Hyungon Moon (문현곤)

Associate Professor
Computer Systems Security Lab
Department of Computer Science and Engineering
Ulsan National Institute of Science and Technology (UNIST)

hyungon@unist.ac.kr —— https://hyungon.unist.ac.kr —— https://cssl.unist.ac.kr

Last updated: March 1, 2024

Contents

EDUCATION

Seoul National University, Seoul, Korea. ..... Mar 2010 – Feb 2017

Ph.D. in Electrical Engineering and Computer Science

Thesis: Hardware Techniques against Memory Corruption Attacks

Advisor: Yunheung Paek

Seoul National University, Seoul, Korea. ..... Mar 2005 – Feb 2010

B.S. in Electrical Engineering

B.S. in Mathematical Science

Cum Laude

EMPLOYMENT HISTORY

Ulsan National Institute of Science and Technology (UNIST). Ulsan, Korea .... Aug 2018 – Current

Associate Professor ..... Sep 2022 – Current

Assistant Professor ..... Aug 2018 – Aug 2022

Georgia Institute of Technology. Atlanta, GA, USA ..... May 2017 – Aug 2018

Postdoctoral Fellow

Advisor: Taesoo Kim

RESEARCH INTERESTS

Systems Security, Operating Systems, Computer Architecture, Program Analysis

PUBLICATIONS

Summary

Publication in Top CS Conferences							
S&P	Security	CCS	NDSS	ATC	FAST	ICCAD	**Total**
2	3	1	1	1	1	2	**11**

Refereed Publications

[1] [SEC24], **Metasafe: Compiling for protecting smart pointer metadata to ensure safe rust integrity**. Martin Kayondo, Inyoung Bang, Yeongjun Kwak, Hyungon Moon*, and Yunheung Paek*. In *USENIX Security Symposium (Security)*, August 2024.
(**KIISE S, BK21 IF: 4, CSRankings**).

[2] [NDSS24], **Efficient use-after-free prevention with opportunistic page-level sweeping**. Chanyoung Park and Hyungon Moon*. In *Network and Distributed System Security Symposium (NDSS)*, San Diego, California, USA, February 2024.
(**KIISE S, BK21 IF: 2, CSRankings**).

[3] [SoCC23], **Kvsev: A secure in-memory key-value store with secure encrypted virtualization**. Junseung You, Kyeongryong Lee, Hyungon Moon*, Yeongpil Cho, and Yunheung Paek*. In *ACM Symposium on Cloud Computing (SoCC)*, Santa Cruz, California, USA, October 2023.
(**KIISE A, BK21 IF: 1**).

[4] [ICCAD23], **Hyperdimensional computing as a rescue for efficient privacy-preserving machine learning-as-a-service**. Jaewoo Park, Chenghao Quan, Hyungon Moon*, and Jongeun Lee*. In *International Conference on Computer-Aided Design (ICCAD)*, San Francisco, California, USA, October 2023. URL `https://arxiv.org/abs/2310.06840`.
(**KIISE A, BK21 IF: 3, CSRankings**).

[5] **Protecting Kernel Code integrity with PMP on RISC-V**. Seon Ha and Hyungon Moon**. In *World Conference on Information Security Applications (WISA)*, August 2023.

[6] [SEC23], **Trust: A compilation framework for in-process isolation to protect safe rust against untrusted code**. Inyoung Bang, Martin Kayondo, Hyungon Moon*, and Yunheung Paek*. In *USENIX Security Symposium (Security)*, August 2023.
(**KIISE S, BK21 IF: 4, CSRankings**).

[7] **Kernel code integrity protection at the physical address level on risc-v**. Seon Ha, Minsang Yu, Hyungon** Moon, and Jongeun Lee. *IEEE Access (Access)*, pages 1–1, June 2023. doi: 10.1109/ACCESS.2023.3285876.

[8] [ICCAD22], **Accelerating n-bit operations over tfhe on commodity cpu-fpga**. Kevin Nam, Hyunyoung Oh, Hyungon Moon*, and Yunheung Paek*. In *International Conference on Computer-Aided Design (ICCAD)*, San Diego, California, USA, October 2022.
(**KIISE A, BK21 IF: 3, CSRankings**).

[9] [ESORICS22], **Precise extraction of deep learning models via side-channel attacks on edge/endpoint devices**. Younghan Lee, Sohee Jun, Yungi Cho, Woorim Han, Hyungon Moon*, and Yunheung Paek*. In *European Symposium on Research in Computer Security (ESORICS)*, 2022.
(**KIISE A, BK21 IF: 2**).

[10] [DATE22], **XtenStore: Extensible Secure In-memory Key-Value Store on a Hybrid x86-FPGA System**. Hyunyoung Oh, Maja Malenko, Dongil Hwang, Myunghyun Cho, Hyungon Moon*, Marcel Baunach, and Yunheung Paek*. In *Design, Automation & Test in Europe (DATE)*, 2022.
Interactive Presentation,
(**KIISE A, BK21 IF: 1**).

[11] [FAST22], **A Log-Structured Merge Tree-aware Message Authentication Scheme for Persistent Key-Value Stores**. Igjae Kim, J. Hyun Kim, Minu Chung, Hyungon Moon**, and Sam H. Noh. In *Proceedings of the 22nd USENIX Conference on File and Storage Technologies (FAST)*, February 2022.
(**KIISE S, BK21 IF: 3, CSRankings**).

[12] [TMC], **Ambassy: A Runtime Framework to Delegate Trusted Applications in an ARM/FPGA Hybrid System**. Dongil Hwang, Sanzhar Yeleuov, Jiwon Seo, Minu Chung, Hyungon Moon*, and Yunheung Paek*. *IEEE Transactions on Mobile Computing (TMC)*, May 2023.
(**SCI**).

[13] [ATC19], **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 2019 USENIX Annual Technical Conference (ATC)*, Renton, WA, July 2019.
(**KIISE S, BK21 IF: 3, CSRankings**).

[14] [SP19], **Fuzzing File Systems via Two-Dimensional Input Space Exploration**. Wen Xu, Hyungon Moon, Sanidhya Kashyap, Po-Ning Tseng, and Taesoo Kim. In *Proceedings of the 40th IEEE Symposium on Security and Privacy (Oakland)*, San Francisco, CA, May 2019.

(**KIISE S, BK21 IF: 4, CSRankings**).

[15] [**TDSC**], **KI-Mon ARM: A Hardware-assisted Event-triggered Monitoring Platform for Mutable Kernel Object**. Hojoon Lee, Hyungon Moon, Ingoo Heo, Daehee Jang, Jinsoo Jang, Kihwan Kim, Yunheung Paek*, and Brent Byunghoon Kang*. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2019.
(**SCI**).

[16] [**RAID18**], **Hardware-Assisted Randomization of Data**. Brian Belleville***, Hyungon Moon***, Jangseop Shin, Dongil Hwang, Joseph Michael Nash, Seonhwa Jung, Yeoul Na, Stijn Volckaert, Per Larsen, Yunheung Paek*, and Michael Franz. In *Proceedings of the 21st International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, Heraklion, Crete, Greece, September 2018.
***: joint first authors, contributted equally,
(**KIISE A, BK21 IF: 2**).

[17] [**TODAES**], **Architectural Supports to Protect OS Kernels from Code-Injection Attacks and Their Applications**. Hyungon Moon, Jinyong Lee, Dongil Hwang, Seonhwa Jung, Jiwon Seo, and Yunheung Paek. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 23(1), October 2017.
(**SCI**).

[18] [**TDSC**], **Detecting and Preventing Kernel Rootkit Attacks with Bus Snooping**. Hyungon Moon, Hojoon Lee***, Ingoo Heo, Kihwan Kim, Yunheung Paek, and Brent Byunghoon Kang. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 14(2), March 2017. ***: co-first author,
(**SCI**).

[19] [**HASP16**], **Architectural Supports to Protect OS Kernels from Code-Injection Attacks**. Hyungon Moon, Jinyong Lee, Dongil Hwang, Seonhwa Jung, Jiwon Seo, and Yunheung Paek. In *Proceedings of the Hardware and Architectural Support for Security and Privacy (HASP)*, 2016.

[20] [**SP16**], **HDFI: Hardware-Assisted Data-Flow Isolation**. Chengyu Song, Hyungon Moon, Monjur Alam, Insu Yun, Byoungyoung Lee, Taesoo Kim, Wenke Lee, and Yunheung Paek. In *Proceedings of the 37th IEEE Symposium on Security and Privacy (Oakland)*, San Jose, CA, May 2016.
(**KIISE S, BK21 IF: 4, CSRankings**).

[21] [**JSTS**], **Efficient Kernel Integrity Monitor Design for Commodity Mobile Application Processors**. Ingoo Heo, Daehee Jang, Hyungon Moon, Hansoo Cho, Seungwook Lee, Brent Byunghoon Kang, and Yunheung Paek. *Journal of Semiconductor Technology and Science (JSTS)*, 15(1), February 2015.
(**SCI**).

[22] [**DATE15**], **Extrax: Security Extension to Extract Cache Resident Information for Snoop-based External Monitors**. Jinyong Lee, Yonje Lee, Hyungon Moon, Ingoo Heo, and Yunheung Paek. In *Proceedings of the Design, Automation & Test in Europe (DATE)*, Grenoble, France, March 2015.
(**KIISE A, BK21 IF: 2**).

[23] [**SEC13**], **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 the 22th USENIX Security Symposium (Security)*, Washington, DC, August 2013.
(**KIISE S, BK21 IF: 4, CSRankings**).

[24] [**CCS12**], **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 19th ACM Conference on Computer and Communications Security (CCS)*, Raleigh, NC, October 2012.
(**KIISE S, BK21 IF: 4, CSRankings**).

Patents

[25] **Apparatus and Method for Deallocating Memory Area Dynamically Allocated**, Hyungon Moon, Chanyoung Park, Jaehyu Lee, and Daeyeon Kim. February 2023. KR Patent No. 10-2023-0035857, Applied.

[26] **Secure computing device and method for key value store using log structured merge tree**, Hyungon Moon, Sam H. Noh, Igjae Kim, J. Hyun Kim, and Minu Chung. February 2023. PCT/KR2023/002276, Applied.

[27] **Electronic device and method for controlling the operation of the kernel code region**, Hyungon Moon Seon Ha. February 2023. KR Patent No. 10-2022-0110820, Applied.

[28] **Secure computing device and method for key value store using log structured merge tree**, Hyungon Moon, Sam H. Noh, Igjae Kim, J. Hyun Kim, and Minu Chung. February 2022. KR Patent No. 10-2022-0021722, Applied.

[29] **Snoop-based kernel integrity monitoring apparatus and method thereof**, Yunheung Paek, Brent Byunghoon Kang, Hyungon Moon, Hojoon Lee, Jihoon Lee, and Kihwan Kim. January 2017. US Patent No. S9542557, Granted.

[30] **Hardware-based detection of kernel code injection attack apparatus and method thereof**, Yunheung Paek, Hyungon Moon, and Jinyong Lee. September 2016. Republic of Korea Patent No. 1016586410000, Granted.

Domestic

[31] **Extracting instruction set architecture semantics from a processor register-transfer level**. Seon Ha and Hyungon Moon**. *Journal of KIISE (JOK)*, 2023.

[32] **An Operating System Support-based Prevention Mechanism for Use-After-Free Attacks on the Glibc Memory Allocator**. Chanyoung Park, Jaehyu Lee, Daeyeon Kim, and Hyungon Moon**. *Journal of KIISE (JOK)*, 2023.

[33] **FunRank: Finding 1-day Vulnerabilities with Call-site and Data-flow Analysis**. Jaehyo Lee, Jihun Baek, and Hyungon Moon**. *Journal of The Korea Institute of Information Security and Cryptology (JKIISC)*, 2023.

[34] **Funrank: Finding 1-day vulnerabilities with data-flow analysis**. Jaehyu Lee, Jihun Baek, and Hyungon Moon*. In *Korea Software Congress (KSC)*, 2022.
Distinguished Paper Presentation Award.

[35] **Extracting isa semantics from a processor rtl**. Seon Ha and Hyungon Moon*. In *Korea Software Congress (KSC)*, 2022.
Best Paper Award.

SERVICES

Program Committee

European Conference on Computer Systems (EuroSys), 2025

USENIX Security Symposium (SEC), 2024

World Conference on Information Security Applications (WISA), 2023

USENIX Conference on File and Storage Technologies (FAST), 2023

Other Conference Activities

Organizing Committee, KIISE Computer System Society Conference 2024

Session Chair, ACM SIGOPS Asia-Pacific Workshop on Systems (APSys), 2023

Session Chair, USENIX Conference on File and Storage Technologies (FAST), 2023

Journal Editor

Associate Editor, Journal of Information Processing Systems, 2024

Associate Editor, KIPS Transactions on Computer and Communication Systems, 2024

Journal Reviewer

Journal of The Korea Institute of Information Security and Cryptology (JKIISC), 2023, 2022, 2021
IEEE Transactions on Computer, 2020

Student Program Committee

IEEE Symposium on Security and Privacy, 2016

Sub-reviewer

USENIX Conference on File and Storage Technologies (FAST), 2024
Usenix Security Symposium, 2018
Usenix Annual Technical Conference, 2018
European Conference on Computer Systems, 2018
The Network and Distributed System Security Symposium, 2018
ACM Conference on Computer and Communications Security, 2017
ACM/IFIP/USENIX International Middleware Conference, 2017
Design Automation Conference, 2017
IEEE Transactions on Computers, 2016
International Workshop on Software and Compilers for Embedded Systems, 2014
IEEE International Parallel and Distributed Processing Symposium, 2013
Workshop on Synthesis And System Integration of Mixed Information technologies, 2012

Miscellaneous

Organizing Committee, Winter Conference on Information Security and Cryptography (CISC-W), Korea Institute of Information Security & Cryptography (KIISC), 2020

TALKS

Invited Talks

1) Privacy-preserving Machine Learning Services
Workshop on AI Semiconductor, Annual Conference of KIPS (ACK) 2023, Nov 2023

2) Confidential Outsourced Data Processing on Cloud
Pohang University of Science and Technology (POSTECH), May 2023

3) Confidential Outsourced Data Processing on Cloud
Samsung Advanced Institute of Technology, Nov 2022

4) Key-Value Stores on Enclave: Opportunities and Challenges
Operating System Support for Next Generation Large Scale NVRAM (NVRAMOS), Oct 2022

5) Adapting Key-Value Stores for Trusted Execution Environments
Hanyang University, Mar 2022

6) Recent Studies on Model Extraction Attacks and Defenses
ETRI, Dec 2021

7) Trusted Execution Environments on Personal Mobile Devices for Third-parties
Annual Conference of KIPS (ACK) 2021, Nov 2021

8) Hardware-based mechanisms to defeat ransomware
ETRI, Mar 2021

9) Trusted Execution Environments on Personal Mobile Devices for Third-parties
Security@KAIST, Nov 2020

10) Trusted Execution Environments on Personal Mobile Devices for Third-parties
Yonsei University, Oct 2020

11) Understanding and exploiting hardware for secure computer systems
ETRI, Sep 2020

12) Teaching a computer systems course remotely
UNIST Workshop on Innovations in Post-pandemic Online Education, Jul 2020

13) libmpk: Software Abstraction for Intel Memory Protection Keys (Intel MPK)
KIISE Computer System Society Winter Workshop, Feb 2020

14) Hardware Techniques for Software Security
KIISE Korea Software Congress, Dec 2018

Open Source

1) KVSEV [3] (★: 0, Fork: 0) `https://github.com/cssl-unist/kvsev`
2) TRust [6] (★: 0, Fork: 0) `https://github.com/cssl-unist/trust-sec23`
3) PrivLock [7] (★: 0 Fork: 0) `https://github.com/cssl-unist/priv-code-lock`
4) Tweezer [11] (★: 4 Fork: 3) `https://github.com/cssl-unist/tweezer`
5) libMPK [13] (★: 38 Fork: 8) `https://github.com/sslab-gatech/libmpk`
6) Janus [14] (★: 190 Fork: 26) `https://github.com/sslab-gatech/janus`
7) HDFI [20] (★: 25 Fork: 13) `https://github.com/sslab-gatech/hdfi`

Students

Graduate Students

1) **Seon Ha** [5, 7, 35, 31] (PhD Student) Mar 2021 — Current
(Master Student) Mar 2019 — Feb 2021

2) **Minu Chung** [11, 12] (Master-Phd Combined) Mar 2021 — Current
(Undergraduate) Sep 2019 — Feb 2021

3) **Chanyoung Park** [2, 32] (Master-Phd Combined) Mar 2022 — Current
(Undergraduate) Jan 2020 — Feb 2022

4) **Jihun Baek** [33] (Master Student) Mar 2024 — Current
(Undergraduate) Jul 2022 — Feb 2024

5) **Yeongjun Kwak** [1] (Master Student) Mar 2024 — Current
(Undergraduate) Dec 2022 — Feb 2024

Alumni

1) **Jaehyu Lee** [32, 33, 34] (FESCARO) (Master Student) Mar 2021 — Feb 2023
(Intern, U-WURF/Remote, from Chungbuk National University) Jan 2020 — Feb 2021

Undergraduate Students, Interns, and Collaborators

1) **Marlen Raushanov** Nov 2023 — Current
2) **Jaewoo Park (w/Jongeun Lee)** [4] May 2023 — Current
3) **Jiwon Park** Aug 2023 — Current

Past Undergraduate Students

1) **Igjae Kim** [11] (PhD Student at KAIST) Jan 2020 — Aug 2021
2) **Daeyeon Kim** [32] (LG CNS) Jan 2020 — Dec 2020
3) **Sanzhar Yeleuov** [12] (Master Student at SECCLO) Mar 2019 — Dec 2019

Past Undergraduate Interns

1) **Eungyeong Baek** Jun 2023 — Dec 2023
2) **Jaewon Lee (U-WURF)** Jan 2023 — Feb 2023
3) **Vyacheslav Kim** Sep 2022 — Dec 2022
4) **Jinwoo Choi** Mar 2022 — Aug 2022
5) **Dung Nguyen** May 2021 — Jun 2022
6) **Alisher Karim** Jun 2021 — Jun 2022
7) **Kasymzhan Abdyldayev** Mar 2022 — Jun 2022
8) **Kaiyrly Mukhametkarim** Jun 2021 — Dec 2021
9) **Aibar Oshakbayev** Jan 2021 — Jan 2022
10) **Junhyeok Song** Jan 2021 — May 2021
11) **Jeongseok Nam** Jul 2020 — May 2021
12) **Hwarang Kim** (Naver) Jul 2020 — Dec 2020
13) **Ryeongyun Kim** Jan 2020 — Jun 2020
14) **Azhar Smagulova** Mar 2019 — Jun 2019
15) **Kadyrbek Narmamatov** Mar 2019 — Jun 2019
16) **Sungduck Cho** Jan 2019 — Feb 2019
17) **Donggi Yang** Sep 2018 — Jun 2019

Past Visitors and Remote Interns

1) **Seungho Song** (U-SURF Visitor from Inha University) Jul 2020 — Aug 2020
2) **Jiwon Seo** [12] (from SNU ECE) Jan 2019 — Jan 2019
3) **Dongil Hwang** [10, 12] (from SNU ECE) Jan 2019 — Jan 2019

FUNDING

1. **Protecting the Integrity of Key-value Storeson Untrusted Memory and Storage**

   Jun 2022 — Dec 2024

   KRW 156,428,000

   Principal Investigator (100%)

   National Research Foundation of Korea

2. **Industry-Academic Cooperation Project**

   May 2022 — Apr 2024

   KRW 240,000,000

   Co-Principal Investigator

3. **Security Analysis of OSS-based Network Firmware**

   Apr 2022 — Oct 2022

   KRW 60,000,000

   Principal Investigator (100%)

   NSR

4. **(ITRC) Development of Next-Generation Computing Techniques for Hyper-Composable Data-centers**

   Jul 2021 – Dec 2028

   KRW 600,000,000 (out of KRW 6,000,000,000)

   Researcher (10%)

   IITP

5. **A TEE-aware design of LSM tree-based Key-Value Stores**

   Jun 2021 – May 2022

   KRW 47,761,000

   Principal Investigator (100%)

   National Research Foundation of Korea

6. **RISC-V based Secure CPU Architecture Design for Embedded System Malware Detection and Response**

Apr 2021 — Dec 2024

KRW 245,000,000 (out of KRW 7,500,000,000)

Co-Principal Investigator (3.3%)

IITP

7. **OSS-based IoT Firmware Security Analysis**

   Apr 2021 — Oct 2021

   KRW 60,000,000

   Principal Investigator (100%)

   NSR

8. **Development of RISC-V CPU extensions to prevent privileged code injection attacks**

   Sep 2020 — Nov 2020

   KRW 31,000,000

   Principal Investigator (100%)

   ETRI

9. **Analysis, modularization and formal modeling of automated storage and retrieval system management software**

   Jun 2020 — Jun 2021

   KRW 68,000,000

   Principal Investigator (100%)

   Hyundai NGV

10. **Automatically identifying security-critical bugs in application-specific computing systems**

    Sep 2018 – Aug 2021

    KRW 90,000,000

    Principal Investigator (100%)

    National Research Foundation of Korea

AWARDS

Distinguished Paper Presentation Award (Jaehyo Lee), Korea Software Congress (KSC) 2022

Best Paper Award, Korea Software Congress (KSC) 2022

Highly Cited Paper Award, Department of ECE, SNU 2017

Outstanding Collaborative Research Award, Department of ECE, SNU 2016

TEACHING

Advanced Operating Systems (CSE514) . . . . . Spring 2023
Building Customized Computers (CSE302) . . . . . Fall 2022
Software Hacking and Defense (UNI204) . . . . . Spring 2022
Computer Architecture (CSE261) . . . . . Fall 2021
Principles of Programming Languages (CSE271, CSE341) . . . . . Fall 2021, Fall 2020, Fall 2023
Advanced Computer Architecture (CSE551) . . . . . Fall 2020, Spring 2021, Spring 2022, Spring 2024
Computer Security (CSE467) . . . . . Spring 2020
Special Topics in CSE II(Software and Systems Security) (CSE481) . . . . . Fall 2019
Data Structures (CSE221) . . . . . Spring 2019
System Programming (CSE251) . . . . . Spring 2019
Special Topics in CSE II(Computer Systems Security) (CSE481) . . . . . Fall 2018