Hyungon Moon (문현곤)

Assistant 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: July 15, 2022

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

Assistant Professor

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

Refereed Publications

[1] **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. Accepted.

[2] **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. Conditionally Accepted.

[3] **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.

[4] **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.

[5] **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)*. Early Access.

[6] **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.

[7] **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.

[8] **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.

[9] **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.

[10] **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.

[11] **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.

[12] **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.

[13] **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.

[14] **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.

[15] **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.

[16] **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.

[17] **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.

Patents

[18] **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.

[19] **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.

[20] **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.

SERVICES

Program Committee

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

Journal Reviewer

Journal of The Korea Institute of Information Security and Cryptology (JKIISC), 2022

Journal of The Korea Institute of Information Security and Cryptology (JKIISC), 2021

IEEE Transactions on Computer, 2020

Student Program Committee

IEEE Symposium on Security and Privacy, 2016

External reviewer

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

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

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

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

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

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

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

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

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

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

OPEN SOURCE

1) Tweezer (★: 0 Fork: 0) `https://github.com/cssl-unist/tweezer`
2) libMPK (★: 31 Fork: 5) `https://github.com/sslab-gatech/libmpk`
3) Janus (★: 156 Fork: 26) `https://github.com/sslab-gatech/janus`
4) HDFI (★: 24 Fork: 12) `https://github.com/sslab-gatech/hdfi`

STUDENTS

PhD Students

1) **Seon Ha** (PhD Student) Mar 2021 — Current
(Master Student) Mar 2019 — Feb 2021

2) **Minu Chung** [4, 5] (Master-Phd Combined) Mar 2021 — Current
(Undergraduate) Sep 2019 — Feb 2021

3) **Chanyoung Park** (Master-Phd Combined) Mar 2022 — Current
(Undergraduate) Jan 2020 — Feb 2022

Master Students

1) **Jaehyu Lee** (Master Student) Mar 2021 — Current
(Intern, U-WURF/Remote, from Chungbuk National University) Jan 2020 — Feb 2021

Undergraduate Students and Interns

1) **Jinu Choi** Mar 2022 — Current

2) **Jihun Baek** Jul 2022 — Current

Past Undergraduate Students

1) **Igjae Kim** [4] (Master Student at KAIST) Jan 2020 — Aug 2021
2) **Daeyeon Kim** (LG CNS) Jan 2020 — Dec 2020
3) **Sanzhar Yeleuov** [5] (Master Student at SECCLO) Mar 2019 — Dec 2019

Past Undergraduate Interns

1) **Dung Nguyen** May 2021 — Jun 2022
2) **Alisher Karim** Jun 2021 — Jun 2022
3) **Kasymzhan Abdyldayev** Mar 2022 — Jun 2022
4) **Kaiyrly Mukhametkarim** Jun 2021 — Dec 2021
5) **Aibar Oshakbayev** Jan 2021 — Jan 2022
6) **Junhyeok Song** Jan 2021 — May 2021
7) **Jeongseok Nam** Jul 2020 — May 2021
8) **Hwarang Kim** (Naver) Jul 2020 — Dec 2020
9) **Ryeongyun Kim** Jan 2020 — Jun 2020
10) **Azhar Smagulova** Mar 2019 — Jun 2019
11) **Kadyrbek Narmamatov** Mar 2019 — Jun 2019
12) **Sungduck Cho** Jan 2019 — Feb 2019
13) **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** (from SNU ECE) Jan 2019 — Jan 2019
3) **Dongil Hwang** (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 2023

   KRW 120,000,000

   Researcher

   Samsung Electronics

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 Datacenters**

   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

TEACHING

Software Hacking and Defense (UNI204) . . . . . Spring 2022

Computer Architecture (CSE261) . . . . . Fall 2021

Principles of Programming Languages (CSE271, CSE341) . . . . . Fall 2021, Fall 2020

Advanced Computer Architecture (CSE551) . . . . . Fall 2020, Spring 2021, Spring 2022

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