Kyoungmin Roh

Cybersecurity Researcher & Engineer

Seongnam, Republic of Korea
imsie1@dankook.ac.kr
+82 10-2506-3409
GitHub | LinkedIn | Google Scholar | ORCID

PROFESSIONAL SUMMARY

Cybersecurity researcher with experience in trustworthy AI, confidential computing, embedded security, and CPS/robotics security. Developed concept-drift-resilient Android malware detection methods and TrustZone/CCA-based secure-system designs, producing a first-author SCIE Q1 journal article, a first-author ACM SAC paper, additional peer-reviewed publications, a Korean patent application, and multiple paper awards. Combines security research with implementation across ARM trusted execution environments, post-quantum cryptography, Android analysis, and embedded platforms.

Research Interests: Trustworthy AI for Security; Android Malware Detection; Concept Drift; Trusted Execution Environments; ARM TrustZone and CCA; Post-Quantum Cryptography; Embedded and Cyber-Physical Systems Security.

EDUCATION

Dankook University *Yongin, Republic of Korea*
Bachelors of Engineering in Industrial Security *Mar 2021 – Feb 2027*

- **GPA:** 3.20/4.50 (grade percentage: 87/100)
- **Honors:** Danwoo Academic Merit Scholarship - top 6% of the department (Spring 2026); Academic Research Scholarship (Fall 2025, Spring 2026); Specialized Project Scholarship (Fall 2022, Fall 2025); Admission Scholarship (Spring 2021)
- **Undergraduate thesis:** "Qrust: AI-Powered QR Phishing Detection and Secure QR Generation" [Link]
- **Selected coursework:** Artificial Intelligence and Information Security, Digital Forensics, Reverse Engineering

RESEARCH EXPERIENCE

Seoul National University | Security Optimization Research Lab *Seoul, Republic of Korea*
Research Intern | Supervisor: Prof. Yunheung Paek; Mentor: Martin Kayondo *Jun 2026 – Present*

Confidential Computing for Software-Defined Vehicles

- To isolate mixed-criticality SDV workloads from an untrusted hypervisor, designed a Zephyr-in-Realm shim architecture with Automotive Grade Linux as the IVI domain and Zephyr as a virtualized ECU under ARM CCA Realms, establishing the system architecture for prototype evaluation.
- Threat-modeled lying-hypervisor behavior, plaintext shared-memory communication, and temporal trust-consistency failures in virtualized automotive ECUs, translating the analysis into concrete security requirements for an in-progress manuscript.

Security of Robot Foundation Models and Vision-Language-Action Architectures

- To clarify poorly defined attack surfaces in embodied AI, reviewed RFM and VLA execution pipelines and mapped vulnerabilities across multimodal inputs, model reasoning, tool interfaces, and closed-loop control, creating a structured basis for follow-on experimental work.

Dankook University | Computer Security and Operating Systems Lab *Yongin, Republic of Korea*
Undergraduate Research Assistant | Supervisor: Prof. Seong-je Cho *Mar 2025 – Jul 2026*

Concept-Drift-Resilient and Trustworthy AI

- To preserve Android malware detection performance as behaviors changed over time, built temporally separated evaluation pipelines using API co-occurrence graphs, Louvain/Leiden communities, clustering, mixture models, and adaptive thresholds, enabling explicit measurement of future-year generalization.
- To make model decisions inspectable, built evidence mechanisms from social-network metrics and behavior clusters; the work yielded first-author SCIE Q1 and ACM SAC papers, a patent application, and Best Paper awards.

Applied Post-Quantum Cryptography in Embedded Systems

- To reduce the trusted computing base of ML-KEM on constrained TrustZone-A devices, designed and implemented a split-execution architecture that kept secret-dependent operations in the Secure World while offloading public computation to the Normal World.
- Evaluated trusted-code size, secure-monitor-call overhead, and end-to-end latency; the resulting work received a KCC 2026 Distinguished Paper Award and first place in Dankook University's Cyber Security Contest research-paper track.

Indiana University Bloomington | CPS Security Lab *Bloomington, IN, USA (Remote)*
Research Intern | Supervisor: Prof. Hyungsub Kim *Oct 2025 – Jan 2026*

- To make fragmented open-source CPS vulnerability evidence suitable for empirical study, collected and normalized reports from OSV, GitHub Issues, and security forums into a structured dataset.
- Classified evidence by affected component, failure mode, attack surface, and security impact, producing a reusable foundation for systematic analysis of real-world CPS software weaknesses.

LEADERSHIP EXPERIENCE

KATUSA - Korean Augmentation to the U.S. Army *Camp Carroll, Republic of Korea*
U.S. Eighth Army, 35th Air Defense Artillery Brigade, 2-1 ADA Battalion *Aug 2023 – Feb 2025*

- To support day-to-day readiness in a bilingual U.S.-ROK unit, served concurrently as an artillery supply soldier, environmental officer, and interpreter, coordinating logistics and communication across military systems and cultures.
- Demonstrated team performance under field and duty constraints as a member of the winning Best Warrior Squad, leading to the Best KATUSA Award, the Army Commendation Medal, and end-of-service recognition from U.S. and ROK Army organizations.

PUBLICATIONS

An asterisk (*) denotes co-first authorship.

International Journal Article

1. **Kyoungmin Roh**, Seungmin Lee, Seong-je Cho, Youngsup Hwang, and Dongjae Kim. "SCAN: Structural Clustering with Adaptive Thresholds for Intelligent and Robust Android Malware Detection under Concept Drift." *Computer Modeling in Engineering & Sciences (CMES)*, Apr 2026. **[SCIE Q1]** [Link]

International Conference Papers

1. **Kyoungmin Roh**, Seungmin Lee, Seong-je Cho, and Youngsup Hwang. "ALARM: Android Malware Detection with Leiden API Communities and Robust Mixture of Experts." *Proceedings of the 41st ACM/SIGAPP Symposium on Applied Computing (SAC 2026)*, Thessaloniki, Greece, Mar 2026. **[BK21 Outstanding Conference]** [Link]
2. Nahee Kwon, **Kyoungmin Roh**, Youngsup Hwang, Seong-je Cho, and Boojoong Kang. "C-STAR: Cost-Aware Adaptive Learning under Concept Drift for Android Malware Detection." *Proceedings of the 23rd International Conference on Security and Cryptography (SECRYPT 2026)*, Porto, Portugal, Jul 2026. [Link]

Domestic Journal Article

1. **Kyoungmin Roh** and Seong-je Cho. "Concept Drift-Resilient Android Malware Detection via API Co-occurrence Graphs and Louvain Communities." *KIISE Transactions on Computing Practices*, Jan 2026. Invited article. [Link]

Domestic Conference and Workshop Papers

1. **Kyoungmin Roh***, Nahee Kwon*, Suhyeon Park, and Seong-je Cho. "A Lightweight ML-KEM Architecture via Secret-Dependency-Based Partitioning for Embedded TrustZone-A Systems." *Korea Computer Congress (KCC 2026)*, Jeju, Republic of Korea, Jun 2026. **[Distinguished Paper Award]**. [Link]
2. Nahee Kwon, **Kyoungmin Roh**, Suhyeon Park, and Seong-je Cho. "SCA: A Security Descriptor-Guided Logit Calibration Module for Concept Drift Adaptation in Android Malware Detection." *Korea Computer Congress (KCC 2026)*, Jeju, Republic of Korea, Jun 2026. [Link]

3. **Kyoungmin Roh**, Suhyeon Park, and Seong-je Cho. "Drift-Aware Security Module Based on Louvain Communities for Retraining-Free Android Malware Detection." *Korea Software Congress (KSC 2025)*, Yeosu, Republic of Korea, Dec 2025. **Best Paper Award**. [Link]
4. **Kyoungmin Roh**, Seungmin Lee, Yudam Kim, Seokhyun Ahn, and Seong-je Cho. "Android Malware Detection Using Co-occurrence Graphs of APIs and Louvain Method for Community Detection." *Workshop on Dependable and Secure Computing (WDSC 2025)*, Jeju, Republic of Korea, Aug 2025. **Best Paper Award**. [Link]
5. Seungmin Lee, **Kyoungmin Roh**, Jiheon Jung, Suhyeon Park, and Seong-je Cho. "Classifying File Fragment Types for IVI System Forensics." *Workshop on Dependable and Secure Computing (WDSC 2025)*, Jeju, Republic of Korea, Aug 2025. [Link]

Additional Research Publication

1. **Kyoungmin Roh**, Nahee Kwon, Bogyeom Kim, and Subin Jeon. "A Lightweight Secret-Isolated Post-Quantum Cryptographic Architecture for ARM TrustZone." *Cyber Security Contest*, Department of Cybersecurity, Dankook University, Dec 2025. **First Place Award**. [Link]

PATENT

1. **Kyoungmin Roh**, Seungmin Lee, Seong-je Cho, and Yoonho Choi. "A Malware Detection Method Combining Clustering and Supervised Learning Models." Korean Patent Application No. 10-2025-0098855, 2025. Filed.

FUNDED RESEARCH PROJECTS

Future Policing Challenge Technology Development — *Dankook University*
Undergraduate Researcher — *Apr 2026 – Jul 2026*
Commissioned by: Korean National Police Agency and Ministry of Science and ICT

Project: Development of a Reconfigurable Vehicle Living Lab and Digital Forensic Tools for Advanced Mobility

- To support a reconfigurable vehicle-forensics testbed, implemented front-end components, reviewed relevant systems literature, and contributed technical material to the project proposal, delivering an initial interface and documented design inputs for the research team.

Intelligent Autonomous Building Energy and Environmental Management System — *Dankook University*
Undergraduate Researcher — *Oct 2025 – Jul 2026*
Commissioned by: Korea Energy Technology Evaluation and Planning

- To connect mobile-platform AI security research with a funded intelligent-building program, conducted experiments and contributed to peer-reviewed manuscript preparation, producing research outputs within the laboratory's concept-drift workstream.

Effective and Intelligent Framework for Mobile Platform-Based Vehicle Forensics — *Dankook University*
Undergraduate Researcher — *Oct 2025 – Jul 2026*
Commissioned by: National Research Foundation of Korea and Ministry of Science and ICT

- To advance data-driven vehicle-forensics research, contributed literature analysis, experimental work, and peer-reviewed writing on mobile-platform AI security, supporting the laboratory's publication pipeline.

AWARDS

Research, Paper, and Project Awards

KCC 2026 Distinguished Paper Award | *Korean Institute of Information Scientists and Engineers* — *Jun 2026*
Honored the paper on ML-KEM partitioning for embedded TrustZone-A

Cyber Security Contest, First Place | *Dankook University, Department of Cybersecurity* — *Dec 2025*
Won the research-paper track for split ML-KEM on TrustZone-A

KSC 2025 Best Paper Award | *Korean Institute of Information Scientists and Engineers* — *Dec 2025*
Honored retraining-free Android malware detection with Louvain communities

Capstone Festival Audience Choice Award | *Dankook University, National Center of Excellence in Software* *Dec 2025*
Audience-selected award for the Qrust secure-QR phishing detector

Dankook Startup Hackathon, 3rd Place | *Dankook University, National Center of Excellence in Software* *Sep 2025*
Third place for the accessibility-focused DDobak speech-therapy prototype

WDSC 2025 Best Paper Award | *Korean Institute of Information Scientists and Engineers* *Aug 2025*
Honored Android malware detection using API co-occurrence communities

Cipher Application Competition, 1st Place | *Dankook University, Department of Cybersecurity* *Sep 2023*
First place for a Lamport OTS and Merkle-tree signature prototype

Military and Leadership Honors

Certificate of Appreciation | *United States Army Garrison Daegu* *Feb 2025*
Recognized contributions to U.S. Army operations in Korea

Republic of Korea Army Soldier Award | *Republic of Korea Army* *Feb 2025*
Recognized exemplary service during the KATUSA assignment

Army Commendation Medal (ARCOM) | *United States Department of the Army* *Dec 2024*
Awarded for meritorious service with the 35th Air Defense Artillery Brigade

Best KATUSA Award | *Eighth U.S. Army ROK Army Support Group* *Oct 2024*
Recognized outstanding duty performance as a KATUSA

SCHOLARSHIPS

Danwoo Academic Merit Scholarship | *Dankook University* *Aug 2026*
Awarded for academic performance ranking in the top 6% of the department

Academic Research Scholarship | *Dankook University, National Center of Excellence in Software* *Aug 2026*
Recognized sustained undergraduate research and scholarly output

Specialized Project Scholarship | *Dankook University, Department of Cybersecurity* *Dec 2025*
Recognized high performance in a department-designated security project

Academic Research Scholarship | *Dankook University, National Center of Excellence in Software* *Dec 2025*
Recognized undergraduate research performance and publication activity

Special Academic Merit Scholarship | *Dankook University, Department of Industrial Security* *Dec 2022*
Awarded for strong academic performance in the major

Specialized Project Scholarship | *Dankook University, Department of Industrial Security* *Dec 2022*
Recognized high performance in a department-designated project

Admission Scholarship | *Dankook University, National Program of Excellence in Software* *Mar 2021*
Entrance scholarship awarded through the university's software-excellence program

ADDITIONAL COURSEWORK AND TRAINING

Chinese Native-Speaker Tutoring Program *Dankook University OIA*
Participant *Sep 2025 – Dec 2025*

- To improve practical cross-cultural communication, completed weekly one-on-one sessions with a native Chinese instructor, strengthening speaking and listening through sustained conversational practice.

LG Aimers AI Bootcamp *LG AI Research*
Participant *Jun 2023 – Jul 2023*

- To solve a smart-factory classification task after intensive coursework in machine learning, deep learning, linear algebra, and statistics, led model training, evaluation design, and the final team presentation, completing the applied AI project.

EXTRACURRICULAR ACTIVITIES

AEGIS Cybersecurity Club, Dankook University | Website *Yongin, Republic of Korea*
Member *Jul 2025 – Present*

- To strengthen practical security skills alongside academic research, participate in weekly CTF exercises and technical seminars spanning cryptography, reversing, and systems security, maintaining regular hands-on practice across core security domains.
- Led the club's hacking team to top 10% in the CCE 2025 (Cyber Conflict Exercise) preliminary round, top 10% at HacktheOn Sejong 2025.

OSINT Team | Website *Remote*
Contributing Writer *Mar 2025 – Present*

- To make security concepts accessible to a broader audience, author cybersecurity-awareness and technical articles for a global OSINT education platform, translating technical topics into practical guidance for non-specialist readers.

RubiyaLab CTF Team | Website *Seoul, Republic of Korea*
Member *Jul 2025 – Nov 2025*

- To practice adversarial problem solving under time constraints, contributed to cryptography and reverse-engineering challenges with a top-ranked Korean CTF team, applying security knowledge in international competitions.

Kendo Club, Dankook University | Website *Yongin, Republic of Korea*
Member *Mar 2022 – Dec 2022*

- Mentored international junior members on fundamental kendo techniques and etiquette, successfully helping them integrate into the club.

Turing Crypto Club, Department of Cybersecurity, Dankook University | Website *Yongin, Republic of Korea*
Member *May 2022 – Dec 2022*

- To build an applied cryptography foundation, studied core constructions with peers and delivered seminar presentations, which informed the later post-quantum signature prototype.

VOLUNTEER EXPERIENCE

Rural Volunteer Service *Buyeo County, Republic of Korea*
Volunteer - 21 hours *Sep 2025*

- To support seasonal agricultural work, assisted with greenhouse maintenance and chestnut harvesting through a national rural-volunteering initiative, completing 21 service hours.

PROFESSIONAL AFFILIATIONS

- Korean Institute of Information Scientists and Engineers (KIISE) *Member*
- Korean Defense Veterans Association (KDVA) *Member*

CERTIFICATE

Language Certificates

- **TOEFL:** Reading 5.5; Listening 5.0; Writing 5.5; Speaking 4.0; Overall 5.0 (CEFR C1) [2026.9.16]

LANGUAGES

- **Korean:** Native.
- **English:** Professional Proficiency.
- **Japanese:** Conversational Proficiency.
- **Chinese:** Basic.
- **Arabic:** Basic.

REFERENCES

Available upon request.