

Sang Jun “Gabriel” Kim

U.S. Permanent Resident

(646) 881-7190 | sjkksj03@gmail.com

Portfolio: sjkcyber.com | LinkedIn: www.linkedin.com/in/sang-jun-kim

Education:

University at Albany, Albany, NY - Cybersecurity B.S. | May 2026

Research Experience:

University at Albany - Research Assistant - 2026

Cyber Cascade Risk (CCR)

Project: Assessing Zero Trust Segmentation in IoT & Legacy Environments

- Designing and implementing a Zero Trust architecture for an IoT environment using network segmentation (Attacker/IoT/Admin zones).
- Conducting MITM and packet-capture attacks (Wi-Fi Pineapple, Kali Linux, Wireshark) to analyze lateral movement and validate segmentation effectiveness.

Cognitive-Security, Accountability, Fairness and Explainability (CAFÉ) Lab

Project: Behavioral Pattern Extraction & Early Detection of Emerging 01flip Ransomware Using Automated Host Log Analysis

- Built and configured a Windows VM, and Cuckoo sandbox environment to safely execute 01flip ransomware sample, and analyze system behavior before and after infection.
- Analyzing host-level activity (file modification, process execution, and system changes) to identify behavioral patterns and compare detection gaps across ransomware families.

Cybersecurity & Cryptography Lab (CCL)

Project: Evaluating Cryptographic Protections & Trust Assumptions in Kernel-Level Anti-Cheat Architectures

- Building a controlled virtual environment to deploy and test open-source kernels-level Anti-Cheat drivers, analyzing system behavior and after execution.
- Evaluating trust enforcement and integrity mechanisms in kernel-level anti-cheat systems to identify privileged access risks and expanded attack surfaces.

Professional Experience:

Maggie McFly's - Server - Albany, NY

Dec 2024 - Present

- Promoted from food runner to server within one month based on performance, reliability, and ability to work in a fast-paced environment.
- Providing efficient customer service under pressure by managing multiple tasks, communicating effectively with customers and team members, and ensuring accurate transactions and consistent service standards.

Skills:

Languages: Korean (Native), English (Fluent)

Tools & Platforms: Kali Linux, Wireshark, Wi-Fi Pineapple, Nmap, SIEM, Windows VMs, GitHub, Visual Studio, Windows WDK, MITRE ATT&CK

Programming Languages: Bash, HTML/CSS, SQL (fundamentals)

Certifications: Google Cybersecurity Certificate (Expected by April 2026), CompTIA Security+ (Expected by June 2026)