tnstnii23@gmail.com
linkedin.com/in/mk-alsroad/

Minkyung Park

Security Researcher

github.com/alsroad
alsroad.github.io/

I'm currently working as a postdoctoral researcher in the Department of Computer Science and Engineering at Seoul National University in South Korea. My research topic lies in privacy and security. Specifically, I'm interested in information flow control, trusted execution environment (TEE; Intel SGX, Arm TrustZone), privacy-preserving advertising, and so on.

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

Skills

Languages	C/C++ (Proficient), Java, Python
Quantitative Research	Privacy (Information Flow Control), Trusted Execution Environment (Intel SGX), Public Key Infrastructure (PKI), and Transport Layer Security (TLS), Network (TCP and Data Center Networking)
Communication	English, Korean (Native)

Selected Papers

Ph.D Thesis: Information Flow Control for Privacy-preserving.
- Keywords: Privacy-preserving Advertising, Information Flow Control, Intel SGX, Side/covert-channel Attack
- Advisor: Prof. Taekyoung "Ted" Kwon

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

Pay-Per-Use in User-Provided Networks: A Bitcoin-based Approach (poster)
- **M. Park**, S. Park, E. Cho and T. T. Kwon
- International Conference on emerging Networking EXperiments and Technologies (ACM Conext) Incheon, Korea 2017
- Keywords: User privacy, Pay-Per-Use, Blockchain, User-Provided Network

Selected Projects

Development of Homomorphic Encryption and Trusted Execution Environment for Data Privacy
- Role: Implemented an OP-TEE application (Arm TrustZone) that uses private data (homomorphically encrypted)
- Keywords: Arm TrustZone, Data Privacy, FHE, Cloud Machine Learning
- Supported by Ministry of SMEs and Startups June 2022 — Present

Research on Grey-box Fuzzing Techniques for TLS Protocol
- Role (project manager): Designed and implemented a grey-box fuzzer for TLS protocol. (The follow-up study is being carried out.)
- Keywords: TLS, Fuzzing, Differential analysis
- Supported 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. (The follow-up study is being carried out.)
- Keywords: Information Flow Control, Intel SGX
- Supported 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 it (especially, a scheduler).
- Keywords: GPU, Cuda, FHE, BGV, HElib
- Supported by KOREA INSTITUTE OF INFORMATION SECURITY & CRYPTOLOGY (KIISC) Febrary 2020 — November 2020

Misc activities

Technical Advisor (volunteer work), Global IT Challenge — Mar 2016 –– Feb 2017
Researcher, Samsung Software Membership — Jan 2012 –– Dec 2013

Complete List of Papers

TwinPeaks: An Approach for Certificateless Public Key Distribution for the Internet and Internet of Things
- Eunsang Cho, Jeongnyeo Kim, **Minkyung Park**, Hyeonmin Lee, Chorom Hamm, Soobin Park, Sungmin Sohn, Minhyeok Kang, Ted "Taekyoung" Kwon
- Elsevier Computer Networks (SCI-E) 2020

An SGX-Based Key Management Framework for Data Centric Networking
- **Minkyung Park**, Jeongnyeo Kim, Youngho Kim, Eunsang Cho, Soobin Park, Sungmin Sohn, Minhyeok Kang, Ted "Taekyoung" Kwon
- IEEE Access (SCI-E) 2020

D2TLS: Delegation-based DTLS for Cloud-based IoT Services
- Eunsang Cho, **Minkyung Park**, Hyunwoo Lee, Junhyeok Choi, and Ted "Taekyoung" Kwon
- ACM/IEEE Fourth International Conference on Internet-of-Things Design and Implementation (IEEE IoTDI) Montreal, Canada 2019

MaxPass: Credit-based multipath transmission for load balancing in data centers
- **Minkyung Park**, Sungmin Sohn, Kwangwook Kwon, Ted "Taekyoung" Kwon
- IEEE Journal of Communications and Networks (JCN) (SCI-E) 2019

User-Centric Identity Management System Using Smart Contact
- Minhyeok Kang, **Minkyung Park**, and Ted "Taekyoung" Kwon
- Korean Institutes of Communications and Information Sciences Conference (KICS Conference) Jungsun, Korea 2018

An Automatic Attendance Checking System using Smartphones: An Infrastructureless Approach
- Selin Chun, Myungchul Kwak, **Minkyung Park**, and Ted "Taekyoung" Kwon
- International Conference on Indoor Positioning and Indoor Navigation (IPIN) Sapporo, Japan 2017

Pay-Per-Use in User-Provided Networks: A Bitcoin-based Approach (poster)
- **Minkyung Park**, Soobin Park, Eunsang Cho and Ted "Taekyoung" Kwon
- International Conference on emerging Networking EXperiments and Technologies (ACM Conext) Incheon, Korea 2017

TwinPeaks: A New Approach for Certificateless Public Key Distribution
- Eunsang Cho,**Minkyung Park**, Ted "Taekyoung" Kwon
- IEEE Conference on Communications and Network Security (IEEE CNS) Philadelphia, USA 2016

Privacy-preserving Authoriztaion Scheme for the Internet of Things (poster)
- **Minkyung Park**, Eunsang Cho and Ted "Taekyoung" Kwon
- The 11th International Conference on Future Internet Technologies (CFI) Nanjing, China 2016

Multi Server Password Authenticated Key Exchange Using Attribute-based Encryption
- **Minkyung Park**, Eunsang Cho and Ted "Taekyoung" Kwon
- The Journal of Korean Institute of Communications and Information Sciences (JKICS) 2015

Multi Server Password Authenticated Key Exchange Using Attribute-based Encryption
- **Minkyung Park**, Eunsang Cho and Ted "Taekyoung" Kwon
- Korean Institutes of Communications and Information Sciences Conference (KICS Conference) Jungsun, Korea 2015

Complete List of Projects

Development of Homomorphic Encryption and Trusted Execution Environment for Data Privacy
- Supported by Ministry of SMEs and Startups — June 2022 — Present

Research on Grey-box Fuzzing Techniques for TLS Protocol
- Supported by KOREA INSTITUTE OF INFORMATION SECURITY & CRYPTOLOGY (KIISC) — March 2022 — November 2022

Research on Traceability for Data Stability on Cloud-edge Lifecycle
- Supported by Institute for Information and Communications Technology Promotion (IITP) — April 2020 — December 2021

Research on GPU Acceleration for Fully Homomorphic Encryption (FHE)
- Supported by KOREA INSTITUTE OF INFORMATION SECURITY & CRYPTOLOGY (KIISC) — Febrary 2020 — November 2020

Developing high-performance programming environments and computing systems
- Supported by National Research Foundation of Korea (NRF) — November 2016 — June 2021

Research on Security Scheme for Interconnection of Heterogeneous Networks
- Supported by Electronics and Telecommunications Research Institute (ETRI) — June 2019 — November 2019

Research on Decentralized Internet Architecture
- Supported by Electronics and Telecommunications Research Institute (ETRI) — March 2019 — November 2019

Research on Security for Data-centric Platform
- Supported by Electronics and Telecommunications Research Institute (ETRI) — November 2017 — March 2018

Research on Trust and Security Scheme for Interconnection of Heterogeneous Networks
- Supported by Electronics and Telecommunications Research Institute (ETRI) — September 2018 — November 2018

Smartcampus: A Research on Localization Scheme based on Multiple Sensors
- Supported by Samsung Electronics — May 2016 — December 2019

Mashup API Design Consultation for the Advancement of IoT Platform
- Supported by JC square — January 2016 — March 2016

Development of Network Security Acceleration for Next-generation Low-power SoC
- Supported by Samsung Electronics — July 2015 — December 2015

Study on IP-based IoT Security Architecture
- Supported by SK Telecom — October 2014 — December 2014

Content Delivery Framework Using Spatial and Temporal Dynamics in Mobile networks
- Supported by National Research Foundation of Korea (NRF) — March 2014 — April 2016