Jongseong Kim

nevul37@gmail.com | nevul37.github.io | linkedin.com/in/jongseongkim

Education

University of Illinois Urbana-Champaign, United States Starting Aug. 2026

Master of Science in Computer Science

Ajou University, Republic of Korea Mar. 2020 – Aug. 2025

Bachelor of Engineering in Cyber Security

- GPA: 4.02/4.5 (Top 5%)

Research Experiences

LLM-Agent for Race Condition Vulnerability Discovery in Windows Systems May. 2025 – Nov. 2025

Advisor: Prof. Lingming Zhang

- Created LLM-powered binary analysis frameworks integrating IDA Pro with agent-based reasoning to automate Windows COM race condition detection.
- Identified 24 Microsoft-confirmed vulnerabilities (**24 CVEs** assigned) including high impact sandbox escapes, achieving **$120k** in bounties through automated vulnerability discovery.

Fuzzing the Windows Userland with Automated Crash Classification Mar. 2024 – Jun. 2024

Advisor: Prof. Taeshik Shon

- Built a snapshot-based fuzzing framework for Windows userland applications using kAFL, featuring automated crash detection via exception handlers.
- Developed a system for automated crash dump collection utilizing vmcall instruction for hypervisor communication, enabling efficient vulnerability analysis and reproduction with call stacks and payloads.

Fuzzing the Windows Kernel Driver 203 ★ Aug. 2023 – Dec. 2023

Mentor: Jinho Jung

- Co-developed **msFuzz**, a Windows kernel driver fuzzing framework integrating Angr-based constraint discovery with kernel fuzzing
- Automated IOCTL constraint inference and harness generation for kernel drivers to expand coverage and improve crash discovery rate.
- Conducted vulnerability research across Windows, AMD, and device vendor drivers; contributed to coordinated disclosure.

Professional Experiences

Offensive Security Researcher, ENKI WhiteHat (Seoul, Republic of Korea) Sep. 2024 – Present

- Specialize in Windows offensive security research, analyzing kernel drivers and system internals.

Offensive Security Researcher, CW Research (Seoul, Republic of Korea) Mar. 2024 – Jul. 2024

- Researched Windows Kernel Security, focusing on fuzzing and vulnerability discovery in kernel drivers.

Signal Intelligence Analyst, Republic of Korea Army Dec. 2021 – Jun. 2023

Awards & Recognition

Microsoft Security Response Center (MSRC) Most Valuable Researcher (MVR)

Prestigious recognition for security researchers reporting high-impact vulnerabilities to Microsoft.

- MSRC Global Top 100: 2023 Q4 | 2024 Q2–Q4 | 2025 Q1–Q3 & Overall

DEF CON 33 Capture The Flag (CTF) — Team SuperDiceCode Aug. 2025

- Achieved **3rd place** in the most prestigious global CTF competition.

Information Security Specialized Scholarship, Ajou University Fall 2024, Spring 2024

- Awarded for outstanding achievements in the field of information security

Skills

Security Research: Binary Analysis (IDA Pro, Binary Ninja), Fuzzing (AFL-based Fuzzer), Vulnerability Discovery, Reverse Engineering, Exploit Development, Windows Internals

Programming Languages: C/C++, Python, x86/x64 Assembly

Research Focus: Windows COM/RPC Analysis, Windows Kernel Driver Analysis, LLM-based Binary Analysis

Conference Presentations

J. Kim, D. Kim (2025). COM-pletely Unplanned: A Windows Bug Hunter's Journey to LPE. Presentation at *Off-By-One 2025*, Singapore

S. Park, **J. Kim**, Y. Park (2024). 1-Click-Fuzz: Systematically Fuzzing the Windows Kernel Driver with Symbolic Execution. Presentation at *CODE BLUE 2024*, Tokyo, Japan

Vulnerability Research

Discovered and reported **100+ vulnerabilities** in commercial software, resulting in **60+ CVEs**.

CVE-2025-60717 — Windows Broadcast DVR User Service Vulnerability Microsoft (Nov. 2025)

CVE-2025-59515 — Windows Broadcast DVR User Service Vulnerability Microsoft (Nov. 2025)

CVE-2025-59210 — Windows ReFS Deduplication Service Vulnerability Microsoft (Oct. 2025)

CVE-2025-59198 — Windows Search Service Vulnerability Microsoft (Oct. 2025)

CVE-2025-59190 — Windows Search Service Vulnerability Microsoft (Oct. 2025)

CVE-2025-55691 — Windows PrintWorkflowUserSvc Vulnerability Microsoft (Oct. 2025)

CVE-2025-55690 — Windows PrintWorkflowUserSvc Vulnerability Microsoft (Oct. 2025)

CVE-2025-55689 — Windows PrintWorkflowUserSvc Vulnerability Microsoft (Oct. 2025)

CVE-2025-55688 — Windows PrintWorkflowUserSvc Vulnerability Microsoft (Oct. 2025)

CVE-2025-55686 — Windows PrintWorkflowUserSvc Vulnerability Microsoft (Oct. 2025)

CVE-2025-55685 — Windows PrintWorkflowUserSvc Vulnerability Microsoft (Oct. 2025)

CVE-2025-55684 — Windows PrintWorkflowUserSvc Vulnerability Microsoft (Oct. 2025)

CVE-2025-55677 — Windows Device Association Broker Service Vulnerability Microsoft (Oct. 2025)

CVE-2025-53150 — Windows Digital Media Service Vulnerability Microsoft (Oct. 2025)

CVE-2025-50174 — Windows Device Association Broker Service Vulnerability Microsoft (Oct. 2025)

CVE-2025-59289 — Windows Bluetooth Service Vulnerability Microsoft (Sep. 2025)

CVE-2025-59220 — Windows Bluetooth Service Vulnerability Microsoft (Sep. 2025)

CVE-2025-53802 — Windows Bluetooth Service Vulnerability Microsoft (Sep. 2025)

CVE-2025-53133 — Windows PrintWorkflowUserSvc Vulnerability Microsoft (Aug. 2025)

CVE-2025-49664 — Windows User-Mode Driver Framework Host Vulnerability Microsoft (Jul. 2025)

CVE-2025-29838 — Windows ExecutionContext Driver Vulnerability Microsoft (May. 2025)

CVE-2025-27730 — Windows Digital Media Service Vulnerability Microsoft (Apr. 2025)

CVE-2025-27476 — Windows Digital Media Service Vulnerability Microsoft (Apr. 2025)

CVE-2025-27475 — Windows Update Stack Vulnerability Microsoft (Apr. 2025)

CVE-2025-27467 — Windows Digital Media Service Vulnerability — Microsoft (Apr. 2025)

CVE-2025-26688 — Microsoft Virtual Hard Disk Vulnerability — Microsoft (Apr. 2025)

CVE-2025-21183 — Windows ReFS Deduplication Service Vulnerability — Microsoft (Feb. 2025)

CVE-2025-21182 — Windows ReFS Deduplication Service Vulnerability — Microsoft (Feb. 2025)

CVE-2025-21235 — Windows PrintWorkflowUserSvc Vulnerability — Microsoft (Jan. 2025)

CVE-2025-21234 — Windows PrintWorkflowUserSvc Vulnerability — Microsoft (Jan. 2025)

CVE-2024-49097 — Windows PrintWorkflowUserSvc Vulnerability — Microsoft (Dec. 2024)

CVE-2024-49095 — Windows PrintWorkflowUserSvc Vulnerability — Microsoft (Dec. 2024)

CVE-2024-43624 — Windows Hyper-V Shared Virtual Disk Vulnerability — Microsoft (Nov. 2024)

CVE-2024-38155 — Security Center Broker Vulnerability — Microsoft (Aug. 2024)

CVE-2024-21445 — Windows USB Print Driver Vulnerability — Microsoft (Mar. 2024)

CVE-2024-21442 — Windows USB Print Driver Vulnerability — Microsoft (Mar. 2024)

CVE-2024-20653 — Microsoft Common Log File System Vulnerability — Microsoft (Jan. 2024)

CVE-2023-42833 — Webkit Remote Code Execution Vulnerability — Apple (Sep. 2023)

CVE-2023-35074 — Webkit Remote Code Execution Vulnerability — Apple (Sep. 2023)

Other Vendors (Mitsubishi, MSI, AMD, SIEMENS, Open-source, etc.):
CVE-2025-48071, CVE-2024-26314, CVE-2024-25088, CVE-2024-25087, CVE-2024-25086, CVE-2024-22106, CVE-2024-22105, CVE-2024-22104, CVE-2024-22103, CVE-2024-22102, CVE-2023-51778, CVE-2023-51777, CVE-2023-51776, CVE-2023-47572, CVE-2023-47571, CVE-2023-47569, CVE-2023-47450, CVE-2023-46859, CVE-2023-46280, CVE-2023-31341, CVE-2022-2598, CVE-2022-2549

Other Research:
Discovered and reported **40+ vulnerabilities** in various Korean security software products, including antivirus solutions, EDR platforms, and system utilities.