Youngjoon Kim

Seoul, South Korea

School of Cybersecurity and Privacy, Georgia Tech
Security Researcher at Team Atlanta

acorn421.github.io
acorn421@gmail.com

Education

Korea University **Sep. 2018 – Feb. 2025**
***Ph.D.** in Information Security* *Seoul, Korea*

Korea University **Mar. 2013 – Feb. 2017**
***B.S.** in Cyber Defense* *Seoul, Korea*

Experience

Georgia Tech **Aug. 2025 – Present**
Postdoctoral Researcher *Atlanta, USA*

Korea University **Jun. 2025 – Aug. 2025**
Postdoctoral Researcher *Seoul, Korea*

Georgia Tech **Mar. 2025 – Apr. 2025**
Visiting Scholar *Georgia, USA*

- Developed a SARIF Assessment CRS for **AIxCC Final** as a member of **Team-Atlanta**.

R.O.K. Cyber Operation Command **Oct. 2022 – May. 2024**
Security Engineer *Seoul, Korea*

- Performed **vulnerability assessments** for R.O.K. military IT infrastructure.
- Worked as a **red team** during R.O.K. military cyber operation exercises.

Agency For Defense Development **Jul. 2017 – Sep. 2022**
Security Researcher *Seoul, Korea*

Research on National-level cyberattack defense technologies **Jan. 2021 – Sep. 2022**

- Goal: Organize adversaries' cyberattack operations into attack chains, categorize them into appropriate campaigns, and respond automatically to disrupt the attacker's ultimate goals.
- Researched predicting the next attack using Bayesian network and MITRE ATT&CK.

Research on techniques for evaluating binary fuzzing results **Jan. 2018 – Oct. 2020**

- Goal: Develop techniques to analyze and evaluate crashes generated from software fuzzing to identify root causes and automatically assess whether they could lead to vulnerabilities.
- Converted Linux-based taint analysis tool for Windows x64.
- Developed crash triage technique using additional directed fuzzing and taint analysis.

Publications

- **Logs In, Patches Out: Automated Vulnerability Repair via Tree-of-Thought LLM Analysis.**
  Youngjoon Kim, Sunguk Shin, Hyoungshick Kim*, and Jiwon Yoon*
  * *Corresponding authors*
  USENIX Security, 2025

- **Enhancing Graph Of Thought: Enhancing Prompts with LLM Rationales and Dynamic Temperature Control.**
  Sunguk Shin and **Youngjoon Kim***
  * *Corresponding author*
  International Conference on Learning Representations (ICLR), 2025

- **SCVMON: Data-oriented attack recovery for RVs based on safety-critical variable monitoring.**
  Sangbin Park, **Youngjoon Kim**, and Donghoon Lee
  International Symposium on Research in Attacks, Intrusions, and Defenses (RAID), 2023

- **BAN: Predicting APT Attack Based on Bayesian Network With MITRE ATT&CK Framework.**
  Youngjoon Kim, Insup Lee, Hyuk Kwon, Gyeongsik Lee, and Jiwon Yoon
  IEEE Access, 2023

- **A new approach to training more interpretable model with additional segmentation.**
  Sunguk Shin, **Youngjoon Kim** and Jiwon Yoon
  Pattern Recognition Letters, 2021

- **Maxafl: Maximizing code coverage with a gradient-based optimization technique.**
  Youngjoon Kim and Jiwon Yoon
  Electronics, 2020

Other Experiences

AIxCC Final — Dec. 2024 – Present

Member of Team ATLANTA

- Developed a SARIF Assessment module.
- Framework: CodeQL, SVF, SootUp
- Language: Python, Java

AIxCC Semi-final — Apr. 2024 – Aug. 2024

Tech Leader of Team KORIA

- Developing a Cyber Reasoning System for automatically identifying and patching open source vulnerabilities using LLM.

1-day Vulnerability Analysis — Apr. 2019 – Nov. 2021

Student Intern — *Sponsored by Korea University*

- Wrote a 1-day vulnerability analysis report and implemented proof-of-concept code as a Metasploit module.

Skills

Programming Languages: *Proficient* - C/C++, Python, Java / *Occasional* - JavaScript, Node.js, R, Solidity, Rust

Cloud Platforms: AWS, Google Cloud

Frameworks/Tools: AFL, Pintool, Burp suite, IDA, WinDBG, Langchain, PyTorch, TensorFlow