Minkyung Park

Security Researcher

✉ tnstnii23@gmail.com
linkedin.com/in/mk-alsroad
alsroad.github.io

I am a security researcher with a focus on system and network security. My research involves designing privacy-preserving system architectures and analyzing the security of programs.

Research Area

Trusted Execution Environment (Intel SGX, Arm TrustZone, Side-Channel Attacks)
Information Flow Control, Program Analysis (Fuzz Testing, Secure Multi-Execution, Taint Tracking, Static Analysis)
Authentication and authorization (PKI, TLS, DNS security, etc.)
Network Protocol (Layer 3 – Layer 4)
User privacy (tracking/fingerprinting and privacy-preserving computations)
Programming Language: C/C++ (Proficient), Intel Assembly, Python, Go, etc.

Professional Experience

Postdoctoral Researcher, *Software and System Security Laboratory, University of Texas at Dallas* November 2023 — Current

- Research on Fuzzing Techniques for Embedded Systems
- Research on Privacy Attacks in Deep Learning Using Side-Channel Information

Postdoctoral Researcher, *Network Convergence and Security Laboratory, Seoul National University* September 2022 — July 2023

- Design and implementing privacy-enhancing frameworks (in Linux and TEE environments)
- Analyzing network protocol specification and its implementations to identify potential security threats and vulnerabilities

Education

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

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

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

Selected Papers

PAVE: Information Flow Control for Privacy-preserving Online Data Processing Services

- **Minkyung Park**, Jaeseung Choi, Hyeonmin Lee, and Taekyoung Kwon
- Architectural Support for Programming Languages and Operating Systems (ASPLOS); Top Conference; March 2025

TZ-DATASHIELD: Automated Data Protection for Embedded Systems via Data-Flow-Based Compartmentalization

- Zelun Kong, **Minkyung Park**, Le Guan, Ning Zhang, Chung Hwan Kim
- Network and Distributed System Security Symposium (NDSS); Top Conference, 2025

An SGX-Based Key Management Framework for Data Centric Networking

- **Minkyung Park**, Jeongnyeo Kim, Youngho Kim, Eunsang Cho, Soobin Park, Sungmin Sohn, Minhyeok Kang, Taekyoung 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

- **Minkyung Park**, Sungmin Sohn, Kwangwook Kwon, Taekyoung Kwon
- IEEE Journal of Communications and Networks (JCN); SCI-E, 2019
- Keywords: Data Center Networking, Transport Layer Protocol

Selected Projects

Research on Fuzzing Techniques for Embedded Systems

- Role: Design and implement a fuzzer to find vulnerabilities in firmware
- Keywords: Fuzzing, static analysis, firmware, Arm Cortex-M Dev 2024 — Present

Research on Privacy Attacks in Deep Learning Using Side-Channel Information

- Role: Design and implement model extraction attacks on deep neural networks (DNNs)
- Keywords: DNN, side-channel attacks, Intel SGX, model extraction attacks Nov 2023 — 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 March 2022 — November 2022

Minkyung Park

Security Researcher

✉ tnstnii23@gmail.com

linkedin.com/in/mk-alsroad

🌐 alsroad.github.io

Misc activities

Technical Advisor (volunteer work), Global IT Challenge

- Facilitated quiz activities and provided IT guidance at the IT Challenge, an international event supporting 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

Complete List of Papers

PAVE: Information Flow Control for Privacy-preserving Online Data Processing Services

- Minkyung Park, Jaeseung Choi, Hyeonmin Lee, and Taekyoung Kwon
- ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), March 2025

TZ-DATASHIELD: Automated Data Protection for Embedded Systems via Data-Flow-Based Compartmentalization

- Zelun Kong, Minkyung Park, Le Guan, Ning Zhang, Chung Hwan Kim
- Network and Distributed System Security Symposium (NDSS), February 2025

A Study on Fuzzing the Linux Kernel Networking Subsystem Using Syzkaller

- Subin Song, Minkyung Park, and Taekyoung Kwon
- Annual Symposium of KIPS (ASK), May 2024

How to decentralized the internet: A focus on data consolidation and user privacy

- Ted “Taekyoung” Kwon, Junghwan Song, Heeyoung Jung, Selin Chun, Hyunwoo Lee, Minhyeok Kang, Minkyoung Park, Eunsang Cho
- Computer Networks, Volume 234, October 2023

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

Research on Fuzzing Techniques for Embedded Systems
- Role: Design and implement a fuzzer to find vulnerabilities in firmware
- Keywords: Fuzzing, static analysis, firmware, Arm Cortex-M — December 2024 — Present

Research on Privacy Attacks in Deep Learning Using Side-Channel Information
- Role: Design and implement model extraction attacks on deep neural networks (DNNs)
- Keywords: DNN, side-channel attacks, Intel SGX, model extraction attacks — November 2023 — Present

Development of Homomorphic Encryption and Trusted Execution Environment for Data Privacy
- Funded by Ministry of SMEs and Startups — June 2022 — July 2023

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

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

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

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

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

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

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

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

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

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

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

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

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