Sanghak Oh

CONTACT INFORMATION

Department of Computer Science and Engineering
College of Computing
Hanyang University ERICA, Ansan, Korea

office: +82 31 400 1038
mobile: +82 10 6525 5466
e-mail: sanghak@hanyang.ac.kr

RESEARCH INTEREST

Network Security, Usable Security, AI Security, and Security Engineering

EDUCATION

Ph.D Department of Electrical and Computer Engineering, Sungkyunkwan University, Korea **2021-2026**

- Advisor: Prof. Hyoungshick Kim
- Thesis: Robust Application Fingerprinting on Encrypted Network Traffic

M.S Department of Software, Sungkyunkwan University, Korea **2015-2017**

- Advisor: Prof. Hyoungshick Kim
- Thesis: Empirical Analysis of SSL/TLS Weaknesses in Real Websites: Who Cares?

B.S Department of Software, Sungkyunkwan University, Korea **2011-2015**

- Advisor: Prof. Hyoungshick Kim

PROFESSIONAL EXPERIENCE

Hanyang University ERICA, Ansan, Korea
Assistant Professor **2026-Present**

Sungkyunkwan University, Suwon, Korea
Postdoctoral Researcher - Security Engineering Laboratory **2026**

Korea Military Academy, Seoul, Korea
Assistant Professor - Department of Computer Science **2018-2020**
Lecturer - Department of Computer Science **2017-2018**

PUBLICATIONS

CONFERENCES & JOURNALS

* indicates equal contributions.

CCA-Droid: Context-Aware Cryptographic API Misuse Detection in Android Apps.
Minwook Lee, Eunsoo Kim, **Sanghak Oh**, Joonsang Baek, Willy Susilo, and Hyoungshick Kim.
ASIACCS'26: The 21st ACM Asia Conference on Computer and Communications Security.

PP-Vul: Privacy-Preserving Vulnerability Detection Using Homomorphic Encryption.
Seungho Kim, Seonhye Park, Jihun Kim, Eunsoo Kim, **Sanghak Oh**, Hyunmin Choi, and Hyoungshick Kim.
ASIACCS'26: The 21st ACM Asia Conference on Computer and Communications Security.

When Does Wasm Malware Detection Fail? A Systematic Analysis of Their Robustness to Evasion.
Taeyoung Kim, **Sanghak Oh**, Kiho Lee, Weihang Wang, Yonghwi Kwon, Sanghyun Hong, and Hyoungshick Kim.
ASE'25: The 40th IEEE/ACM International Conference on Automated Software Engineering.

Windows plays Jenga: Uncovering Design Weaknesses in Windows File System Security.
Dong-uk Kim*, Junyoung Park*, **Sanghak Oh**, Hyoungshick Kim and Insu Yun.
CCS'25: The 32nd ACM Conference on Computer and Communications Security.

Understanding and Improving User Adoption and Security Awareness in Password Checkup Services.
Sanghak Oh, Heewon Baek, Jun Ho Huh, Taeyoung Kim, Woojin Jeon, Ian Oakley, and Hyoungshick Kim.
CHI'25: The 43rd ACM SIGCHI Conference on Human Factors in Computing Systems.

Poisoned ChatGPT Finds Work for Idle Hands: Exploring Developers' Coding Practices with Insecure Suggestions from Poisoned AI Models.
Sanghak Oh*, Kiho Lee*, Seonhye Park, Doowon Kim, and Hyoungshick Kim.
S&P'24: The 45th IEEE Symposium on Security and Privacy.

AppSniffer: Towards Robust Mobile App Fingerprinting Against VPN.
Sanghak Oh, Minwook Lee, Hyunwoo Lee, Elisa Bertino, and Hyoungshick Kim.
TheWebConf'23: The 32nd ACM Web Conference (formerly WWW).

A Comparative Study of Time Series Anomaly Detection Models for Industrial Control Systems.
Bedeuro Kim, Mohsen Ali Alawami, Eunsoo Kim, **Sanghak Oh**, Jeongyong Park, and Hyoungshick Kim.
Sensors 2023.

Wrong Siren! A Location Spoofing Attack on Indoor Positioning Systems: The Starbucks Case Study.
Junsung Cho, Jaegwan Yu, **Sanghak Oh**, Jungwoo Ryoo, Jaeseung Song and Hyoungshick Kim.
IEEE Communications Magazine 2017.

A Flexible Architecture for Orchestrating Network Security Functions to Support High-Level Security Policies.
Sanghak Oh, Eunsoo Kim, Jaehoon Jeong, Hoon Ko and Hyoungshick Kim.
IMCOM'17: The 11th ACM International Conference on Ubiquitous Information Management and Communication.

Empirical Analysis of SSL/TLS Weaknesses in Real Websites: Who Cares?
Sanghak Oh, Eunsoo Kim, and Hyoungshick Kim.
WISA'16: The 17th World Conference on Information Security Applications.

POSTERS

Insecure Coding Habits Die Hard. Can PEFT Really Turn LLMs into Secure Coders?
Sangjun Chae, Jangseop Choi, Taeyang Kim, Eun Jung, **Sanghak Oh** and Hyoungshick Kim.
CCS'25: The 32nd ACM Conference on Computer and Communications Security.

Adversarial Perturbation Attacks on the State-of-the-Art Cryptojacking Detection System in IoT Networks.
Kiho Lee, **Sanghak Oh** and Hyoungshick Kim.
CCS'22: The 29th ACM Conference on Computer and Communications Security.

Teaching

Teaching Assistant, Sungkyunkwan University: Algorithms (2022-2023)

Teaching Assistant, Sungkyunkwan University: Advanced in Information Security (2022)

Teaching Assistant, Sungkyunkwan University: Computer Security (2022)

Teaching Assistant, Sungkyunkwan University: Security Engineering (2021-2022)

Assistant Professor, Korea Military Academy: Algorithms of Information Security (2020)

Assistant Professor, Korea Military Academy: Basic Programming Languages (2019-2020)

Assistant Professor, Korea Military Academy: Discrete Mathematics (2019)

Assistant Professor, Korea Military Academy: Introduction to Cyber Warfare (2018-2019)

Lecturer, Korea Military Academy: Introduction to Cyber Warfare (2017)

Lecturer, Korea Military Academy: Introduction to Computer Science (2017-2018)

Teaching Assistant, Sungkyunkwan University: Security Engineering (2016)

Awards

Outstanding Student Researcher Award, Telecommunications Technology Association	**2025**
Superior Research Award (Runner up), Sungkyunkwan University	**2023**
Excellent Paper Award, CISC 2021	**2021**
Academic Excellence Scholarship, Sungkyunkwan University	**2021-2022**
National Cryptography Competition, National Security Research Institute	**2015**
National Science & Technology Scholarship, Korea Student Aid Foundation	**2011**

Academic Services

External Reviewer

ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)	**2026**
IEEE/ACM Transactions on Networking	**2023**

Patents

Hyoungshick Kim, **Sanghak Oh**. "A Traffic Detection Apparatus and Method for Enhancing Security of Mobile Application Fingerprinting," KR-Patent (10-2947377), 2026.

Jaehoon (Paul) Jeong, Hyoungshick Kim, **Sanghak Oh**, Eunsoo Kim. "An Apparatus and Method for Security Management in Network Functions Virtualization," KR-Patent (10-1863236), 2018.

References

Hyoungshick Kim
Professor
Department of Computer Science and Engineering
Sungkyunkwan University
e-mail: *Available Upon Request*

Elisa Bertino
Professor
Department of Computer Science
Purdue University
e-mail: *Available Upon Request*

Yonghwi Kwon
Assistant Professor
Department of Electrical and Computer Engineering
University of Maryland
e-mail: *Available Upon Request*

Doowon Kim
Assistant Professor
Department of Electrical Engineering and Computer Science
University of Tennessee, Knoxville
e-mail: *Available Upon Request*

Hyunwoo Lee
Assistant Professor
Department of Energy Engineering
Korea Institute of Energy Technology
e-mail: *Available Upon Request*