

Kiho Lee

Visiting Scholar of Cybersecurity & AI Research
University of Tennessee, Knoxville, TN
klee120@utk.edu — [GitHub Profile](#) — [LinkedIn](#)

RESEARCH INTERESTS

AI for Cybersecurity [\[USENIX '24\]](#) [\[WWW '24\]](#) | [\[IEEE S&P '24\]](#) | [\[CCS '22\]](#)

APPOINTMENTS

University of Tennessee, Knoxville, Knoxville, TN Jan. 2024 — Present
Visiting Scholar for Cybersecurity & AI Research
Advisor: Prof. Doowon Kim

EDUCATION

Sungkyunkwan University (SKKU), Suwon, South Korea Mar. 2022 — Feb. 2024
M.S. in Computer Science and Engineering (Convergence Security Track) Cumulative GPA: 4.31/4.5
Advisor: Prof. Hyoungshick Kim

Hongik University, Seoul, South Korea Mar. 2015 — Feb. 2019
B.E. in Computer Science and Engineering

PEER-REVIEWED CONFERENCE PUBLICATIONS

* Underline: 1st author.

Submitted / Under Review

Parameter-Efficient Fine-Tuning for Secure Code Generation with Large Language Models

Kiho Lee, Jungkon Kim, Daehoon Ko, Hyoungshick Kim, and Doowon Kim

Under review, submitted to [\[FSE '25\]](#)

On the Effectiveness and Robustness of Visual Similarity-based Phishing Detection Models

Under review, submitted to [\[NDSS '25\]](#)

Do Phishing Attackers Consider Security? Comprehensive Analysis of the Phishing Ecosystem with Security Configurations

Under review, submitted to [\[NDSS '25\]](#)

Refereed Conference Proceedings

C.3.An LLM-Assisted Easy-to-Trigger Poisoning Attack on Code Completion Models: Injecting Disguised Vulnerabilities against Strong Detection [\[PDF\]](#)

Shenao Yan, Shen Wang, Yue Duan, Hanbin Hong, **Kiho Lee**, Doowon Kim, and Yuan Hong

[\[USENIX Security '24\]](#): The 33rd USENIX Security Symposium (USENIX Security) 2024.

C.2.Poisoned ChatGPT Finds Work for Idle Hands: Exploring Developers' Coding Practices with Insecure Suggestions from Poisoned AI Models [\[PDF\]](#)

Sanghak Oh, **Kiho Lee**, Seonhye Park, Doowon Kim, and Hyoungshick Kim

[\[IEEE S&P '24\]](#): The 45th IEEE Symposium on Security and Privacy, San Francisco, USA, 2024.

C.1.AdFlush: A Real-World Deployable Machine Learning Solution for Effective Advertisement and Web Tracker Prevention [\[PDF\]](#) [\[CODE\]](#)

Kiho Lee, Chaejin Lim, Beomjin Jin, Taeyoung Kim, and Hyoungshick Kim

[\[WWW '24\]](#): The 33rd World Wide Web Conference, Singapore, 2024.

Refereed Posters and Demos

P.1. Adversarial Perturbation Attacks on the State-of-the-Art Cryptojacking Detection System in IoT Networks (Poster) [\[PDF\]](#)

Kiho Lee, Sanghak Oh, and Hyoungshick Kim

[\[CCS '22\]](#): The 29th ACM Conference on Computer and Communications Security, Los Angeles, USA, 2022.

SERVICES

- ACM **TheWebConf (World Wide Web) Conference Security Reviewer**, 2025
- The 34th **USENIX Security Symposium Artifact Evaluation Program Committee**, 2025

HONORS & AWARDS

- Best Student Researcher Award, Sungkyunkwan University, 2024
- Simsan Scholarship (Outstanding Graduate Student), Sungkyunkwan University, 2023
- SKKU CTF Challenge 2nd place, Sungkyunkwan University, 2023
- Software Development Security Hackathon 2st place, Korea Internet & Security Agency (KISA), 2023
- AI Security Technology Detection Competition 1st place, Korea Internet & Security Agency (KISA), 2021

WORK EXPERIENCE

Republic of Korea Army (Military service, Army ROTC), South Korea Mar. 2019 — Jun. 2021

- Cyber Intelligence Operations Officer (1st Lieutenant)
- Radio and Tactical Satellite Platoon Leader (2nd Lieutenant)

UPSYSTEMS, Inc., South Korea

- Intern - Software Versioning, Managing IDS/IPS Policies Dec. 2015 — Jun. 2016
- Software Developer (Remote) - Developing File Encryption Systems Jan. 2023 — Jun. 2024

PROJECTS

Machine learning-based web tracker prevention framework Jun. 2022 — Dec. 2023

Korea Internet & Security Agency (KISA), South Korea

Implementing an auto code generation with fine-tuned large language model Mar. 2023 — Dec. 2023

Electronics and Telecommunications Research Institute (ETRI), South Korea

Unsupervised learning-based anomaly detection for industrial control systems Mar. 2022 — Dec. 2022

National Security Research Institute (NSR), South Korea

Implementing the Gidra Emulation Plugin for firmware rehosting May. 2022 — Nov. 2022

National Security Research Institute (NSR), South Korea

SKILLS

Language: C/C++; Rust; Python; JavaScript (TypeScript); SQL (PostgreSQL; SQLite3); Shell;

OS: Debian (Ubuntu; Kali Linux); CentOS; OpenBSD;

Machine learning: Pytorch; Tensorflow; AWS SageMaker; PEFT; DeepSpeed; HuggingFace;

Security:

- **Penetration testing:** Web applications; Burp Suite; Postman; Active Directory; OWASP ZAP;

- **Reverse Engineering:** Ghidra; IDA PRO;

REFERENCES

Prof. Doowon Kim

Assistant Professor of Electrical Engineering and Computer Science, University of Tennessee, Knoxville

E-mail: doowon@utk.edu

Prof. Hyounghshick Kim

Associate Professor of Electrical Engineering and Computer Science, Sungkyunkwan University, South Korea

E-mail: hyoung@skku.edu