<Professor Yongdae Kim's Lab.>

System Security Lab (SysSec)

Professor: Yongdae Kim

■ **Contact information**

Professor : **yongdaek@kaist.ac.kr** TEL : **042-350-7430**

Website : **syssec.kr, syssec.kr/~yongdaek**

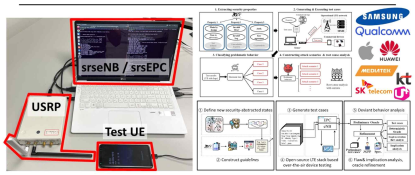
■ **Current state of the Lab. (2025 Spring)**

Postdoctoral Fellows : 1 PhD Students: 11 Master's Student: 2 Visiting Student & Undergraduates: 4

■ **Research Areas**

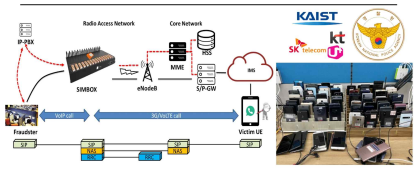
Research Area: Cellular Network

Fuzzing on Cellular Network and Devices



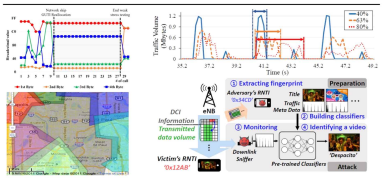
Finding security flaws at smartphone and cellular network

Preventing and Tracking Voice Phishing Crimes



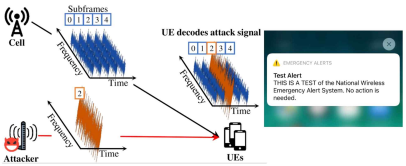
Device (SIMBOX) detection and location tracking

Tracking User's Locations and Applications



Location tracking & Video fingerprinting attack

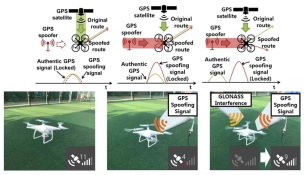
Physical Layer Injection Attack



Inject fake LTE messages (e.g. fake emergency alert)

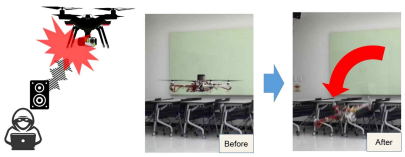
Research Area: Drones and Self-driving Cars

Hijacking Drones using GPS Spoofing Attack



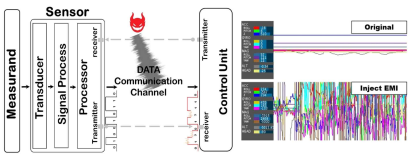
Hijacking the drones using a fake GPS signal

Dropping Drones using Sound Attack



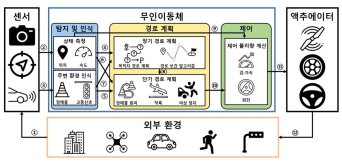
Dropping the drones using acoustic resonance

Dropping Drones using EM Attack



Crashing drones via EM attack on communication channel

Self-driving Safety Testing



Finding misbehaviors in a self-driving car

■ Recommended courses & Career after graduation

- **Academia**(faculty positions): Univ. of Central Florida, Liberty University, Sungshin Univ., Sungkyunkwan Univ., KyungHee Univ., Military Academy, etc.
- **Big companies**: Microsoft, Intel, U.S. Bank, VMWare, Qualcomm, Samsung, Hyundai Motors, NAVER, Theori, etc.
- **Research institutes**: NSR, ADD, ETRI, KEPCO, KATECH, etc.

■ Introduction to other activities besides research

- Engaging in practical research in **collaboration with leading corporations** (internship)
- Exploring diverse career paths through an active community and annual homecoming events with **alumni working in various fields**
- **Bug bounties, CTFs (extra $$$)**

■ Introduction to the Lab

Our lab conducts cutting-edge research to uncover security vulnerabilities in cellular network, self-driving cars and various other emerging systems. We are seeking passionate students to join us in discovering new vulnerabilities and advancing the field of cybersecurity!

■ Recent research achievements ('23~'25)

- Too Much of a Good Thing: (In-)Security of Mandatory Security Software for Financial Services in South Korea (USENIX Security '25)
- LLFUZZ: An Over-the-Air Dynamic Testing Framework (USENIX Security '25)
- Revisiting GPS Spoofing in Phasor Measurement: Real-World Exploitation and Practical Detection in Power Grids (TOPS '25)
- FirmState: Bringing Cellular Protocol States to Shannon Baseband Emulation (WiSec '25)
- Enhancing synchrophasor Reliability Through Network-Based Time Synchronization: KEPCO's Practical Approach (IEEE Symposium on Security and Privacy '24)
- Enabling Physical Localization of Uncooperative Cellular Devices (ACM MobiCom '24)
- A Systematic Study of Physical Sensor Attack Hardness (S&P '24)
- Delegation of TLS Authentication to CDNs using Revocable Delegated Credentials (ACSAC '23)
- BASECOMP: A Comparative Analysis for Integrity Protection in Cellular Baseband Software (NDSS '23)
- LTESniffer: An Open-source LTE Downlink/Uplink Eavesdropper (WiSec '23)
- Un-Rocking Drones: Foundations of Acoustic Injection Attacks and Recovery Thereof (NDSS '23)
- Preventing SIM Box Fraud Using Device Fingerprinting (NDSS '23)
- Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels (NDSS '23)
- Lightbox: Sensor Attack Detection for Photoelectric Sensors via Spectrum Fingerprinting (TOPS '23)