Hojoon **Lee**

ASSISTANT PROFESSOR @ SUNGKYUNKWAN UNIVERSITY (SKKU)

Engineering Building 1 Room 23122, 2066 Seobu-ro, Jangan-gu, Suwon-si, Gyeonggi-do, Republic of Korea

+82 31 290 7697 | hojoon.lee [at] skku [dot] edu | https://sslab.skku.edu

Research Interests

- Software Security
- Operating Systems
- Confidential Computing

Experience

Dept. of Computer Science and Engineering, Sungkyunkwan University   *Suwon, Korea*
ASSISTANT PROFESSOR   *Sep. 2019 - Current*

CISPA-Stanford Center for Cybersecurity   *Saarbruecken, Germany*
POSTDOCTORAL RESEARCHER (ADVISOR: PROF. MICHAEL BACKES)   *Sep. 2018 - Sep. 2019*

Education

KAIST   *Daejeon, Korea*
PhD IN INFORMATION SECURITY   *Sep, 2013 - Feb, 2018*
- Dissertation: "A Study on Design, Implementation, and Optimizations of External Hardware-based Kernel Integrity Monitor" (Advised by Prof. Brent Byunghoon Kang)

KAIST   *Daejeon, Korea*
M.S. IN INFORMATION SECURITY   *Sep, 2011 - Aug, 2013*

The University of Texas at Austin   *Austin TX, USA*
B.S. IN ELECTRICAL AND COMPUTER ENGINEERING   *Sep, 2006 - Dec, 2010*

Honors & Awards

2015 **MSRA PhD Fellow**, Microsoft Research Asia PhD Fellowship   *Beijing, China*
2013 **Backwoon Scholarship**, Backwoon Foundation Scholarship   *Seoul, Korea*

Publications

REFEREED CONFERENCE PAPERS

1. **Capacity: Cryptographically-Enforced In-process Capabilities for Modern ARM Architectures**
   Kha Dinh Duy, Kyuwon Cho, Taehyun Noh, **Hojoon Lee**
   In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, (CCS '23) (To Appear)

2. **Lord of the x86 Rings: A Portable User Mode Privilege Separation Architecture on x86.**
   Hojoon Lee, Chihyun Song, and Brent Byunghoon Kang.
   In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, (CCS '18)

3. **ATRA: Address Translation Redirection Attack Against Hardware-based External Monitors.**
   Daehee Jang, **Hojoon Lee**, Minsu Kim, Daehyeok Kim. Daegyeong Kim, and Brent Byunghoon Kang.
   In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, (CCS '14)

4. **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, and Brent Byunghoon Kang.
   In Proceedings of 22nd USENIX Security Symposium (USENIX Security '13)

5. **Vigilare: Toward Snoop-based Kernel Integrity Monitor.**
   Hyungon Moon, **Hojoon Lee**, Jihoon Lee, Kihwan Kim, Yunheung Paek, and Brent Byunghoon Kang.
   In Proceedings of the 2012 ACM Conference on Computer and Communications Security, (CCS '12)

Refereed Journal Papers

1. **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**, and Brent Byunghoon Kang
   Elsevier Simulation Modelling Practice and Theory (2023)

2. **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)

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

4. **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)

5. **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)

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

7. **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)

8. **On the Analysis of Byte-Granularity Heap Randomization**
Daehee Jang, Jonghwan Kim, **Hojoon Lee**, Minjun Park, Yunjong Jung, Minsu Kim, Brent Byunghoon Kang
IEEE Transactions on Dependable and Secure Computing (2019)

9. **A Dynamic Per-context Verification of Kernel Address Integrity from External Monitors.**
Hojoon Lee, Minsu Kim, Yunheung Paek Brent Byunghoon Kang.
Elsevier Computers & Security (2018)

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

11. **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) (2017)

Teaching

- **SWE3009: Internet Services and Information Security**
- **SWE3025: Introduction to Information Security**
- **SWE2001: System Program**
- **GEDT019: Basis and Practice in Programming**
- **SWE3028: Capstone Design**
- **ESW4010: Special Topics in Systems Security**