WOOHYUK CHOI / Ph.D. Student

Dept. of Electrical and Computer Engineering
Seoul National University
South Korea

Phone: (+82) 10-9173-4357 | Mail: 00cwooh@snu.ac.kr | Lab: CompSec at SNU
Web: cw00h.github.io | Google Scholar

Last updated: November 24, 2026

ABOUT ME

I am a Ph.D. student in Electrical and Computer Engineering at Seoul National University, advised by Prof. Byoungyoung Lee. My research focuses on the security of AI agents, covering both new attack classes and system-level defenses. I discovered **Agent Data Injection (ADI)**, a new class of attacks that exploits the misinterpretation of untrusted data as trusted data in AI agents. I also designed **Prompt Flow Integrity** and **DualView**, system-level mitigations against prompt injection attacks in LLM agents. Beyond AI security, I have worked on system security, including a GPU-to-host memory attack and fuzzing the Linux kernel for race vulnerabilities.

RESEARCH INTERESTS

I am interested in **security for AI** and **system security** in general. In particular, my research focuses on **AI agent security**, i.e., discovering new classes of vulnerabilities in agentic systems and building system-level mitigations against prompt injection that can be deployed in practice.

PUBLICATIONS

- **Agent Data Injection Attacks are Realistic Threats to AI Agents**
  Woohyuk Choi*, Juhee Kim*, Taehyun Kang, Jihyeon Jeong, Luyi Xing, and Byoungyoung Lee
  arXiv:2607.05120, 2026 (* Equal contribution)

- **DualView: Preventing Indirect Prompt Injection in Personal AI Agents**
  Woohyuk Choi*, Juhee Kim*, Taehyun Kang, Youngmin Kim, and Byoungyoung Lee
  arXiv:2607.03821, 2026 (* Equal contribution)

- **GHost in the SHELL: A GPU-to-Host Memory Attack and Its Mitigation**
  Sihyun Roh, **Woohyuk Choi**, Jaeyoung Chung, Yoochan Lee, Suhwan Song and Byoungyoung Lee
  IEEE Symposium on Security and Privacy (S&P), 2026

- **Prompt Flow Integrity to Prevent Privilege Escalation in LLM Agents**
  Woohyuk Choi*, Juhee Kim*, and Byoungyoung Lee
  arXiv:2503.15547, 2025 (* Equal contribution)

EXPERIENCE

Internship, Samsung MX (Mobile eXperience), Security Engineering Group Jan 2024 - Feb 2024
Samsung MX, Suwon, South Korea
- Developed and tested an eSE-based Digital-Wallet Application for Samsung mobile devices.

PROJECTS

Race Vulnerability Discovery in Linux Kernel Binder System Calls Mar 2024 – Aug 2024
Platform Stability Committee (Governmental advisory board project)

- Extended Syzkaller with concurrency-aware fuzzing techniques (inspired by Segfuzz, a kernel race fuzzer) to uncover race vulnerabilities in Android Binder syscalls.

EDUCATION

Seoul National University Mar 2025 - Present
Seoul, South Korea *Anticipated Feb 2031*

Ph.D. in Electrical and Computer Engineering (Advisor: Byoungyoung Lee)

Seoul National University Mar 2019 - Feb 2025
Seoul, South Korea *military service (2 years)*

B.S. in Electrical and Computer Engineering

GPA: 3.95 (Major: 3.99)/4.30 (Summa Cum Laude)

AWARDS

Excellence Award, AI-based Vulnerability Discovery System Competition Nov 2025
Korea Institute of Information Security and Cryptology (KIISC), KRW 5,000,000 prize

- **Agent CLI Vulnerability Scanner.** Automated tooling to discover security vulnerabilities in AI agent CLI tools by analyzing command validation logic in minified JavaScript code.

SCHOLARSHIPS

- **Electrical and Computer Engineering Foundation (Seoul National University), Full tuition support**
  Sep 2025 - Present

TEACHING ASSISTANT

Programming Methodology (430.211) Spring 2026
Seoul National University

Programming Methodology (430.211) Spring 2025
Seoul National University