CheolJun Park

Postdoctoral researcher
School of Electrical Engineering, KAIST
Email: cheoljunp@kaist.ac.kr

Summary

I am a security researcher. My research interests focus on cellular network security, including (1) dynamic analysis to find implementation flaws, (2) attacks on the cellular physical layer and (3) designing secure specifications. All my works are empirically verified with open-source mobile network stacks and software-defined radios. Recently, I successfully defended my Ph.D. dissertation at the School of Electrical Engineering, KAIST.

Education

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

Ph.D. in School of Electrical Engineering — Mar. 2019 – Feb. 2024
- Topic: Cellular network, security, protocol negative testing, cellular security design
- Dissertation Title: A study on dynamic method for finding implementation vulnerabilities in cellular baseband
- Advisor: Prof. Yongdae Kim

M.S. in School of Electrical Engineering — Mar. 2017 – Feb. 2019
- Thesis Title: Lock-in-amplification-based low-power high-resolution EM sensor interface for 3D localization
- Advisor: Prof. Minkyu Je

B.S. in School of Electrical Engineering — Mar. 2013 – Feb. 2017
- Topic: Security analysis of segway ninebot mini pro
- Advisor: Prof. Yongdae Kim

High School Diploma in Korea Science Academy — Feb. 2010 – Feb. 2013

CISPA Helmholtz Center for Information Security, Saarbrücken, Germany

Visiting Researcher — May. 2022 – Aug. 2022
- Topic: Cellular network, security, grammar-guided protocol testing, memory bug
- Advisor: Prof. Thorsten Holz

Qualcomm Incorporated, San Diego, USA

Interim Engineering Intern — May. 2023 – Aug. 2023
- Team: Over-the-air team, QPSI (Qualcomm product security initiative)
- Topic: Dynamic security testing on the cellular modem
- Manager: Dr. Patrick Stewin

Publications

International Conferences (∗: co-first authors)

1. **BASECOMP: A Comparative Analysis for Integrity Protection in Cellular Baseband Software** [paper]
   Eunsoo Kim*, Min Woo Baek*, **CheolJun Park**, Dongkwan Kim, Yongdae Kim, and Insu Yun
   USENIX Conference on Security Symposium (USENIX Security'23) Aug. 2023
   CVE-2022-23425
2. **LTESniffer: An Open-source LTE Downlink/Uplink Eavesdropper** [paper]
   Tuan Dinh Hoang, **CheolJun Park**, Mincheol Son, Taekkyung Oh, Sangwook Bae, Junho Ahn, BeomSeok

Oh, and Yongdae Kim

ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'23) May. 2023

3. **DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices** [paper] [video]
   CheolJun Park*, Sangwook Bae*, BeomSeok Oh, Jiho Lee, Eunkyu Lee, Insu Yun, and Yongdae Kim
   USENIX Conference on Security Symposium (USENIX Security'22) Aug. 2022
   CVE-2019-2289, CVE-2021-30826, SVE-2021-20291 (CVE-2021-25516)
   - Built negative testing framework based on srsLTE, and discovered 26 implementation flaws (including 22 previously unknown ones) from 43 devices from 5 different baseband manufacturers.
4. **Watching the Watchers: Practical Video Identification Attack in LTE Networks** [paper]
   Sangwook Bae, Mincheol Son, Dongkwan Kim, **CheolJun Park**, Jiho Lee, Sooel Son, and Yongdae Kim
   USENIX Conference on Security Symposium (USENIX Security'22) Aug. 2022
   - Demonstrate an end-to-end attack scenario, disclosing the physical locations of victims with an emergency alert message, by using a new unicast message injection attack in PHY layer.
   - Propose the mitigation to prevent identity mapping attacks and evaluate the performance.
5. **BaseSpec: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols** [paper]
   Dongkwan Kim*, Eunsoo Kim*, **CheolJun Park**, Insu Yun, and Yongdae Kim
   The Network and Distributed System Security Symposium (NDSS'21) Feb. 2021
   Acceptance rate: 15.18% (87 of 573)

Invited Talks

1. **Finding memory bugs in the cellular baseband via over-the-air interface**
   Qualcomm Product Security Summit (QPSS) San Diego, May. 2024
2. **Finding implementation vulnerabilities in cellular baseband**
   Tech session at .HACK conference Seoul, May. 2024
   Invited seminar at Korea Air Force Academy Cheongju, Apr. 2024
   Invited seminar at National Security Research Institute Daejeon, Mar. 2024
   Invited seminar at Haboob (cybersecurity company) Riyadh, Feb. 2024
3. **Finding memory bugs in the cellular baseband using over-the-air framework**
   Security at KAIST Daejeon, Nov. 2023
4. **Security attacks against the LTE network**
   Invited seminar at Sungshin Women's University Seoul, Nov. 2022
5. **DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices** [video]
   31st USENIX Security Symposium (USENIX Security'22) Boston, Aug. 2022
6. **SigOver + alpha: Signal overshadowing attack on LTE and its applications** [video] [article]
   Chaos Communication Congress (CCC) Conference (36C3) Leipzig, Dec. 2019

Skills

Tools: open-source LTE, 5G software suites (*e.g.* srsRAN, OpenAirInterface) using SDR (USRP B210, X310), SCAT (open-source mobile signalling traffic analysis tool), and wireshark

- Craft standard-compliant cellular protocol messages, mutate, and send them over the air (both uplink and downlink)

- Implementation and evaluation with passive sniffers, rogue base station, and signal injection attacks
- Experience with testing cellular implementation of many mobile devices (> 50)

Projects Involved

[G] Development of anti-sniffing technology for mobile communication and AirGap environments
- IITP grant funded by the Korean government Jun. 2024 – present
- RS-2024-00437252

[G] Development of private 5G security technology for integrated private 5G and enterprise network security
- IITP grant funded by the Korean government Apr. 2024 – present
- RS-2024-00397469

[C] Enhancing 6G security through an analysis of 5G control plane protocol vulnerabilities Apr. 2024 – present
- National Security Research Institute

[C] A study on security verification techniques for cellular networks using 5G UE simulator Apr. 2024 – present
- National Security Research Institute

[I] Research on 6G security Aug. 2021 – present
- Samsung Electronics

[G] Tracking and identifying devices and call traffic in voice phishing ecosystem Apr. 2022 – present
- Korean National Police Agency

[G] A Study on Physical Layer Security for Heterogeneous Wireless Network Jul. 2020 – Dec. 2022
- IITP grant funded by the Korean government
- No.2018-0-00831

[G] Automated security diagnosis framework for cellular network protocol using formal & comparative analysis
- IITP grant funded by the Korean government Apr. 2020 – Mar. 2023
- No.2020-0-00428

[I] Dynamic Security Testing of Control Plane Protocols Against Cellular Basebands Jul. 2019 – Jul. 2020
- Samsung Electronics

[G] Intelligent 5G core network abnormal attack detection & countermeasure technology development
- IITP grant funded by the Korean government Apr. 2019 – Dec. 2022
- No.2019-0-00793

[C] A Study on the Baseband Firmware Test Case Creation and Fuzzing Technology Mar. 2019 – Oct. 2019
- National Security Research Institute

Patents

1. KR 10-2022-0182441 (Filed)
   Stateful Black Box Testing for 5G Standalone Cellular Network
2. US18472021 (Filed), KR 10-2022-0120586 (Filed)
   Method for IMEI verification and unauthorized device detection using control plane message and the system thereof
3. US17960246 (Filed), KR 10-2514797 (Granted)
   Security analysis system and method based on negative testing for protocol implementation of LTE device
4. KR 10-254946 (Granted)
   Method and system for automatically analyzing bugs in cellular baseband software using comparative analysis based on cellular specifications
5. KR 10-2020-0133926 (Filed)
   Method to prevent mapping of user identifiers in the mobile communication system

6. US17451123 (Filed), KR 10-2450114 (Granted)
   FBS redirection attack method using unicast message injection in lte and the system thereof
7. KR 10-2514809 (Granted)
   Video identification method in lte networks and the system thereof
8. KR 10-2287190 (Granted)
   Method for measuring induced electromotive force, mtheod for tracking marker position using induced electromotive force, and apparatus for performing the same
9. PCT/KR2018/015731 (Filed), KR 10-2092445-0000 (Granted)
   Powerless electromagnetic sensor and surgical navigation system including same

Services

Reviewer

ACM Conference on Computer and Communications Security (CCS) Artifact Evaluation Committee	2024
Network and Distributed System Security Symposium (NDSS) Artifact Evaluation Committee	2025
Journal of Information Processing Systems	2024

Secondary Reviewer

IEEE Symposium on Security and Privacy (Oakland)	2021, 2024
USENIX Security Symposium (Security)	2020, 2022 – 2025
Network and Distributed System Security Symposium (NDSS)	2020, 2021, 2023, 2024
ACM Conference on Computer and Communications Security (CCS)	2019 – 2021, 2023
ACM ASIA Conference on Computer and Communications Security (ASIACCS)	2019 – 2020
USENIX Workshop on Offensive Technologies (WOOT)	2019, 2024
ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)	2024

Honors & Awards

1. Best paper award (Ministry of the Interior and Safety of South Korea), Conference on Information Security and Cryptography — Nov. 2022
2. Best paper award, Conference on Information Security and Cryptography — Nov. 2021
3. Grand prize, KIISC-KAIS Research Paper Competition — Oct. 2021
4. Best paper award (NSR Director), Conference on Information Security and Cryptography — Nov. 2020
5. Best paper award (ETRI President), Conference on Information Security and Cryptography — Jul. 2020
6. Korean Government Scholarship (Full-Ride) — Mar. 2013 – Feb. 2017

Reported Security Vulnerabilities

1. CVE-2023-43551 : Qualcomm baseband chipsets, “Cryptographic issue while performing attach with a LTE network, FBS can skip the authentication phase” (Internal report) [Qualcomm Security Bulletins]
2. CVE-2024-20039 : MediaTek baseband chipsets, “Memory crash vulnerability in NAS EMM protocol message” [Mediatek acknowledgements]
3. CVE-2023-37366 : Pixel devices, “Pixel 7 crash due to incorrect handling of malformed NAS message”, $5,000 [Android security acknowledgements]
4. CVE-2023-32890 : MediaTek baseband chipsets, “Modem crash due to incorrect handling of RRC DLInformationTransfer message” [Mediatek acknowledgements]
5. Acknowledgement from Apple: Apple devices, “Misimplementation on handling LTE test mode procedure messages” [iOS16.4 updates]

6. CVE-2022-40521, CVE-2022-40536: Qualcomm baseband chipsets, "Transient DOS due to improper authorization handling LTE test mode procedure messages" [Qualcomm Security Bulletins]
7. CVE-2022-23425: Samsung baseband chipsets, "LTE NAS authentication bypass", $14,760
8. CVE-2021-25516: Samsung baseband chipset, "Not standard-compliant behavior on handling RRC MeasurementReport message, which can result into location tracking", $2,310
9. CVE-2021-30826: Apple devices, "Authentication and key agreement (AKA) bypass issue that disables integrity and ciphering protection" [iOS15 updates]
10. CVE-2019-2289: Qualcomm baseband chipsets, "Lack of integrity check allowing modem to accept any LTE NAS messages, which can result into authentication bypass of NAS", $15,000

Experience Abroad

Student Exchange Program, TU Dortmund University, Germany	Mar. 2016 – Aug. 2016
Student Exchange Program, National Junior College, Singapore	Jul. 2012 – Jul. 2012
Summer Program, University of Michigan, USA	Jun. 2011 – Jul. 2011