Unpatched Design Vulnerabilities in Cellular Standards

Yongdae Kim

SysSec@KAIST

joint work with many of my students and collaborators

Cellular Security Publications

1. Location leaks on the GSM Air Interface, NDSS'12
2. Gaining Control of Cellular Traffic Accounting by Spurious TCP Retransmission, NDSS' 14
3. Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations, CCS'15
4. When Cellular Networks Met IPv6: Security Problems of Middleboxes in IPv6 Cellular Networks, EuroS&P'17
5. GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier, NDSS'18
6. Peeking over the Cellular Walled Gardens: A Method for Closed Network Diagnosis, IEEE TMC'18
7. Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane, S&P'19
8. Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE, Usenix Sec'19
9. Hidden Figures: Comparative Latency Analysis of Cellular Networks with Fine-grained State Machine Models, Hotmobile'19
10. BASESPEC: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols, NDSS'21
11. DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices, Usenix Sec'22
12. Watching the Watchers: Practical Video Identification Attack in LTE Networks, Usenix Sec'22
13. Preventing SIM Box Fraud Using Device Fingerprinting, NDSS'23

Cellular Security: Why Difficult? Meta

- New Generation (Technology) every 10 years
  - New Standards, Implementation, and Deployment ➔ New vulnerabilities
- Generation overlap: e.g. 3G, LTE and CSFB vulnerabilities in CSFB
- Backward compatibility: e.g. supporting 2G
- Government > Carrier > Device vendors > Customers ☺
- Walled Garden
  - Carriers and vendors don't talk to each other.
  - Carriers: (Mostly) No response to responsible disclosure
- New HW/SW tools are needed for each generation.
  - Slow/imperfect open-source development (Thank you, SRS)
  - Still waiting for 5G SA radio (USRP was useful for LTE)

"Cellular Security: Why is it difficult?", A Keynote at AsiaCCS'22, https://youtu.be/I9bUWn_xu-E

Cellular Security: Why difficult? Standard

- Complicated and huge standards ➔ Hard to find bugs, need a large group
  - Multiple protocols co-work, but written in separate docs
- Quite a few unpatched design vulnerabilities
- Standards are written ambiguously
  - Misunderstanding by vendors and carriers
  - Spec ➔ State machine for formal analysis
- Leave many implementation details for vendors
- Cellular networks/devices could be different from each carrier and vendor
  - Therefore, vulnerabilities are different
- Conformance testing standard, but (almost) no security testing standard

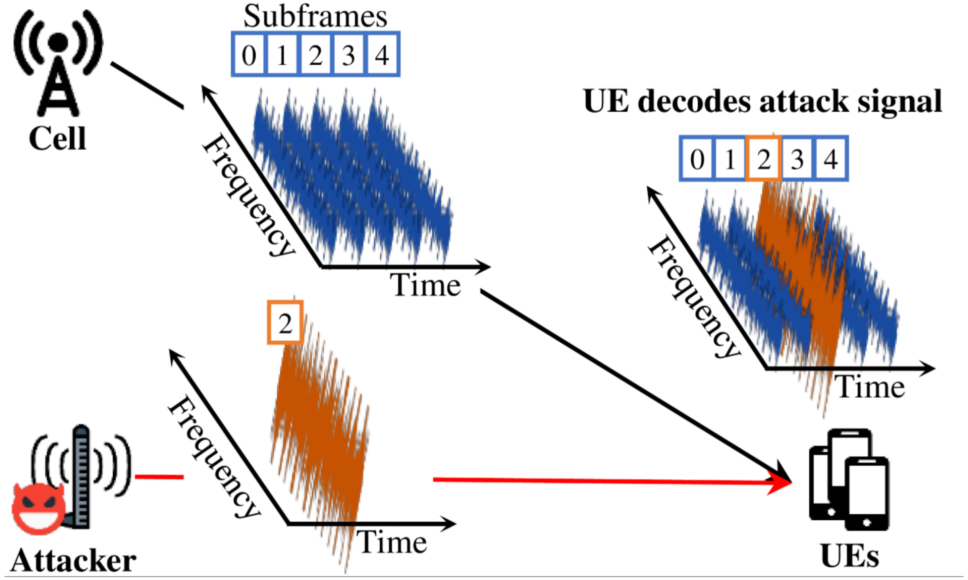
1. Unauthenticated Broadcast

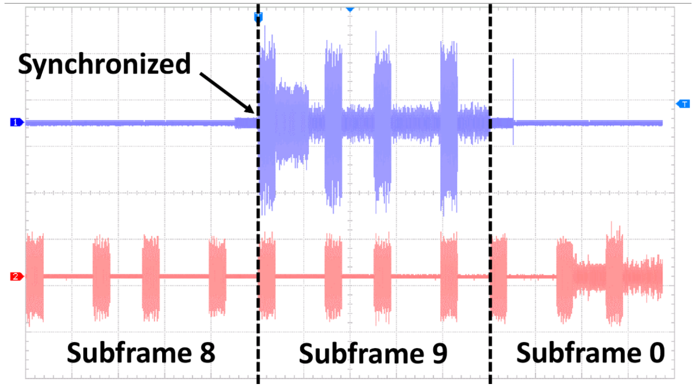
- eNB broadcasts System Information (SI) periodically
  - MIB, SIB, Paging Message
- No authentication whatsoever

Fake CMAS broadcast attack

Signal Overshadowing: SigOver Attack

- ❖ Signal injection attack exploits broadcast messages in LTE
  - – Broadcast messages in LTE have never been integrity protected!
- ❖ Transmit time- and frequency-synchronized signal





Demonstration of Signal Injection attack

DATA RESTRICTIONS

2. Unauthenticated Unicast

- Types
  - Pre-authentication messages: Attach/Identity/Authentication/TAU Re quest
  - Reject messages: Attach/TAU reject, Authentication failure

3. Unprotected Control Channel

- ❖ Downlink Control Information (DCI)
  - Requested resource by the UE
  - Scheduling information of a UE

- ❖ MAC Control Element
  - Carrier Aggregation (CA) Information
  - # of Secondary Cell

4. Linkable Identities

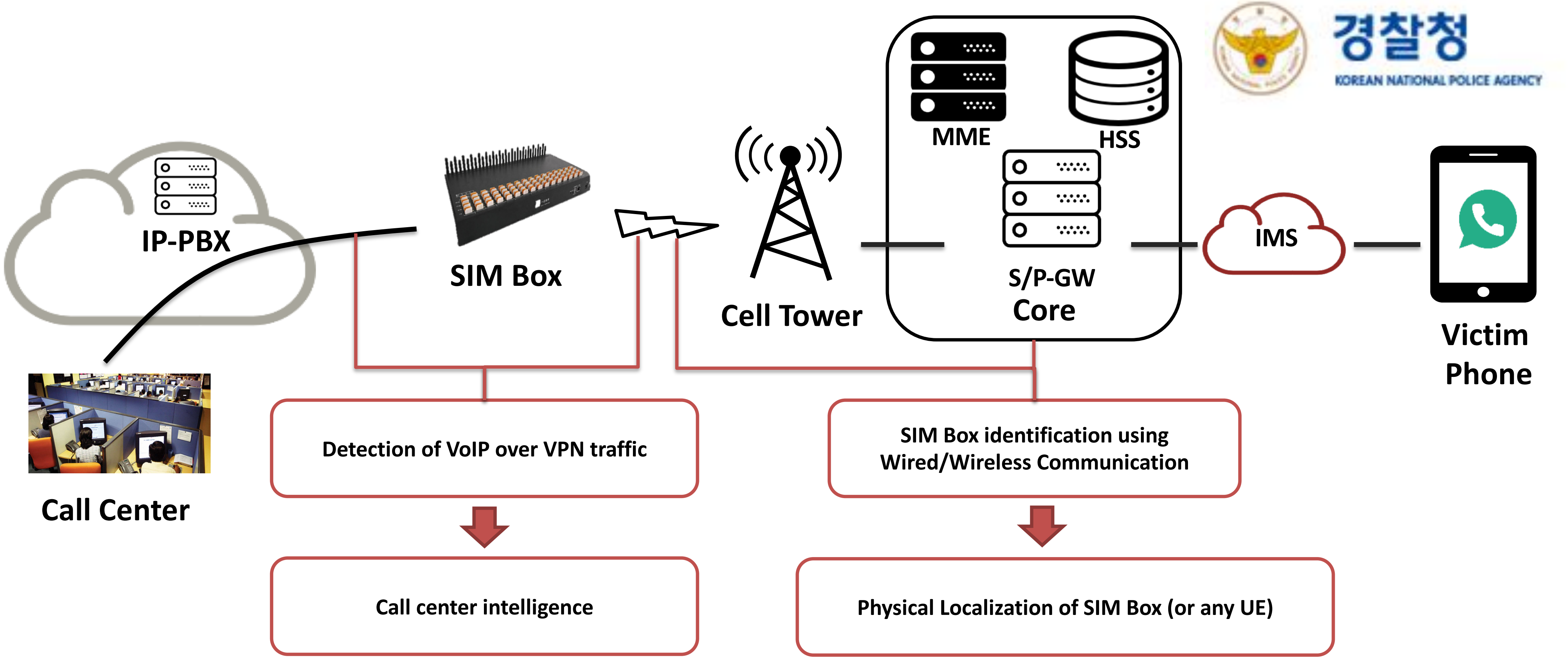
- 2G, 3G: unchanging TMSI
- 4G: unchanging GUTI ➔ Changing but linkable ➔ Mandatory unpredictability but no one implements
- 5G: Mandatory unpredictability, but have not seen any deployed one

- RNTI, GUTI, … : Application level binding

Etc.

- Still symmetric key-based key management
- Lawful interception
  - Voice call/SMS, location tracking
- eSIM vs. Physical SIM
  - SIMswap vs. SIMClone
- IMEI Spoofing

Network-based Voice Phishing Defense



경찰청
KOREAN NATIONAL POLICE AGENCY

Detection of VoIP over VPN traffic

Call center intelligence

SIM Box identification using Wired/Wireless Communication

Physical Localization of SIM Box (or any UE)

3 Projects

- Advanced Stingray
- Cellular Communication under Adversarial Network
- 6G Security Standardization after finding more design bugs

Questions?

❖ Yongdae Kim

- email: yongdaek@kaist.ac.kr
- Home: http://syssec.kaist.ac.kr/~yongdaek
- Facebook: https://www.facebook.com/y0ngdaek
- Twitter: https://twitter.com/yongdaek
- Google “Yongdae Kim”

Ministry of Science and ICT

IITP Institute of Information
& Communications
Technology Planning & Evaluation

경찰청
KOREAN NATIONAL POLICE AGENCY

SAMSUNG