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 & Workshop

1. Saerom Park, **Seongmin Kim** (corresponding), and Yeon-Sup Lim. "Fairness Audit of Machine Learning Models with Confidential Computing". *The ACM Web Conference 2022 (WWW'22)* (To appear).

2. 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).*

3. 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).*

4. 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).*

5. **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).*

6. 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).*

7. 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.*

8. **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.*
9. 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.*
10. 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.*
11. 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. **Seongmin Kim**. "An Optimization Methodology for Adapting Legacy SGX Applications to Use Switchless Calls". *MDPI Applied Sciences*. vol. 11, no. 18, pp. 8379. September 2021.
2. 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.
3. **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.
4. 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.

TEACHING

Sungshin Women's University, Seoul, Korea

- Contribution in undergraduate education in the department of Convergence Security Engineering
- Contribution in graduate education in the department of Future Convergence Technology Engineering

Undergraduate Course

- LB003800 Introduction to Convergence Security
  - Spring 2021: 100 students, evaluation rating 4.49/5.0
- LC001800 Java Programming
  - Spring 2021 (Given in English): 35 students, evaluation rating 4.85/5.0
- LB001700 System Security
  - Fall 2020: 50 students, evaluation rating 4.77/5.0
- LB002700 Hacking Laboratory 2
  - Fall 2020: 40 students, evaluation rating 4.55/5.0
- LB002400 Information Security Consulting
  - Fall 2021: 68 students, evaluation rating 4.7/5.0

- LB002800 Digital Forensics Laboratory
  - Fall 2021: 45 students, evaluation rating 4.71/5.0

Graduate Course

- 290508 Cyber Forensics
  - Spring 2021: 10 students, evaluation rating 4.82/5.0

Students Supervised/Under-supervision
Sara Hong, Hyeon No, Heekyung Shin, Yeun Kim, Jiwon Ock (Master candidate)
Jiwon Jang (Master candidate, Co-advisor: Daehee Jang)

Undergraduate Internship
Dark Web: Daeun Kim, Yuji Park, Yejin Do, Sangyeon Han
Trusted Execution Environment: Jiwoo Kang

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`)

INVITED TALKS

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

RESEARCH FUNDING RECEIVED

Totaling 1.5B KRW in research fund (PI: 0.1B KRW)

1. "Secure and Privacy-Preserving Multi-Tenancy for 5G Network Services and Edge Cloud" (90,000,000 KRW), funded by National Research Foundation of Korea (NRF), Mar. 2021 Feb. 2024. **(PI)**
2. "Training R&D professionals to protect industrial technology based on the 4th industrial revolution" (1,402,200,000 KRW), funded by Ministry of Trade, Industry and Energy (MOTIE), Mar. 2021 - Feb, 2024.
3. "Toward enhancing security of runtime and system software for emerging 5G network" (20,000,000 KRW), Sungshin Women's University, Sep. 2020 - Aug, 2021. **(PI)**