TAEKKYUNG OH (TK)

+82 10 9133 2496 | ohtk@kaist.ac.kr

https://ohtaekkk.github.io

EDUCATION

KAIST **DAEJEON, SOUTH KOREA**

DOCTOR OF PHILOSOPHY, GRADUATE SCHOOL OF INFORMATION SECURITY AUG 2026

- **Thesis: Cellular Dual-Use Technologies Exploiting Specification Vulnerabilities: Physical Localization and Fake Base Stations**
- **Supervisor: Prof. Yongdae Kim**

KAIST **DAEJEON, SOUTH KOREA**

MASTER OF SCIENCE, GRADUATE SCHOOL OF INFORMATION SECURITY AUG 2021

- **Thesis: 3D Physical Localization of Voice Phishing SIMBOX on Cellular Networks**
- **Supervisor: Prof. Yongdae Kim**

SUNGKYUNKWAN UNIVERSITY **SUWON, SOUTH KOREA**

BACHELOR OF SCIENCE, ELECTRONIC AND ELECTRICAL ENGINEERING AUG 2019

BACHELOR OF SCIENCE, COMPUTER SCIENCE AND ENGINEERING (DOUBLE MAJOR) AUG 2019

WORK EXPERIENCE

POSTDOCTORAL RESEARCHER AT KAIST **SOUTH KOREA**

SEP 2026 ~ PRESENT

- Conduct research on cellular and wireless security, focusing on fake base station (FBS) attacks and detection, non-terrestrial network (NTN) security, and physical localization of cellular devices.
- Investigate AI-assisted security analysis of cellular specifications, AI-based threat modeling and detection in NTNs, and reinforcement learning-based waveform shaping for secure downlink channels in AI-RAN.
- Collaborate with industry and government partners on cellular security research, including SK Telecom, LIG D&A (defense company), ETRI, the National Security Research Institute, and the Korean National Police Agency.

VISITING RESEARCHER AT UNIVERSITY OF FLORIDA **USA**

OCT 2025 ~ APR 2026

- Conducted research on fake base station modeling to characterize diverse and realistic threats in cellular networks.
- Developed an FBS detection system based on *LTESniffer* and conducted real-world measurements.
- Collaborated with Prof. Patrick Traynor at the Florida Institute for Cybersecurity Research.
- Supported by the Global Advanced Cybersecurity Human Resources Development program, South Korea, as principal investigator of the visiting research project.

UNDERGRADUATE RESEARCHER AT SUNGKYUNKWAN UNIVERSITY **SOUTH KOREA**

DEC 2016 ~ DEC 2018

- Conducted research on voice authentication and usable security, including spectral analysis for detecting voice replay attacks, audio CAPTCHA, and ultrasonic voice-command jamming.
- Supervised by Prof. Hyoungshick Kim.

RESEARCH EXPERIENCE

TOPIC OF RESEARCH*: PRACTICAL SYSTEM DESIGN AND PROTOCOL ANALYSIS FOR *CELLULAR SECURITY

I. Designed, implemented, and evaluated practical systems for cellular security, combining protocol analysis, radio signal processing, and real-world experiments.
   - Designed a reference fake base station model, *Devilray*, incorporating diverse, realistic, and evasive attacker behaviors across protocol and physical layers to support diagnosing, improving, and benchmarking FBS detectors [C1].

- Developed a practical system for end-to-end physical localization of uncooperative cellular devices by exploiting cellular protocols and applying radio direction finding [C4].
- Developed *LTESniffer*, an open-source tool for LTE downlink and uplink eavesdropping [C5].

II. Conducted security analysis of cellular standards and protocol implementations.
- Analyzed vulnerabilities in location-based access restriction mechanisms in NTN specifications and demonstrated subsequent relay-based denial-of-service (DoS) attacks against commercial devices [C2].
- Developed a specification-guided over-the-air fuzzing framework, *LLFuzz*, for identifying vulnerabilities in commercial baseband implementations of PHY, MAC, RLC, and PDCP (lower layers) [C3].

III. Responsibly disclosed practical security findings to secure cellular networks.

Relevant skills: software-defined radio (SDR); open-source and commercial cellular platforms (srsRAN, OCUDU, OpenAirInterface, Open5GS, LTESniffer, Kamailio, and AMARI Callbox); and commercial device diagnostics and control using DM tools, SCAT, ADB, and AT commands.

KEY OUTCOMES OF RESEARCH

I. Practical systems for cellular security
- *Devilray* [C1]: Identified blind spots (unexplored attack behaviors leading to detection failures) in existing FBS detection systems using *Devilray*, which supports 2,592 FBS instantiations. The model is currently used by the Electronic Frontier Foundation (EFF) to improve their FBS detector. It is also being used to conduct carrier testbed experiments in collaboration with SK Telecom (a major Korean carrier) for network-side detection. The research was presented at the GSMA Fraud and Security Group (FASG) meeting for future FBS detection.
- *End-to-end physical localization* [C4]: Adopted for voice phishing (vishing) investigations in collaboration with the Korean National Police Agency to support the tracking and seizure of devices used in crimes.
- *LTESniffer* [C5]: Released as an open-source platform, with 2.3k GitHub stars and 240 forks as of Nov. 2026.

II. Security findings in cellular standards and implementations
- *NTN vulnerability* [C2]: Demonstrated prolonged DoS on three commercial NTN devices, including its impact on subsequent terrestrial network access. The vulnerability was acknowledged under GSMA's coordinated vulnerability disclosure (CVD) program.
- *LLFuzz* [C3]: Identified nine previously unknown memory corruption vulnerabilities across PDCP, RLC, and MAC implementations through the evaluation of 15 commercial basebands from five vendors (Qualcomm, MediaTek, Samsung, Google, and Huawei).

III. Contributions to secure cellular networks (responsible disclosures)
- Acknowledged by major baseband vendors and GSMA for security findings – five CVEs and three GSMA CVDs.
- Disclosures led to security patches for affected commercial products.

EXPECTED FUTURE RESEARCH DIRECTIONS

- Extending experience in system design, protocol analysis, and physical-layer signal processing to AI-based cellular security research.
  - AI-assisted standards analysis to identify security gaps across 3GPP and regional cellular specifications.
  - RL-based waveform shaping for secure downlink channels in AI-RAN to hinder passive SDR eavesdropping while maintaining service to legitimate devices.
  - ML-based fake satellite base station detection in non-terrestrial networks, leveraging orbit information and RF characteristics such as Doppler shifts.

PROJECT EXPERIENCE

ONGOING PROJECTS

SECURITY ASSESSMENT AND THREAT EVALUATION OF SK TELECOM'S NETWORK AGAINST SUBSCRIBER INFORMATION-BASED ATTACKS

Research Participant JUN 2026 ~ PRESENT

- **Funding:** SK Telecom (SKT), South Korea.

- Characterize communication and privacy threats posed by fake base stations through experiments in SK Telecom's commercial testbed.
- Develop a network-side FBS detection system to address communication and privacy threats.

DEVELOPMENT OF SECURITY THREAT RESPONSE AND PRIVACY PROTECTION TECHNOLOGIES AND INTERNATIONAL COOPERATION FOR ESTABLISHING A TRUSTED GLOBAL ECOSYSTEM IN 6G NTN

Research Participant JUL 2025 ~ PRESENT

- **Funding:** Ministry of Science and ICT (MSIT), South Korea.
- Conduct research on security threats and privacy protection technologies for next-generation non-terrestrial networks.
- Identified service disruption and privacy threats exploiting location-based access restriction mechanisms in 3GPP NTN specifications [C2].
    - Led the research and served as a co-corresponding author of the resulting paper published at ACM WiSec '26.

DEVELOPMENT OF PRIVATE 5G SECURITY TECHNOLOGY FOR INTEGRATED PRIVATE 5G AND ENTERPRISE NETWORK SECURITY

Research Participant APR 2024 ~ PRESENT

- **Funding:** Ministry of Science and ICT (MSIT), South Korea.
- Conduct research on fake base station threats and mitigation techniques in private 5G networks.
- Collaborate with Hyundai Motor Company to analyze vulnerabilities in private 5G networks deployed in manufacturing facilities.

COMPLETED PROJECTS

DEVELOPMENT OF A FAKE BASE STATION DETECTION SYSTEM IN CELLULAR NETWORKS

Principal Investigator OCT 2025 ~ APR 2026

- **Funding:** Global Advanced Cybersecurity Human Resources Development program, Ministry of Science and ICT (MSIT), South Korea.
- Conducted visiting research on fake base station modeling and detection with Prof. Patrick Traynor at the University of Florida.
- Developed *Devilray* [C1] and an *LTESniffer*-based FBS detection system, and conducted a real-world measurement study.

DEVELOPING A TECHNOLOGY FOR BYPASSING FAKE BASE STATION DETECTION METHODS

Project Manager MAR 2025 ~ DEC 2025

- **Funding:** National Intelligence Service (NIS), South Korea.
- Managed and conducted research on realistic and evasive fake base station behavior for future FBS detection.

DEVELOPING A TECHNOLOGY FOR DETECTING AN OPEN-SOURCE-BASED FAKE BASE STATION

Project Manager FEB 2024 ~ DEC 2024

- **Funding:** National Intelligence Service (NIS), South Korea.
- Managed and conducted research on detecting fake base stations implemented using open-source cellular stacks.

TRACKING AND IDENTIFYING DEVICES AND CALL TRAFFIC IN THE VOICE PHISHING ECOSYSTEM

Project Manager APR 2022 ~ DEC 2024

- **Funding:** Korean National Police Agency, South Korea.
- Managed and conducted research on developing a defense-in-depth system to prevent vishing across wired and cellular networks.
- Developed an end-to-end physical localization system for uncooperative cellular devices and supported its use in police investigations [C4].

Invited Talks

LASER Workshop 2026 (Scheduled) **Los Angeles, CA, USA**
Learning from Authoritative Security Experiment Results; ACSAC 2026. Dec 2026

- (Tentative) Discussion on the implementation and evaluation of a reference fake base station model, *Devilray*.

srsRAN Project Fall Workshop 2023 **Arlington, VA, USA**
Software Radio Systems (SRS). Oct 2023

- Testing, analyzing, improving security of cellular networks with srsRAN (with Prof. Yongdae Kim).

Security Intelligence Summit (SIS) 2022 .ON **Seoul, South Korea**
S2W Inc. (cybersecurity company). Nov 2022

- Voice phisher intelligence: Location tracking and infrastructure vulnerability analysis.

Security Reports & Acknowledgements

Commercial Baseband Vulnerabilities

- **CVE-2025-20708** – MediaTek: Incorrect handling of undersized PDCP PDUs causing baseband crashes (out-of-bounds write).
- **CVE-2024-48883** – Samsung & Google: Information leak caused by malformed uplink scheduling messages.
- **CVE-2024-23385** – Qualcomm: Incorrect handling of RAR messages containing only sub-headers without any payloads, causing modem resets and denial of service.
- **CVE-2024-20077** – MediaTek: Incorrect handling of MAC PDUs with multiple MAC CE sub-headers, causing baseband crashes and denial of service.
- **CVE-2024-20076** – MediaTek: Incorrect handling of a zero-valued length field in MAC sub-headers, causing baseband crashes and denial of service.

Cellular Specification Vulnerabilities

- **GSMA CVD-2026-0115** – Vulnerability in location-based access restriction mechanisms in non-terrestrial networks (NTN).
- **GSMA CVD-2023-0077** – Vulnerability in uplink scheduling mechanisms in LTE networks.
- **GSMA CVD-2023-0070** – Vulnerability in radio control mechanisms in LTE networks.

Core Competencies

Software-Defined Radio and Cellular Platforms

- SDR-based radio system implementation and experimentation.
- Experience with srsRAN, OCUDU, OpenAirInterface, Open5GS, AMARI Callbox, Kamailio, and LTESniffer.

Radio Signal Processing and Measurement

- LTE/5G downlink and uplink control- and data-channel decoding.
- Radio signal acquisition and analysis, RF characterization, and wireless localization.

Cellular Protocols and Standards

- Analysis of 3GPP specifications and protocol behavior across PHY, MAC, RLC, PDCP, RRC, and NAS.
- Analysis of downlink/uplink control, logical channel configuration, and protocol state transitions.

Device Diagnostics and Protocol Testing

- Commercial device diagnostics and control using DM tools, SCAT, ADB, and AT commands.
- Protocol log analysis using Wireshark, specification-guided over-the-air testing, and baseband crash monitoring.

SOFTWARE SKILLS AND TECHNICAL WRITING

- C, C++, Python, PyTorch, and TensorFlow.
- Implementation, modification, and debugging of cellular protocol stacks and experimental software.
- LLM-based coding agents; prompt engineering and iterative refinement for code generation, debugging, experiment automation, and cellular standards analysis.
- LaTeX; preparation of research manuscripts, technical reports, and vulnerability disclosure reports.

PUBLICATIONS

CONFERENCES

[C1] **Taekkyung Oh***, Duckwoo Kim*, Hansung Bae, Beomseok Oh, CheolJun Park, Tyler Tucker, Nathaniel Bennett, Sangwook Bae, Byeongdo Hong, Patrick Traynor, and Yongdae Kim, **"Devilray: A Reconfigurable Adversarial Baseline for Revealing Blind Spots in Fake Base Station Detection,"** *Annual Computer Security Applications Conference (ACSAC)*, 2026. Accepted; to appear. *Co-first authors.

[C2] Kwangmin Kim, **Taekkyung Oh**†, and Yongdae Kim†, **"Denied by Border: Denial-of-Service Attack Exploiting Location Restrictions in Non-Terrestrial Networks,"** *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2026. †Co-corresponding authors.

[C3] Tuan Dinh Hoang, **Taekkyung Oh**, CheolJun Park, Insu Yun, and Yongdae Kim, **"LLFuzz: An Over-the-Air Dynamic Testing Framework for Cellular Baseband Lower Layers,"** *USENIX Security Symposium*, 2025.

[C4] **Taekkyung Oh**, Sangwook Bae, Junho Ahn, Yonghwa Lee, Tuan Dinh Hoang, Min Suk Kang, Nils Ole Tippenhauer, and Yongdae Kim, **"Enabling Physical Localization of Uncooperative Cellular Devices,"** *Annual International Conference on Mobile Computing and Networking (ACM MobiCom)*, 2024.

[C5] Tuan Dinh Hoang, CheolJun Park, Mincheol Son, **Taekkyung Oh**, Sangwook Bae, Junho Ahn, Beomseok Oh, and Yongdae Kim, "**LTESniffer: An Open-source LTE Downlink/Uplink Eavesdropper,"** *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2023.

[C6] Muhammad Ejaz Ahmed, Il-Youp Kwak, Jun Ho Huh, Iljoo Kim, **Taekkyung Oh**, and Hyoungshick Kim, **"Void: A Fast and Light Voice Liveness Detection System,"** *USENIX Security Symposium*, 2020.

[C7] **Taekkyung Oh**, William Aiken, and Hyoungshick Kim, **"Hey Siri – Are You There?: Jamming of Voice Commands Using the Resonance Effect (Work-in-Progress),"** *IEEE International Conference on Software Security and Assurance (ICSSA)*, 2018.

JOURNALS

[J1] Yooho Jang, Juhong Park, **Taekkyung Oh**, Yongdae Kim, and Seong Ook Park, **"Passive Three-Dimensional User Equipment Tracking Using Long-Term Evolution Uplink Signals,"** *IEEE Transactions on Instrumentation and Measurement (TIM)*, 2025.

POSTERS

[P1] Jusop Choi, **Taekkyung Oh**, William Aiken, Simon S. Woo, and Hyoungshick Kim, **"Poster: I Can't Hear This Because I Am Human: A Novel Design of Audio CAPTCHA System,"** *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2018.