Jeonghyun Sim

Seoul, South Korea wjdgus0425@korea.ac.kr Jeonghyun516

Education

Korea University, Information Security — Seoul, South Korea
Sept 2025 – present
- Thesis Advisor: Prof. Huy Kang Kim
- Hacking and Countermeasure Research Lab (HCRL), Graduate School of Information Security
- GPA: 4.22 / 4.5

Dankook University, Industrial Security — Jukjeon, South Korea
Mar 2020 – Aug 2025
- Intelligent Security Technology Lab (ISTL), Department of Industrial Security
- GPA: 3.85 / 4.5

Experience

HCRL, Korea University, M.S. Student Researcher — Seoul, South Korea
Sept 2025 – present
1 year 3 months
- Threat Modeling and Cyber Attack Defense Simulation for Future Unmanned Vehicles (NRF, May 2026 – Present): RL-based attack/defense agent development
- Development of Common Core Security Technologies for Unmanned Vehicles (NRF, Jan. 2026 – Present): adversarial attacks & defenses on AV perception
- AutoHack Dataset Construction for Automotive Security Research (Korea University, Oct. 2025 – Dec. 2025): real-vehicle CAN attack dataset construction & validation

ISTL, Dankook University, Undergraduate Research Assistant — Jukjeon, South Korea
Apr 2024 – Oct 2024
7 months
- ML-Based Anomaly Detection for File System Metadata (National Security Research Institute): metadata preprocessing and ML model training

Publications

A Generalized Framework for Adversarial Attack Detection and Prevention Using Grad-CAM and Clustering Techniques — Jan 2025
J. H. Sim, H. M. Song
10.3390/systems13020088 (Systems, vol. 13, no. 2, p. 88)

Autoencoder-based Denoising Defense against Adversarial Attacks on Object Detection (Technical Report) — Dec 2025
M. G. Song, G. M. Kim, W. Kim, Y. Kim, **J. H. Sim**, S. Park, H. K. Kim
arxiv.org/abs/2512.16123 (arXiv:2512.16123)

Adversarial Attack Detection Method for Image Classification Models Based on Attention Mechanism — June 2024
J. H. Sim, H. M. Song
(Proceedings of the KIISC Summer Conference, vol. 34, no. 1, pp. 51–54)

Autoencoder-Based Defense Technique against One-Pixel Adversarial Attacks in Image Classification — Dec 2023
J. H. Sim, H. M. Song
(Journal of the Korea Institute of Information Security & Cryptology, vol. 33, no. 6, pp. 1013–1025)

Under Review

- **First author** — LLM multi-agent system security: intent alignment for detecting intentional misalignment in agent reasoning (JCR Q1 journal)
- **Co-author** — Autonomous driving perception robustness: two-stage restoration framework for robust object detection under adversarial perturbation (JCR Q1 journal)

Patents

- High-Frequency Correlation-Based Transformer Model for Adversarial Example Restoration in Autonomous Driving Images — KR Patent Application No. 10-2025-0166315, filed Nov. 6, 2025 (pending)
- Multi-Channel Image-Based Cyber Attack Detection System Using Feature Group-Based Multi-Dataset Integration in UAV Environments — KR Patent Application No. 10-2025-0161718, filed Oct. 31, 2025 (pending)

Awards

BK21 FOUR Graduate Research Fellowship Sept 2025
Selected as a high-achieving graduate researcher under the Brain Korea 21 Project (Phase 4)
National Research Foundation & Ministry of Education, South Korea

Bronze Prize, Daou Technology Undergraduate Programming Contest Jan 2023
Daou Technology

Grand Prize, Security Convergence Idea Hackathon Oct 2022
Dankook University

Skills

Programming Languages

Frameworks & Libraries

Tools