HOJOON LEE

Associate Professor
Computer Science and Engineering, Sungkyunkwan University
hojoon.lee@skku.edu https://sslab.skku.edu

PROFESSIONAL APPOINTMENTS

Sungkyunkwan University *Sep 2024 - Current*
Associate Professor, Department of Computer Science and Engineering

Sungkyunkwan University *Sep 2019 - Aug 2024*
Assistant Professor, Department of Computer Science and Engineering

CISPA Helmholtz Center for Information Security *Sep 2018 - Sep 2019*
Postdoctoral Researcher (Advisor: Prof. Dr. Dr. h.c. Michael Backes)

EDUCATION

KAIST *Sep 2013 - Feb 2018*
PhD in Information Security (Advisor: Prof. Brent Byunghoon Kang)
Dissertation: "*A Study on Design, Implementation, and Optimizations of External Hardware-based Kernel Integrity Monitor*"

KAIST *Sep 2011 - Aug 2013*
M.S. in Information Security

The University of Texas at Austin *Sep 2006 - Dec 2010*
B.S. in Electrical and Computer Engineering

AWARDS AND HONORS

ACM CCS 2024 Distinguished Paper Award *2024*

ACM CCS 2023 Distinguished Paper Award *2023*

Microsoft Research Asia PhD Fellowship *2015*

Backwoon Scholarship *2013*

PUBLICATIONS

1. **uMMU: Securing Data Confidentiality with Unobservable Memory Subsystem** , Hajeong Lim, Jaeyoon Kim, **Hojoon Lee**, ACM Conference on Computer and Communications Security (ACM CCS) 2024 (*Distinguished Paper Award*).
2. **RustSan: Retrofitting AddressSanitizer for Efficient Sanitization of Rust (To Appear),** Kyuwon Cho, Jongyoon Kim, Kha Dinh Duy, Hajeong Lim, **Hojoon Lee**, USENIX Security Symposium 2024.
3. **(In)visible Privacy Indicator: Security Analysis of Privacy Indicator on Android Devices**, Yurak Choe, Hyungseok Yu, Taeho Kim, Shinjae Lee, ***Hojoon Lee**, *Hyoungshick Kim (*Co-corresponding authors) ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS) 2024.
4. **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**, *Brent Byunghoon Kang (*Co-corresponding Authors), ACM/SIGAPP Symposium on Applied Computing (SAC) 2024.

5. **Capacity: Cryptographically-Enforced In-process Capabilities for Modern ARM Architectures**, Kha Dinh Duy, Kyuwon Cho, Taehyun Noh, **Hojoon Lee**, ACM Conference on Computer and Communications Security (CCS) 2023 (*Distinguished Paper Award*).

6. **Towards Scalable and Configurable Simulation for Disaggregated Architecture,** Daegyeong Kim, Wonwoo Choi, Chang-il Lim, Eunjin Kim, Geonwoo Kim, Yongho Song, Junsu Lee, Youngkwang Han, **Hojoon Lee**, Brent Byunghoon Kang, Elsevier Simulation Modelling Practice and Theory (2023).

7. **DID We Miss Anything?: Towards Privacy-Preserving Decentralized ID Architecture,** Siwon Huh, Myungkyu Shim, Jihwan Lee, Simon Woo, Hyoungshick Kim, **Hojoon Lee**, IEEE Transactions on Dependable and Secure Computing (TDSC) (2023).

8. **SE-PIM: In-Memory Acceleration of Data-Intensive Confidential Computing,** Kha Dinh Duy, **Hojoon Lee**, IEEE Transactions on Cloud Computing (2022).

9. **Harnessing the x86 Intermediate Rings for Intra-Process Isolation,** Hojoon Lee, Chihyun Song, Brent Byunghoon Kang, IEEE Transactions on Dependable and Secure Computing (TDSC) (2022).

10. **Confidential Machine Learning Computation in Untrusted Environments: A Systems Security Perspective,** Kha Dinh Duy, Taehyun Noh, Siwon Huh, **Hojoon Lee**, IEEE Access (2021).

11. **A Comprehensive Analysis of Today' s Malware and Its Distribution Network: Common Adversary Strategies and Implications,** Siwon Huh, Seonghwan Cho, Jinho Choi, Seungwon Shin, **Hojoon Lee**, IEEE Access (2021).

12. **EmuID: Detecting Presence of Emulation through Microarchitectural Characteristic on ARM,** Yeseul Choi, Yunjong Jeong, Dahee Jang, Brent Byunghoon Kang, **Hojoon Lee**, Elsevier Computers & Security (2021).

13. **On the Analysis of Byte-Granularity Heap Randomization,** DaeHee Jang, Jonghwan Kim, **Hojoon Lee**, Minjoon Park, Yunjong Jung, Minsu Kim, Brent ByungHoon Kang, IEEE Transactions on Dependable and Secure Computing (TDSC) (2021).

14. **Lord of the x86 Rings: A Portable User Mode Privilege Separation Architecture on x86,** Hojoon Lee, Chihyun Song, and Brent Byunghoon Kang, ACM Conference on Computer and Communications Security (ACM CCS). 2018

15. **A Dynamic Per-context Verification of Kernel Address Integrity from External Monitors**, Hojoon Lee, Minsu Kim, Yunheung Paek, Brent Byunghoon Kang, Elsevier Computers Security, 77:824 – 837, 2018.

16. **KI-Mon ARM: A Hardware- assisted Event-triggered Monitoring Platform for Mutable Kernel Object**, Hojoon Lee, Hyungon Moon, Daehee Jang, Kihwan Kim, Jihoon Lee, Yunheung Paek, Brent Byunghoon Kang, IEEE Transactions on Dependable and Secure Computing (TDSC), pages 1–1, 2018.

17. **Detecting and Preventing Kernel Rootkit Attacks with Bus Snooping**, Hyungon Moon, **Hojoon Lee**, Ingoo Heo, Kihwan Kim, Yunheung Paek, Brent Bynghoon Kang, IEEE Transactions on Dependable and Secure Computing (TDSC), 14(2):145–157, March 2017.

18. **ATRA: Address Translation Redirection Attack Against Hardware-based External Monitors**, Dahee Jang, **Hojoon Lee**, Hyungon Moon, Minsu Kim, Daehyeok Kim, Daegyeong Kim, Brent Byunghoon Kang, ACM Conference on Computer and Communications Security (ACM CCS) 2014.

19. **KI-Mon: A Hardware-assisted Event-triggered Monitoring Platform for Mutable Kernel Object**, Hojoon Lee, Hyungon Moon, Daehee Jang, Kihwan Kim, Jihoon Lee, Yunheung Paek, Brent Byunghoon Kang, USENIX Security Symposium 2013.

20. **Vigilare: Toward Snoop-based Kernel Integrity Monitor**, Hyungon Moon, **Hojoon Lee**, Jihoon Lee, Kihwan Kim, Yunheung Paek, Brent Bynghoon Kang, ACM Conference on Computer and Communications Security (ACM CCS) 2012.

TEACHING

SWE2001: System Program	S21, F21, S22, F22, F23, S24
SWE3009: Internet Services and Information Security	S21, S22, S23, S24
SWE3025: Introduction to Information Security	S20
ESW4010: Special Topics in Systems Security	F21, F22, S23
SWE3028: Capstone Design Project	F20, F23
GEDT019: Basis and Practice in Programming	F20

GRANTS

Oblivious Computation Framework for Confidential Computing in Cloud Feb 2022 - Feb 2026
Role: Principal Investigator,
Outstanding Early-Career Researcher (우수신진연구),
National Research Foundation of Korea (NRF)

Research and Development of Efficient Fuzzing Techniques for Rust Aug 2023 - Aug 2024
Role: Principal Investigator,
Samsung Mobile eXperience (MX) Business, Samsung Electronics

Research of Platform Security for Disaggregated Cloud Architecture Apr 2020 - Apr 2023
Role: Institutional Principal Investigator,
Global Leading Technology Development Project for Information Security
Institute for Information & Communications Technology Planning & Evaluation (IITP)

Security Coprocessor Designs for Processing-In-Memory Feb 2020 - Feb 2022
Role: Principal Investigator,
Outstanding Early-Career Researcher (우수신진연구),
National Research Foundation of Korea (NRF)

Emulator-based Android Kernel Device Driver Vulnerability Analysis Apr 2022 - Oct 2022
Role: Principal Investigator,
National Security Research Institute (NSRI)

Security Analysis of Memory Protection Methods on AARCH64 Apr 2022 - Oct 2022
Role: Principal Investigator,
National Security Research Institute (NSRI)