# 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

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

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

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

**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

## 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*

## Publications

- Sangbin Park, **Youngjoon Kim**, and Donghoon Lee. **"SCVMON: Data-oriented attack recovery for RVs based on safety-critical variable monitoring."** RAID 2023.
- **Youngjoon Kim**, Insup Lee, Hyuk Kwon, Gyeongsik Lee, and Jiwon Yoon. **"BAN: Predicting APT Attack Based on Bayesian Network With MITRE ATT&CK Framework."** IEEE Access 2023.
- Sunguk Shin, **Youngjoon Kim** and Jiwon Yoon. **"A new approach to training more interpretable model with additional segmentation."** Pattern Recognition Letters 2021.
- **Youngjoon Kim** and Jiwon Yoon. **"Maxafl: Maximizing code coverage with a gradient-based optimization technique."** Electronics 2020.

## Skills

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