Dongkwan Kim

Cybersecurity Engineer · AI Security & Red Teaming · Vulnerability Research

0xdkay@gmail.com Homepage Scholar LinkedIn GitHub

Driving full-chain AI security, with a mission to build the next generation of Red Teams.

Professional Experience

- **Postdoctoral Fellow**, Georgia Tech — Atlanta, GA — Feb 2025 – Present
  - DARPA AIxCC Winner: Designed and implemented LLM-based autonomous fuzzing and exploit agents.
  - Currently leading the evaluation of AI's offensive potential in real-world cybersecurity scenarios.
- **Senior Engineer**, Samsung Security Center, Samsung SDS — Seoul, South Korea — Aug 2022 – Dec 2024
  - Drove Red Team operations across AI systems, IoT devices, Android apps, and kernel-level mitigations.
    - Secured 1B+ users through static/dynamic security reviews across 30+ consumer/enterprise products.
    - Secured prompt injection chains against remote code execution, impersonation, and sensitive data leak.
    - Trained 500+ security engineers and presented at 6 industry/academic venues on emerging AI threats.
    - Briefed executive leadership on key security risks and findings through detailed technical reports.
- **Graduate & Postdoctoral Researcher**, KAIST — Daejeon, South Korea — Mar 2014 – Jul 2022
  - Led 8-member research subgroup and conducted security research on emerging systems:
    - Smartphones & Android: Baseband auth bypass, AOSP privilege escalation, VoLTE exploitation.
    - IoT & Embedded Devices: Variant analysis on 1,100+ firmware, finding 20+ 0-days.
    - Cellular Networks: LTE protocol attacks, policy bypass, free data tunneling.
    - Drones & Wearables: Acoustic/EMI attacks, sensor spoofing, wireless analysis.
  - Delivered 27 publications (9 top-tier venues, 1,100+ citations), 10 patents, and 17 funded projects.
  - Discovered 100+ bugs in commercial systems, including Android and smartphone baseband 0-days.
- **Research Intern**, Pinion Industries — Seoul, South Korea — Dec 2013 – Feb 2014
  - Analyzed automotive CAN messages and exploited in-vehicle components, achieving RCE and wiretapping.
- **Student CERT Lead**, KAIST — Daejeon, South Korea — Sep 2010 – Aug 2012
  - Led student team in campus-wide security audit, including probing a critical email attack leading to arrest.

Education

- **Ph.D., School of Electrical Engineering**, KAIST — Daejeon, South Korea — Mar 2016 – Feb 2022
  - Advisor: Yongdae Kim
- **M.S., School of Electrical Engineering**, KAIST — Daejeon, South Korea — Mar 2014 – Feb 2016
  - Advisor: Yongdae Kim
- **B.S., Computer Science**, KAIST — Daejeon, South Korea — Mar 2010 – Feb 2014

Additional Qualifications

- **CTF Player:** 5× DEF CON finalist, led 20-person team, organized Samsung CTF, $115K+ total winnings.
- **Community Contributor:** Delivered 20+ invited talks across academia and industry on emerging threats.
- **AI Frameworks:** LangGraph, LangChain, LiteLLM, Phoenix (exploit agents); PyRIT (safety guardrails).
- **Programming Languages & Tools:** Python, C/C++, Java, JavaScript; IDA, Frida, Burp Suite, ZAP