Seongmin Kim

CONTACT
Assistant Professor
Department of Convergence Security Engineering,
Sungshin Women's University
Tel: (+82)2-920-7449
Email: sm.kim@sungshin.ac.kr

Prime #506, 2, Bomun-ro 34da-gil
Seongbuk-gu, Seoul, 02844, Republic of Korea

RESEARCH INTERESTS
Trusted Computing, System Security, Network Security, Cloud Computing

WORK EXPERIENCE

Sungshin Women's University SEP. 2020 ∼ Present
Assistant Professor, in Department of Convergence Security Engineering

Samsung Research, Samsung Electronics SEP. 2019 ∼ AUG. 2020
Staff Engineer, in Security Team (Security 2 Lab)

Korea Advanced Institute of Science and Technology (KAIST) MAR. 2019 ∼ AUG. 2019
Postdoctoral Researcher, in Information & Electronics Research Institute

EDUCATION

Korea Advanced Institute of Science and Technology (KAIST) MAR. 2015 ∼ FEB. 2019
Ph.D., in Graduate School of Information Security, School of Computing

Korea Advanced Institute of Science and Technology (KAIST) MAR. 2012 ∼ FEB. 2014
M.S., in Department of Electrical Engineering

Korea Advanced Institute of Science and Technology (KAIST) FEB. 2007 ∼ FEB. 2012
B.S., in Department of Electrical Engineering

PUBLICATIONS **Conference**

1. Juhyeng Han, **Seongmin Kim**, Taesoo Kim, and Dongsu Han. "Toward scaling hardware security module for emerging cloud services". *In Proceedings of the 4th Workshop on System Software for Trusted Execution (SysTex'19).*

2. Byungkwon Choi, Jeongmin Kim, Daeyang Cho, **Seongmin Kim**, and Dongsu Han. "APPx: An Automated App Acceleration Framework for Low Latency Mobile App". *In Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies (CoNEXT'18).*

3. Juhyeng Han, **Seongmin Kim**, Jaehyeong Ha, and Dongsu Han. "SGX-Box: Enhancing Visibility on Encrypted Traffic using a Secure Middlebox Module". *In Proceedings of the 1st Asia-Pacific Workshop on Networking (APNet'17).*

4. **Seongmin Kim**, Juhyeng Han, Jaehyeong Ha, Taesoo Kim, and Dongsu Han. "Enhancing Security and Privacy of Tor's Ecosystem by using Execution Environments". *In Proceedings of the 14th USEXNI Symposium on Networked Systems Design and Implementation (NDSI'17).*

5. Jaebaek Seo, Byoungyoung Lee, **Seongmin Kim**, Ming-Wei Shih, Insik Shin, Dongsu Han, and Taesoo Kim. "SGX-Shield: Enabling Address Space Layout Randomization for SGX Programs". *In Proceedings of the 24th Annual Network and Distributed System Security Symposium (NDSS'17).*

6. Prerit Jain, Soham Desai, **Seongmin Kim**, Ming-Wei Shih, Jaehyuk Lee, Changho Choi, Youjung Shin, Taesoo Kim, Brent Byunghoon Kang, Dongsu Han. "OpenSGX: An Open Platform for SGX Research". *In Proceedings of the 23rd Annual Network and Distributed System Security Symposium (NDSS'16), San Diego, United States, Feb 2016.*

7. **Seongmin Kim**, Youjung Shin, Jaehyung Ha, Taesoo Kim, Dongsu Han. "A First Step Towards Leveraging Commodity Trusted Execution Environments for Network Applications". *In Proceedings of the*

14th ACM Workshop on Hot Topics in Networks (ACM HotNets'15), Philadelphia, United States, Nov 2015.

8. Byeoksan Lee, **Seongmin Kim**, Eru Park, Dongsu Han. "MemScope: Analyzing memory Duplication on Android Systems". *In Proceedings of the 6th ACM Asia-Pacific Workshop on Systems (ACM APSys'15), Tokyo, Japan, Jul 2015.*

9. Jong-Hun Choi, **Seong-Min Kim**, Chulmin kim, Ki-Woomg Park, Kyu Ho Park. "OPAMP: Evaluation Framework for Optimal Page Allocation of Hybrid main Memory Architecture". *In Proceedings of the 18th IEEE International Conference on Parallel and Distributed Systems (IEEE ICPADS'12), Singapore, Dec 2012.*

10. Dong-Jae Shin, Sung Kyu Park, **Seong Min Kim**, Kyu Ho Park. "Adaptive Page Grouping for Engery Efficiency in Hybrid PRAM-DRAM Main Memory". *In Proceedings of the 2012 ACM Research in Applied Computation Symposium (ACM RACS'12), San Antonio, United States, Oct 2012.*

Journals

1. Juhyeng Han, **Seongmin Kim**, Daeyang Cho, Byungkwon Choi, Jaehyeong Ha, and Dongsu Han. "A Secure Middlebox Framework for Enabling Visibility Over Multiple Encryption Protocols". *IEEE/ACM Transactions on Networking.* vol. 28, no. 6, pp. 2727-2740. December 2020.

2. **Seongmin Kim**, Juhyeng Han, Jaehyeong Ha, Taesoo Kim, and Dongsu Han. "SGX-Tor: A Secure and Practical Tor Anonymity Network With SGX Enclaves". *IEEE/ACM Transactions on Networking.* vol. 26, no. 5, pp. 2174-2187. October 2018.

3. Kyu Ho Park, Woomin Hwang, Hyunchul Seok, Chulmin Kim, Dong-jae Shin, Dong Jin Kim, Min Kyu Maeng, **Seong Min Kim**. "MN-MATE: Elastic Resource Management of Manycores and a Hybrid Memory Hierarchy for a Cloud Node". *ACM Journal on Emerging Technologies in Computing Systems.* vol. 12, no. 1, article 5. July 2015.

INVITED TALKS
1. Networking System Implementation (NSI) talk, ACM APNet, August 2017.
2. Institute for Information Security & Privacy, Georgia Tech, February 2016.

SOFTWARE PUBLISHED
1. SGX-Tor: Intel SGX-enabled Tor anonymity network (`https://github.com/kaist-ina/SGX-Tor/`)
2. OpenSGX: Open-source Intel SGX emulator (`https://github.com/sslab-gatech/opensgx`)
3. MemScope: Memory duplication analysis tool for x86-android (`https://github.com/kaist-ina/MemScope`)

SKILLS
1. SGX programming: Built various networked systems, including Tor anonymity network and network middleboxes, running on the real SGX hardware. Also familiar with SGX software development kit (SDK) provided by Intel.
2. Emulation of x86 ISA extension: Built an SGX emulator, an x86 ISA extension for a security purpose, based on QEMU.
3. Rust programming: Developed APIs with Rust language for building a secure middlebox.
4. System programming: Built swap I/O system specialized for Android.