

# HOJOON LEE

Associate Professor

Computer Science and Engineering, Sungkyunkwan University

✉ hojoon.lee@skku.edu 🏠 <https://sslabs.skku.edu>

## PROFESSIONAL APPOINTMENTS

---

<b>Sungkyunkwan University</b> Associate Professor, Department of Computer Science and Engineering	<i>Sep 2024 - Current</i>
<b>Sungkyunkwan University</b> Assistant Professor, Department of Computer Science and Engineering	<i>Sep 2019 - Aug 2024</i>
<b>CISPA Helmholtz Center for Information Security</b> Postdoctoral Researcher (Advisor: Prof. Dr. Dr. h.c. Michael Backes)	<i>Sep 2018 - Sep 2019</i>

## EDUCATION

---

<b>KAIST</b> PhD in Information Security (Advisor: Prof. Brent Byunghoon Kang) Dissertation: “ <i>A Study on Design, Implementation, and Optimizations of External Hardware-based Kernel Integrity Monitor</i> ”	<i>Sep 2013 - Feb 2018</i>
<b>KAIST</b> M.S. in Information Security	<i>Sep 2011 - Aug 2013</i>
<b>The University of Texas at Austin</b> B.S. in Electrical and Computer Engineering	<i>Sep 2006 - Dec 2010</i>

## AWARDS AND HONORS

---

<b>ACM CCS 2024 Distinguished Paper Award</b>	<i>2024</i>
<b>ACM CCS 2023 Distinguished Paper Award</b>	<i>2023</i>
<b>Microsoft Research Asia PhD Fellowship</b>	<i>2015</i>
<b>Backwoon Scholarship</b>	<i>2013</i>

## PUBLICATIONS

---

- IncognitOS: A Practical Unikernel Design for Full-System Obfuscation in Confidential Virtual Machines (To Appear)**, Kha Dinh Duy, Jaeyoon Kim, Hajeong Lim, **Hojoon Lee**, IEEE Symposium on Security and Privacy (IEEE S&P) 2025.
- 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).
- RustSan: Retrofitting AddressSanitizer for Efficient Sanitization of Rust**, Kyuwon Cho, Jongyoon Kim, Kha Dinh Duy, Hajeong Lim, **Hojoon Lee**, USENIX Security Symposium 2024.
- (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.

5. **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.
6. **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** ).
7. **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).
8. **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).
9. **SE-PIM: In-Memory Acceleration of Data-Intensive Confidential Computing**, Kha Dinh Duy, **Hojoon Lee**, IEEE Transactions on Cloud Computing (2022).
10. **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).
11. **Confidential Machine Learning Computation in Untrusted Environments: A Systems Security Perspective**, Kha Dinh Duy, Taehyun Noh, Siwon Huh, **Hojoon Lee**, IEEE Access (2021).
12. **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).
13. **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).
14. **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).
15. **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
16. **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.
17. **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.
18. **Detecting and Preventing Kernel Rootkit Attacks with Bus Snooping**, Hyungon Moon, **Hojoon Lee**, Ingoo Heo, Kihwan Kim, Yunheung Paek, Brent Byunghoon Kang, IEEE Transactions on Dependable and Secure Computing (TDSC), 14(2):145–157, March 2017.
19. **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.

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

## TEACHING

---

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

## GRANTS

---

<b>Oblivious Computation Framework for Confidential Computing in Cloud</b>	Feb 2022 - Feb 2026
<i>Role: Principal Investigator,</i> Outstanding Early-Career Researcher (우수신진연구), National Research Foundation of Korea (NRF)	
<b>Research and Development of Efficient Fuzzing Techniques for Rust</b>	Aug 2023 - Aug 2024
<i>Role: Principal Investigator,</i> Samsung Mobile eXperience (MX) Business, Samsung Electronics	
<b>Research of Platform Security for Disaggregated Cloud Architecture</b>	Apr 2020 - Apr 2023
<i>Role: Institutional Principal Investigator,</i> Global Leading Technology Development Project for Information Security Institute for Information & Communications Technology Planning & Evaluation (IITP)	
<b>Security Coprocessor Designs for Processing-In-Memory</b>	Feb 2020 - Feb 2022
<i>Role: Principal Investigator,</i> Outstanding Early-Career Researcher (우수신진연구), National Research Foundation of Korea (NRF)	
<b>Emulator-based Android Kernel Device Driver Vulnerability Analysis</b>	Apr 2022 - Oct 2022
<i>Role: Principal Investigator,</i> National Security Research Institute (NSRI)	
<b>Security Analysis of Memory Protection Methods on AARCH64</b>	Apr 2022 - Oct 2022
<i>Role: Principal Investigator,</i> National Security Research Institute (NSRI)	