

Yeongbin Hwang

Master's Student

School of Electrical Engineering

Korea Advanced Institute of Science and Technology (KAIST)

Email: hyb3565800@gmail.com

Homepage: <https://yeongbin.dev/>

SUMMARY

I am a Master's Student in System Security Lab at KAIST advised by Professor Yongdae Kim. My research interest is to find, analyze, and exploit software and hardware vulnerabilities in cellular networks. Especially, I'm putting my effort into analyzing 5G core network security and network structure.

EDUCATION

Korea Advanced Institute of Science and Technology (KAIST), South Korea

M.S. in School of Electrical Engineering

Mar. 2021 – Feb. 2023

Thesis Title: Dissecting VoLTE: Exploiting Free Data Channels and Security Problems

Advisor: Prof. Yongdae Kim

B.S. in School of Computing

Feb. 2016 – Feb. 2021

PROJECT

5G core network testing: let's induce the collision

2021 – 2022

Implemented a framework based on open5gcore to test the vulnerabilities of the 5G core network. The framework consists of three main components: 1) a Fuzzer that continues testing on UE pod, 2) a Controller that captures packets on the host and relays them to the target, and 3) an Analyzer that analyzes the results of the test.

Systematization of Knowledge in Cellular Network

2021 – 2022

Investigated vulnerabilities existing in cellular networks using symmetric keys, and analyzed whether it was possible to solve the vulnerabilities that exist when PKI was implemented.

Comparison between state machines

2020 – 2021

Implemented a testing framework for building state machines of networks: conduct the study - showing that state machines of networks are different to cause some implementation flaws by fuzzing test.

MitM simulator: Modifying packets between user and network

2019 – 2020

Designed and implemented MitM(Man in the Middle) environment in LTE network to verify vulnerabilities found through formal verification. This MitM simulator executes the attack scenario and determines whether the network or user is functioning normally for it. This allows us to validate attacks on vulnerabilities found using formal analysis.

SKILL

Programming Language

C, C++, Python, Javascript (Node.js)

Framework and Tool

Open source LTE, 5G software using SDR(srsRAN, open5GS), Wireshark, Kubernetes, Docker

WORK EXPERIENCE

- System Security Laboratory (KAIST)**, Research Intern Jan. 2020 – Dec. 2020
Implements MitM(Man in the Middle) simulator in LTE
Professor: Yongdae Kim.
- Network and System Security Laboratory (KAIST)**, Research Intern Sep. 2019 – Dec. 2019
Dark Web security search
Professor: Seungwon Shin.
- Computer Architecture and Memory Systems Laboratory (KAIST)**, Research Intern Jun. 2019 – Aug. 2019
Kernel programming for improving the speed to access the memory
Professor: Myoungsoo Jung.

PATENTS

Applications

- US20220124504A1 Apr. 2022
Method for validating man-in-the-middle attack for cellular control plane protocols and the system thereof
- KR20220050767A Apr. 2022
Method for validating man-in-the-middle attack for cellular control plane protocols and the system thereof

PUBLICATIONS (DOMESTIC, SOUTH KOREA)

- 1. Preventing Voice Phishing Using CMC Call Analysis and Detection**
Junho Ahn, Sangwook Bae, Beomseok Oh, Yonghwa Lee, Jiho Lee, Yeongbin Hwang, Takkyung Oh, Mincheol Son and Yongdae Kim
Conference on Information Security and Cryptography Summer (CISC-S'22)
May 2022
- 2. Revealing the limitations of operating LTE downlink sniffers in real-world**
Tuan Hoang Dinh, Sangwook Bae, Cheoljun Park, Jiho Lee, Taekkyung Oh, Mincheol Son, Yeongbin Hwang and Yongdae Kim
Conference on Information Security and Cryptography Winter (CISC-W'21)
Dec. 2021
- 3. VoLTEFuzz: Framework for Comprehensive Analysis of SIP in VoLTE**
Seokbin Yun, Sangwook Bae, Mincheol Son, Jiho Lee, Cheoljun Park, Yeongbin Hwang, Yongdae Kim and Dongkwan Kim
Conference on Information Security and Cryptography Winter (CISC-W'20)
Dec. 2020
- 4. Coercive FBS Redirection Attack using Unicast Message Injection in LTE**
Cheoljun Park, Sangwook Bae, Mincheol Son, Jiho Lee, Hongil Kim, Seokbin Yun, Yeongbin Hwang and Yongdae Kim
Conference on Information Security and Cryptography Summer (CISC-S'20)
May. 2020

PROFESSIONAL ACTIVITIES

Secondary Reviewer (Security)

USENIX Security Symposium (Security)	2022
IEEE Symposium on Security and Privacy (Oakland)	2022
ACM Conference on Computer and Communications Security (CCS)	2021 – 2022

TEACHING EXPERIENCE

Teaching Assistant, Programming Structure for Electrical Engineering (EE209)	Fall 2022
Teaching Assistant, Software Security (EE595)	Spring 2022
Teaching Assistant, Software development environment and tools practice (EE485)	Fall 2021
Teaching Assistant, Introduction to Programming (CS101)	Fall 2020

LIST OF REFERENCES

Dr. Yongdae Kim

Chair Professor, KAIST
Professor, School of Electrical Engineering and Graduate School of Information Security, KAIST
Homepage: <https://syssec.kaist.ac.kr/~yongdaek/>

Dr. Seungwon Shin

Chair Professor, KAIST
Professor, School of Electrical Engineering, KAIST
Homepage: <https://nss.kaist.ac.kr/>

Dr. Myoungsoo Jung

Chair Professor, KAIST
Professor, School of Electrical Engineering, KAIST
Homepage: <http://camelab.org/>