Minkyung Park

Security Researcher

tnstnii23@gmail.com

linkedin.com/in/mk-alsroad

alsroad.github.io

I am a security researcher. My research focus is in system and network security to protect user privacy, e.g., designing privacy-preserving system architectures or analyzing network protocol security of secure protocols.

Quantitative Research Dynamic Information Flow Control (taint tracking and secure multi execution), Trusted Execution Environment (Intel SGX, Arm TrustZone, side/covert-channel attacks), Authentication and authorization (PKI, SSL/TLS, DNS security, SMTP, etc.), User privacy (tracking/fingerprinting and privacy-preserving advertising), and Software vulnerability (fuzz testing)

Programmings and tools C/C++ (Proficient), Assembly (Intel X64), Java, Python, Linux Operating System

Professional Experience

Postdoctoral Researcher, *Network Convergence and Security Laboratory, Seoul National University* September 2022 — Present

Assistant Researcher, *Network Convergence and Security Laboratory, Seoul National University* March 2014 — August 2022

Education

Ph.D. in Computer Science and Engineering, *Seoul National University* March 2014 — August 2022

B.S. in Computer Science and Engineering, *Korea Aerospace University* March 2010 — February 2014

Selected Papers

Ph.D Thesis: Information Flow Control for Privacy-preserving Advertising.

- Keywords: Privacy-preserving Advertising, Information Flow Control, Intel SGX, Side/covert-channel Attack, Native Client (SFI)
- Advisor: Prof. Taekyoung "Ted" Kwon (tkkwon@snu.ac.kr)

An SGX-Based Key Management Framework for Data Centric Networking

- **M. Park**, J. Kim, Y. Kim, E. Cho, S. Park, S. Sohn, M. Kang, T. T. Kwon
- IEEE Access (SCI-E) 2020
- Keywords: Intel SGX, Public Key Infrastructure, Information Centric Networking

MaxPass: Credit-based multipath transmission for load balancing in data centers

- **M. Park**, S. Sohn, K. Kwon, T. T. Kwon
- IEEE Journal of Communications and Networks (JCN) (SCI-E) 2019
- Keywords: Data Center Networking, Transport Layer Protocol

Selected Projects

Development of Homomorphic Encryption and Trusted Execution Environment for Data Privacy

- Role: Implemented OP-TEE applications that handles private data (homomorphically encrypted)
- Keywords: Arm TrustZone (OP-TEE), Data Privacy, FHE, Cloud Machine Learning
- Funded by Ministry of SMEs and Startups June 2022 — Present

Research on Grey-box Fuzzing Techniques for TLS Protocol

- Role (project manager): Designed a new grey-box fuzzer for the TLS protocol and implemented and tested it with 10+ test programs including OpenSSL, WolfSSL, mbedTLS, lighttpd, etc.
- Keywords: TLS, Fuzzing, Differential analysis
- Funded by KOREA INSTITUTE OF INFORMATION SECURITY & CRYPTOLOGY (KIISC) March 2022 — November 2022

Research on Traceability for Data Stability on Cloud-edge Lifecycle

- Role (project manager): Designed and implemented an Information Flow Control framework that tracks data leakage on a remote server.
- Keywords: Information Flow Control, Intel SGX
- Funded by Institute for Information and Communications Technology Promotion (IITP) April 2020 — December 2021

Research on GPU Acceleration for Fully Homomorphic Encryption (FHE)

- Role (project manager): Designed the GPU-accelerated FHE library (compatible with BGV) and implemented a scheduler that schedule HE evaluation operations to minimize the GPU synchronization overhead.
- Keywords: GPU, CUDA, FHE, BGV, HElib
- Funded by KOREA INSTITUTE OF INFORMATION SECURITY & CRYPTOLOGY (KIISC) Febrary 2020 — November 2020

Misc activities

Technical Advisor (volunteer work), Global IT Challenge

- I made up MS Excel and PowerPoint questions in the IT competition for disabled children. Mar 2016 –– Feb 2017

Researcher, Samsung Software Membership

- Samsung Software Membership is an IT training program supported by Samsung Electronics. Jan 2012 –– Dec 2013