Youngjoon Kim (김영준)

Seoul, South Korea

☎ +82-10-5008-8028 ✉ acorn421@gmail.com t.me/acorn421

acorn421.github.io linkedin.com/in/acorn421 github.com/acorn421

Summary

I am a **captain of the R.O.K. Army** and a **Ph.D. student at Korea University**. I have experience in both security research and security engineering while working at **ADD** and **R.O.K. Cyber Operations Command**. Throughout my career, my main focus has been the **integration of AI and security**. In particular, I would like to apply AI to offensive security. To this end, academically, I am interested in AI-assisted **fuzzing**. Practically, I am interested in AI-assisted **penetration testing**. Recently, I started researching on finding vulnerabilities in **smart contracts**.

Work Experience

R.O.K. Cyber Operation Command — Oct. 2022 – Present

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.
- Analyzed **North Korea's cyberattack techniques** and simulated similar attack scenarios for cybersecurity training.
- Conducted **cybersecurity management ability assessment** for public institutions in South Korea.
- Keywords: Red team, Web hacking, Reverse engineering, Binary exploitation, APT attack
- Frameworks/Tools: Metasploit, Burp suite, IDA, WinDBG, Cobalt strike, Nmap, Python, C/C++, Powershell

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.
- Implemented network-level and host-level automatic defense using SDN.
- Keywords: APT Attack, Automatic response, MITRE ATT&CK, Bayesian Network, SDN
- Frameworks/Tools: MITRE ATT&CK, bnlearn, ONOS
- Language: Python, R, Javascript

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.
- Developed Linux-based taint analysis tool for Windows x64.
- Introduced crash triage technique using additional directed fuzzing and taint analysis.
- Keywords: Fuzzing, Crash triage, Crash prioritization, Root cause analysis, Dynamic binary instrumentation, Taint analysis
- Frameworks/Tools: WinAFL, libdft, WinDBG, Pintool, Dynamorio, Valgrind
- Language: Python, C/C++, Javascript

Research on cyber threat analysis and countermeasures for warship systems — **Jul. 2017 – Dec. 2017**

- Conducted threat analysis and proposed countermeasures for R.O.K. navy warship information systems based on NIST standards.
- Keywords: Threat analysis, Risk management, NIST SP 800-53, NIST SP 800-37, NIST SP 800-30

Plain Bagel, Inc — Mar. 2015 – Feb. 2017

Full Stack Developer(Part-time) — *Seoul, Korea*

Slidee: Platform for editing and sharing YouTube video stills — **Mar. 2015 – Feb. 2017**

- Built a web-based editor to convert YouTube videos into screenshots with captions.
- Built a web platform to share user-generated content.
- Implemented an ELK-based user and service statistics analysis server.
- Optimized cloud hosting and databases for reliable service and cost optimization.
- Framework/Tools: React, Redux, Express.js, MongoDB, ELK stack, AWS, Google Analytics
- Language: Python, Javascript, Node.js

Education

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

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

Hansung Science High School **Mar. 2011 – Feb 2013**
Seoul, Korea

Publications

- **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

Domestic Patents

- **DEVICE AND METHOD FOR DATA-ORIENTED ATTACK DETECTION AND RECOVERY FOR ROBOTIC VEHICLES BASED ON SAFETY-CRITICAL VARIABLES MONITORING.**
  Sangbin Park, **Youngjoon Kim**, and Donghun Lee
  Korean Patent 10-2023-0157140(application number), In review
- **SOFTWARE TAINT ANALYSIS METHOD AND SOFTWARE TAINT ANALYSIS DEVICE USING THE SAME.**
  Kyeongsik Lee, **Youngjoon Kim**, Younggi Park, and Hojun Lee
  Korean Patent 10-2344497-0000, 2021

Other Experiences

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.
- Framework: Metasploit, Django
- Language: Ruby, Python

SW Maestro **Jun. 2015 – Dec. 2015**
Developer *Sponsored by Ministry of Science and ICT*

Matnam **Sep. 2015 – Dec. 2015**

- Advertisement application for local restaurants through Instagram.
- Framework: Android SDK, Google Cloud, Google App Engine
- Language: Java

Random Routing Mutation **Jun. 2015 – Aug. 2015**

- Network security systems using SDN technology.
- Framework: ONOS, Mininet
- Language: Java

Android Malware Anlaysis **Mar. 2014 – Dec. 2014**
Student Intern *Sponsored by KISA*

- Decompiled a real malicious Android app and analyzed its malicious behavior.

- Framework: JEB Decompiler
- Language: Java

SGen club **Jul. 2012 – Jun. 2014**
Developer *Sponsored by Samsung SDS*

ENTOP: Entertainment Top 10 **Jan. 2014 – Jun. 2014**

- Website that recommends the BEST 10 based on user interests.
- Framework: Django, jQuery, MySQL
- Language: Python, Javascript

MIV **Jul. 2013 – Dec. 2013**

- Application that automatically recognizes the video's music and provides music information.
- Framework: Android SDK, MySQL
- Language: Java

LOVIE: MOVIE+LOVE **Jan. 2013 – Jun. 2013**

- Movie recommendation and review application for couples.
- Framework: Android SDK, MySQL
- Language: Java

MonsterAlarm **Jul. 2012 – Dec. 2012**

- Alarm application with game mechanics and nurturing concepts.
- Framework: Android SDK, sqlite
- Language: Java

Skills

Programming Languages: Proficient - C/C++, Python, Java, Occasional - Java, JavaScript, Node.js, R, Solidity, Rust
Cloud Platforms: *AWS*, Google Cloud
Frameworks/Tools: AFL, Pintool, Burp suite, IDA, WinDBG, PyTorch, TensorFlow, React, Git, MongoDB