (TDSC)	2009, 2014, 2018

Talks

Detecting Data Races Efficiently with Per-Thread Memory Protection

GoGE Workshop, SNU, Seoul, South Korea (virtual) November 2021

Securing Hardware-based Trusted Execution Environment

University of Virginia, Charlottesville, Virginia, USA March 2018
University of Waterloo, Waterloo, Ontario, Canada March 2018
Texas A&M University, College Station, Texas, USA February 2018
Microsoft Research, Redmond, Washington, USA February 2018
KAIST, Daejeon, South Korea February 2018

Practical Concolic Testing Techniques for COTS Operating Systems

Korea University, Seoul, South Korea July 2017
KAIST, Daejeon, South Korea June 2017
POSTECH, Pohang, South Korea June 2017

Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing

Intel, Hillsboro, Oregon, USA February 2017

Detection of Suspicious URLs with Conditional Redirection

ETRI, Daejeon, South Korea March 2015

Privacy Leakage from GPU Exploits

KAIST, Daejeon, South Korea March 2015

Web and Browser Security: Attack and Defense

UNIST, Ulsan, South Korea January 2015

Spam and Browsing Privacy Problems on Twitter

KAIST, Daejeon, South Korea May 2013

Last updated: November 28, 2023