WOOHYUK CHOI / Ph.D.

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

Last updated: September 26, 2025

ABOUT ME

I am a Ph.D. student in Electrical and Computer Engineering at Seoul National University, advised by Prof. Byoungyoung Lee. I designed **Prompt Flow Integrity**, a system-level mitigation against prompt injection attacks in LLM agents, and my current research focuses on system-level defenses for web agents. In addition, I have hands-on experience in system security projects and vulnerability discovery, complementing my main focus on securing modern AI-driven systems.

RESEARCH INTERESTS

I am interested in **security for AI** and **system security** in general. In particular, my research focuses on **AI agent security**, e.g., system-level mitigation against prompt injection attacks for AI agents in several domains.

PUBLICATIONS

- **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 (SP) 2026 (accepted, to appear)

- **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.

System-level Mitigation against Prompt Injection Attacks in Web Agents Mar 2025 – Present
CompSec Lab, Seoul National University

EDUCATION

Seoul National University Mar 2025 - Present
Seoul, South Korea

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)

SCHOLARSHIPS

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

TEACHING ASSISTANT

Programming Methodology (430.211) Spring 2025
Seoul National University