

Youngjoon Kim

Postdoc Researcher at [SSLab](#), Georgia Tech
Security Researcher at [Team Atlanta](#) (AlxCC Winner)

✉ youngjoon.kim@gatech.edu [🏠 youngjoon.kim](#) [🌐 acorn421](#) [🔗 acorn421](#)

EDUCATION

Korea University <i>Ph.D. in Information Security</i> Advisor: Jiwon Yoon Thesis: AI-Driven Automated Vulnerability Discovery and Repair	Sep. 2018 – Feb. 2025 <i>Seoul, Korea</i>
Korea University <i>B.S. in Cyber Defense</i>	Mar. 2013 – Feb. 2017 <i>Seoul, Korea</i>

EXPERIENCE

Georgia Tech <i>Postdoctoral Researcher</i> Supervisor: Taesoo Kim	Sep. 2025 – Present <i>Atlanta, USA</i>
Team Atlanta <i>Security Researcher</i> • Won <i>DARPA AlxCC Final</i> (\$4M prize) as a member developing <i>ATLANTIS</i>.	Dec. 2024 – Present
Korea University <i>Postdoctoral Researcher</i> Supervisor: Jiwon Yoon	Jun. 2025 – Aug. 2025 <i>Seoul, Korea</i>
R.O.K. Cyber Operation Command <i>Security Engineer (R.O.K. Army Captain)</i> • Performed <i>vulnerability assessments</i> for R.O.K. military IT infrastructure. • Discovered numerous <i>zero-day vulnerabilities</i> in Korean commercial software. • Worked as a <i>red team</i> during R.O.K. military cyber operation exercises. • Analyzed <i>North Korea's cyberattack techniques</i> and simulated similar attack scenarios for cybersecurity training. • Conducted <i>cybersecurity management ability assessment</i> for public institutions in South Korea.	Oct. 2022 – May 2024 <i>Seoul, Korea</i>
Agency For Defense Development <i>Security Researcher (R.O.K. Army Captain)</i>	Jul. 2017 – Sep. 2022 <i>Seoul, Korea</i>
Research on National-level cyberattack defense technologies • Developed a predictive model for next-stage attacks using Bayesian network and MITRE ATT&CK. • Implemented network-level and host-level automatic defense using SDN.	Jan. 2021 – Sep. 2022

- Ported a taint analysis framework from Linux to Windows x64.
- Developed a crash triage technique combining directed fuzzing and taint analysis.

PUBLICATIONS

PEER-REVIEWED PAPERS

- [C6] CtxFuzz: Context-Aware Directed Fuzzing via Runtime Fuzzer-Agent Cooperation.
Jiho Kim, Dongkwan Kim, HyungSeok Han, **Youngjoon Kim**, Soyeon Park, Sangwoo Ji, Joshua Wang, Dae R. Jeong, and Taesoo Kim
IEEE/ACM International Conference on Automated Software Engineering (ASE), 2026 (To appear)
- [C5] SoK: DARPA's AI Cyber Challenge (AIxCC): Competition Design, Architectures, and Lessons Learned.
Cen Zhang, Younggi Park, Fabian Fleischer, Yu-Fu Fu, Jiho Kim, Dongkwan Kim, **Youngjoon Kim**, Qingxiao Xu, Andrew Chin, Ze Sheng, Hanqing Zhao, Michael Pelican, David J. Musliner, Jeff Huang, Jon Silliman, Mikel Mcdaniel, Jefferson Casavant, Isaac Goldthwaite, Nicholas Vidovich, Matthew Lehman, and Taesoo Kim
USENIX Security, 2026 (To appear)
- [C4] OSS-CRS: Liberating AIxCC Cyber Reasoning Systems for Real-World Open-Source Security.
Andrew Chin, Dongkwan Kim, Yu-Fu Fu, Fabian Fleischer, **Youngjoon Kim**, HyungSeok Han, Cen Zhang, Brian Junekyu Lee, Hanqing Zhao, and Taesoo Kim
20th USENIX WOOT Conference on Offensive Technologies, 2026 (To appear)
- [C3] 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
- [C2] 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
- [C1] 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
- [J3] 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
- [J2] A new approach to training more interpretable model with additional segmentation.
Sunguk Shin, **Youngjoon Kim** and Jiwon Yoon
Pattern Recognition Letters, 2021
- [J1] MaxAFL: Maximizing code coverage with a gradient-based optimization technique.
Youngjoon Kim and Jiwon Yoon
Electronics, 2020

PREPRINTS

[P1] ATLANTIS: AI-driven Threat Localization, Analysis, and Triage Intelligence System.
Taesoo Kim, et al.
arXiv preprint arXiv:2509.14589, 2025

HONORS & AWARDS

DARPA AI Cyber Challenge (AIxCC) Final – 1st Place (\$4M prize)	Aug. 2025
<i>Member of Team Atlanta</i>	

OTHER EXPERIENCES

OSS-CRS	Sep. 2025 – Present
<i>Main Contributor</i>	
AIxCC Final (1st Place)	Dec. 2024 – Aug. 2025
<i>Member of Team Atlanta</i>	
AIxCC Semi-final	Apr. 2024 – Aug. 2024
<i>Tech Leader of Team KORIA</i>	