Minkyung Park

Postdoctoral Research Associate | University of Texas at Dallas (UTD)

mk-alsroad
alsroad.github.io
minkyung.park@utdallas.edu

I am a security researcher with a focus on system and network security.

Research Area

Confidential Computing Design secure systems based on TEEs (Trusted Execution Environments) such as Intel SGX and Arm TrustZone, and analyze their side-channel vulnerabilities.
Network Security Develop and optimize secure end-to-end architectures, including PKI/TLS, authentication, and authorization protocols.
Program Analysis Create novel program analysis techniques to study program behaviors and uncover security flaws (Fuzz Testing, Secure Multi-Execution, Taint Tracking, Static Analysis)
Network Protocol Research and improve protocols at Layers 3–4
User privacy Investigate tracking/fingerprinting techniques and design privacy-preserving computation methods

Professional Experience

Postdoctoral Researcher, *Dept. Computer Science, University of Texas at Dallas* Nov. 2023 — Current
- PI: Prof. Chung Hwan Kim

Postdoctoral Researcher, *Dept. Computer Science and Engineering, Seoul National University* Sep. 2022 — July 2023
- PI: Prof. Taekyoung "Ted" Kwon

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

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

Publications (C: Conference | J: Journal | P: Poster)

[C17] DNN Latency Sequencing: Extracting DNN Architectures from Intel SGX Enclaves with Single-Stepping Attacks (to appear)
- **Minkyung Park**, Zelun Kong, Dave (Jing) Tian, Z. Berkay Celik, and Chung Hwan Kim Top Conference
- Network and Distributed System Security Symposium (NDSS), February 2026
- 한국정보과학회 최우수 학회, BK21플러스 IF Score 2

[C16] PAVE: Information Flow Control for Privacy-preserving Online Data Processing Services
- **Minkyung Park**, Jaeseung Choi, Hyeonmin Lee, and Taekyoung Kwon Top Conference
- ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), March 2025
- 한국정보과학회 최우수 학회, BK21플러스 IF Score 4

[C15] TZ-DATASHIELD: Automated Data Protection for Embedded Systems via Data-Flow-Based Compartmentalization
- Zelun Kong, **Minkyung Park**, Le Guan, Ning Zhang, Chung Hwan Kim Top Conference
- Network and Distributed System Security Symposium (NDSS), February 2025
- 한국정보과학회 최우수 학회, BK21플러스 IF Score 2

[C14] 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

[J13] 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
- SCI-E

[J12] 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
- Computer Networks, July 2020
- SCI-E

[J11] 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 2020
- SCI-E

[J10] 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) 2019
- SCI-E

[C9] 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
- International Workshop on Information Security Applications (WISA), 2019

[C8] 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

[C7] 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

[P6] 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

[C5] 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

[C4] 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

[P3] 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

[J2] 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

[C1] 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

Patents

동형 암호 병렬 연산 방법 및 이를 수행하는 컴퓨팅 장치 **(Homomorphic cryptographic parallel computation method and computing device performing the same method)**
- 권태경, 박민경, 강민혁, 천세린, 이현민
- Registration No. 10-2513552

데이터센터 네트워크의 부하 균형을 위한 신용 기반 다중경로 데이터 전송 방법 **(CREDIT-BASED MULTIPATH TRANSMISSION METHOD FOR DATACENTER NETWORK LOAD BALANCING)**
- 권태경, 최대진, 박민경, 손성민
- Registration No. 10-1932138

Projects

Research on Fuzzing Techniques for libraries
- Role: Design and implement a fuzzer to find vulnerabilities in libraries
- Keywords: Fuzz testing — 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 — November 2024

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

MISCELLANEOUS

Technical Advisor (volunteer work), Global IT Challenge
- Facilitated quiz activities and provided IT guidance at the IT Challenge, an international event supporting disabled children. — March 2016 –– February 2017

Researcher, Samsung Software Membership
- Samsung Software Membership is an IT training program supported by Samsung Electronics. — January 2012 –– December 2013

References

Prof. Ted "Taekyoung" Kwon, Seoul National University
- ✉tkkwon@snu.ac.kr

Prof. Chung Hwan Kim, University of Texas at Dallas
- ✉chungkim@utdallas.edu