Hojoon Lee

Assistant Professor @ Sungkyunkwan University (SKKU)

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

hjlee228@gmail.com

Research Interests

- Systems Security
- Operating Systems
- Hardware Security

Experience

Dept. of Computer Science and Engineering, Sungkyunkwan University (SKKU) — *Suwon, Korea*

Assistant Professor — *Sep. 2019 - Current*

CISPA-Stanford Center for Cybersecurity — *Saarbruecken, Germany*

Postdoctoral Researcher (Advisor: Prof. Michael Backes) — *Sep. 2018 - Aug. 2019*

GSIS, KAIST — *Daejeon, Korea*

Graduate Student Researcher (Advisor: Prof. Brent Byunghoon Kang) — *Sep. 2013 - Aug. 2018*

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*

Publications

Refereed Conference Papers

1. **H. Lee**, C. Song, and B. B. Kang. Lord of the x86 Rings: A Portable User Mode Privilege Separation Architecture on x86. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS '18, pages 1441–1454, New York, NY, USA, 2018. ACM

2. D. Jang, **H. Lee**, M. Kim, D. Kim, D. Kim, and B.B. Kang. ATRA: Address Translation Redirection Attack Against Hardware-based External Monitors. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS '14, pages 167–178, New York, NY, USA, 2014. ACM
3. **H. Lee**, H. Moon, D. Jang, K. Kim, J. Lee, Y. Paek, and B.B. Kang. KI-Mon: A Hardware-assisted Event-triggered Monitoring Platform for Mutable Kernel Object. In Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13), pages 511–526, Washington, D.C., 2013. USENIX
4. H. Moon, **H. Lee**, J. Lee, K. Kim, Y. Paek, and B. B. Kang. Vigilare: Toward Snoop-based Kernel Integrity Monitor. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS '12, pages 28–37, New York, NY, USA, 2012. ACM

Refereed Journal Papers

1. (Under Major Revision) D. Jang, J. Kim, **H.Lee**, M. Park, Y. Jung, M. Kim, B. B. Kang, On the Analysis of Byte-Granularity Heap Randomization, IEEE Transactions on Dependable and Secure Computing
2. **H. Lee**, M. Kim, Y. Paek, and B. B. Kang. A Dynamic Per-context Verification of Kernel Address In- tegrity from External Monitors. Computers & Security, 77:824 – 837, 2018
3. **H. Lee**, H. Moon, I. Heo, D. Jang, J. Jang, K. Kim, Y. Paek, and B. Kang. KI-Mon ARM: A Hardware- assisted Event-triggered Monitoring Platform for Mutable Kernel Object. IEEE Transactions on Dependable and Secure Computing, pages 1–1, 2018
4. H. Moon, **H. Lee**, I. Heo, K. Kim, Y. Paek, and B. B. Kang. Detecting and Preventing Kernel Rootkit Attacks with Bus Snooping. IEEE Transactions on Dependable and Secure Computing, 14(2):145–157, March 2017

Teaching

Lectures

- *Software Attacks and Mitigation*, KAIST Software Graduate Program, Jul 2018
- *Lecture Series: Trusted Execution Environments*, LG Electronics, Jun 2018
- *Research Trends in Hypervisor-based Security Solutions* , SK Telecom, May 2014

Graduate Teaching Assistant

- Course: IS632 Virtualization and Security (Spring 2018)
- Course: IS632 Virtualization and Security (Spring 2014)
- Course: IS631 Kernel System Security (Fall 2013)

Honors & Awards

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

Selected Project Experience

"Towards Dialects Computing in Network and System Protocols" *Daejeon, S.Korea*
Office of Naval Research (USA) *Feb. 2018 - Aug. 2018*

- Lead system protocol team as senior personnel in proposal preparation

"eXecute-No-Read Memory on ARM" *Daejeon, S.Korea*
Nation Security Research Institute (NSRI of Korea) *Apr. 2016 - Oct. 2016*

- Designed execute-only memory scheme on ARM 64bit processor through kernel-level modifications
- Implemented prototype to demonstrate its ability to thwart advanced code-reuse attacks

"Research for New Technology of Cloud Security" *Daejeon, S.Korea*
Nation Security Research Institute (NSRI of Korea) *Jul. 2014 - Feb. 2015*

- Designed and implemented a Linux KVM-based VMI (Virtual Machine Introspection) library
- Demonstrated kernel malware detection examples using implemented VMI library

"Optimizing Linux kernel for external hardware-based kernel integrity monitoring" *Daejeon, S.Korea*
Samsung Electronics *Oct. 2013 - Jan. 2014*

- Discussed possible optimizations necessary for adopting external monitoring in company's products
- Modified SLAB allocator and page tables for data structure congregation

"Development of HW/SW for External System Integrity Monitor" *Daejeon, S.Korea*
Samsung Electronics *Apr. 2013 - Dec. 2013*

- Participated in external system monitor design
- Designed and implemented snooping-based kernel integrity monitoring techniques and software

Skills

Kernel-level Programming	Experienced in Kernel-level software development through academic work and projects
Hypervisor Implementation	Knowledgeable in hypervisor internals (KVM, Xen) from Virtual Machine Introspection (VMI) implementation experience
Reverse Engineering	Acquired reverse engineering through experience and occasional CTF participation
Program Analysis	Striving to master program analysis and transformation for security through LLVM framework