

SEONWOOK KIM

seonwookkim@cmu.edu | linkedin.com/in/seonwook-kim | Pittsburgh, PA

Security Engineer with **8 years of experience** in offensive and product security at Samsung, specializing in **fuzzing, exploit chaining, and program analysis** across Android, Tizen, and embedded systems. Currently developing **LLM-driven vulnerability discovery systems** while completing an MS at **Carnegie Mellon University**.

EDUCATION

Carnegie Mellon University

Master of Science in Information Security (MSIS)

Pittsburgh, PA

Expected Dec 2027

Hanyang University

Bachelor of Science in Computer Science and Engineering

Seoul, South Korea

03/2012 - 02/2018

SKILLS

Languages: C, C++, Python, Java, JavaScript, Bash

Systems & Embedded: Linux, Android, Tizen, embedded IPC, networking and IoT connectivity protocols

Security & Program Analysis: AFL++, stateful fuzzing, GDB, IDA, AddressSanitizer, taint/data-flow analysis

Software Engineering: Java Spring, Node.js, REST APIs, data pipelines, job orchestration, Docker, Git, CI/CD

Security Automation: LLM-assisted vulnerability discovery, multi-agent workflows, deterministic output verification

EXPERIENCE

Samsung Electronics

Security Engineer

Seoul, South Korea

03/2020 - 08/2026

- Conducted product security assessments across Android, Tizen, Linux, web/backend, and embedded systems, covering application, IPC, network, and device interfaces; identified 30+ vulnerabilities including High/Critical issues.
- Developed AFL++-based stateful protocol fuzzing harnesses and custom mutators for IoTivity, an embedded connectivity stack, to exercise deep protocol states.
- Chained four independently discovered vulnerabilities with a publicly disclosed flaw to achieve shell access on production consumer hardware.
- Improved Android taint-analysis tooling built on FlowDroid and Soot by root-causing missed detections and fixing defects in analysis passes.
- Led a five-person Android deep-link security research effort that produced three validated attack chains comprising nine vulnerabilities; set technical direction and expanded individual findings into end-to-end impact scenarios.

Software Engineer

03/2018 - 02/2020

- Designed and operated backend orchestration services for AVAS, an enterprise vulnerability-analysis platform spanning 7,900+ repositories, coordinating static-analysis jobs and vulnerability-data ingestion at scale.
- Developed Java Spring backend services, Python data pipelines and crawlers, and GitHub CI integrations to ingest vulnerability data and run static-analysis engines at scale.

SECURITY RESEARCH & DISCLOSURES

GStreamer Vulnerability Research

- Identified memory-safety vulnerabilities across three GStreamer security advisories, resulting in four assigned CVEs (CVE-2026-73433, CVE-2026-73434, CVE-2026-19389, CVE-2026-19387).

ADDITIONAL

Languages: English (fluent), Korean (native)

Community: Authored three CTF challenges for Samsung Security Tech Forum's Hackers' Playground.