VoLTE Sec + LTEFuzz + 2G/4G Location Tracking

Yongdae Kim

KAIST

SysSec Lab

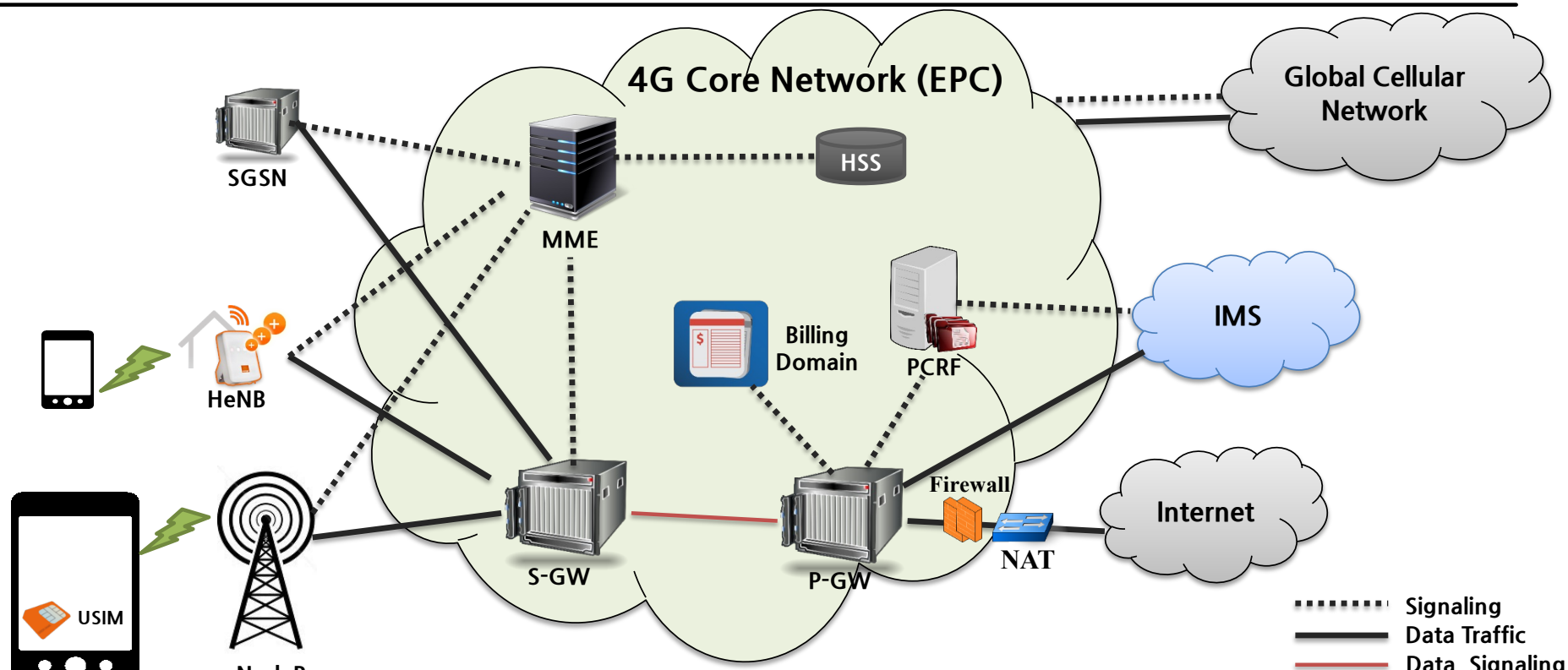
Cellular Security Publications (Selected)

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

Cellular Security US Patents

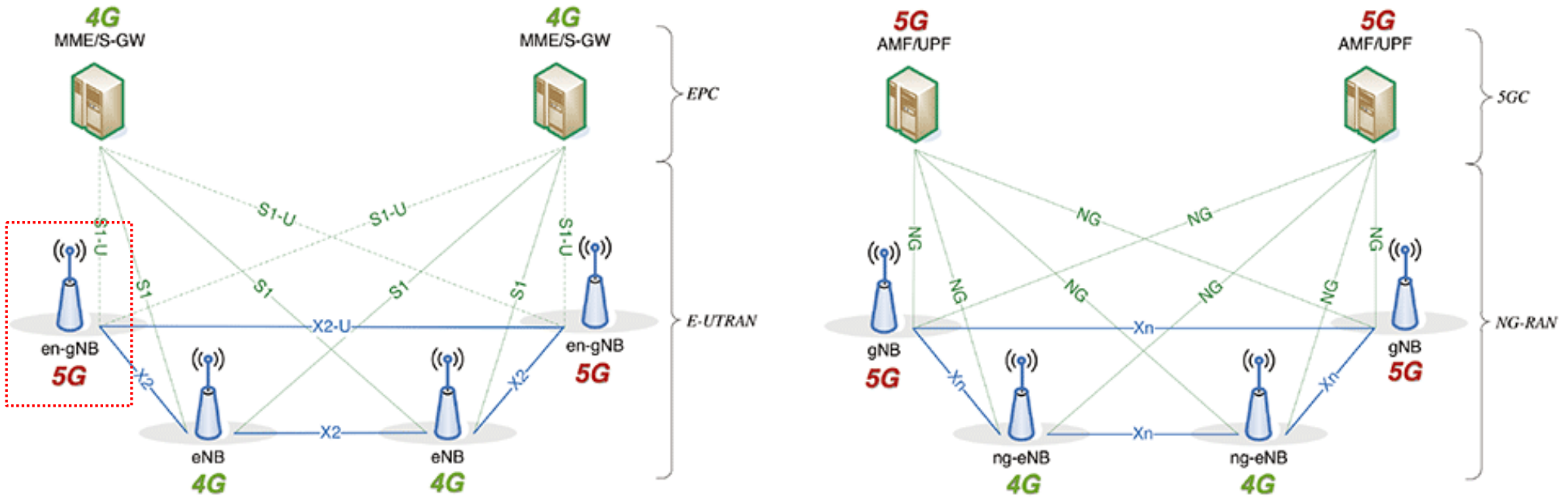
- Apparatus and method for diagnosing anomaly in mobile communication network, US10111120B2
- Physical signal overshadowing attack method for LTE broadcast message and the system thereof, US11405787B2
- Dynamic security analysis method for control plane and system therefore, US11463880B2
- Apparatus and method for diagnosing abnormality of mobile communication network using operational logic modeling and comparative analysis, US11082866B2
- …

4G LTE Cellular Network Overview



- SGSN : Service GPRS Support Node
- HSS : Home Subscriber Server
- MME : Mobility Management Entity
- S-GW : Serving Gateway
- P-GW : PDN Gateway
- PCRF : Policy and Charging Rule Function
- HeNB : Home eNodeB
- EPC : Evolved Packet Core

5G NSA vs. 5G SA



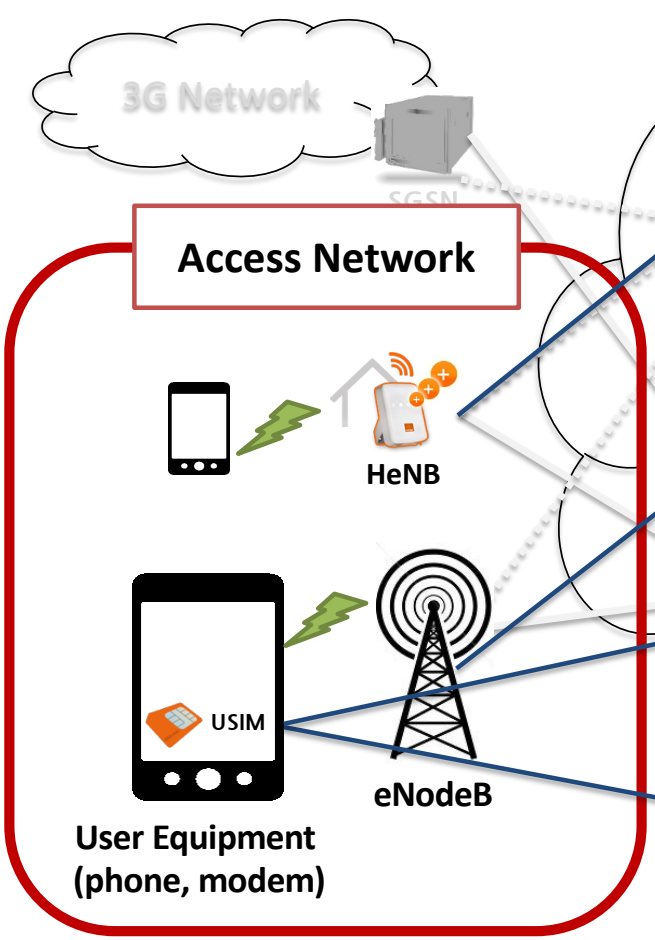
gNB (Next generation NodeB), eNB (Evolved Node B), MME (Mobility Management Entity), SPGW (Serving/Packet data network Gateway), HSS (Home Subscriber Server), IMS (IP Multimedia Subsystem)

5G Security, 6G Security?

- From control plane security point of view, 5G NSA = 4G LTE!
- There are not many devices supporting 5G SA. => No research.
- 6G Security: Too far or design issues

- In LTE alone, there are more than 200 vulnerabilities reported.
  - Still increasing ☹

Security Issues in Device & Access Network



Femtocell security

- Firmware extraction & repackaging
- Remote command injection
- Eavesdropping of call & SMS

Security analysis using SDR

- "Fake Base station": DoS on user device, privacy leak (IMSI), spoofing broadcast channel (i.e. warning message)
- "Fake UE": LTE interception attack, Core network fuzzing

3G/LTE modem security

- Remote access/command injection
- Firmware repackaging

USIM security

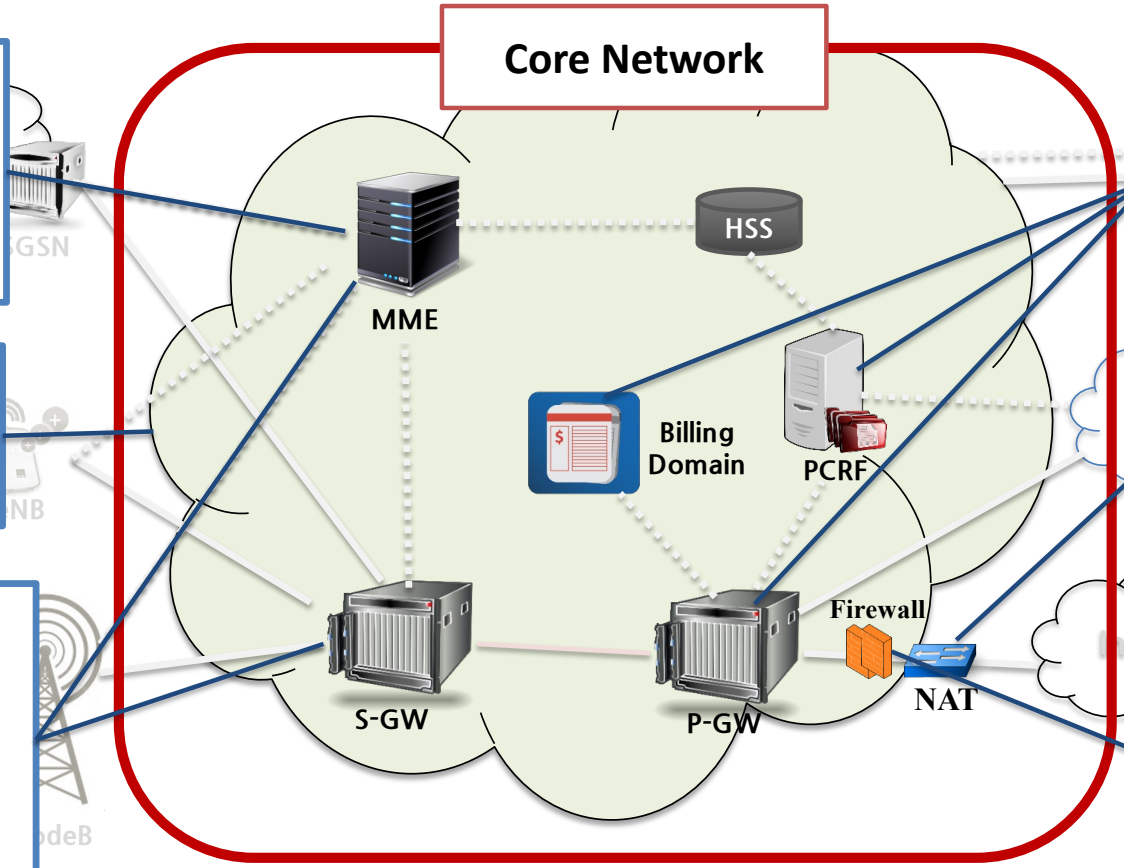
- Reading privacy info. (SMS, Phonebook, cell location)
- Get an authentication vector
- Exploit other applets

Security Issues in Core Network

Temporary ID Issue
- Skip ID Allocation
- Same ID Allocation
- Bytes Pattern
- Location Tracking

Distributed Denial of Service
- 300Gbps DDoS

Problem Diagnosis
- Comparing Signaling
- Time Threshold Detection
- Signaling Failure
- Automatic Analysis

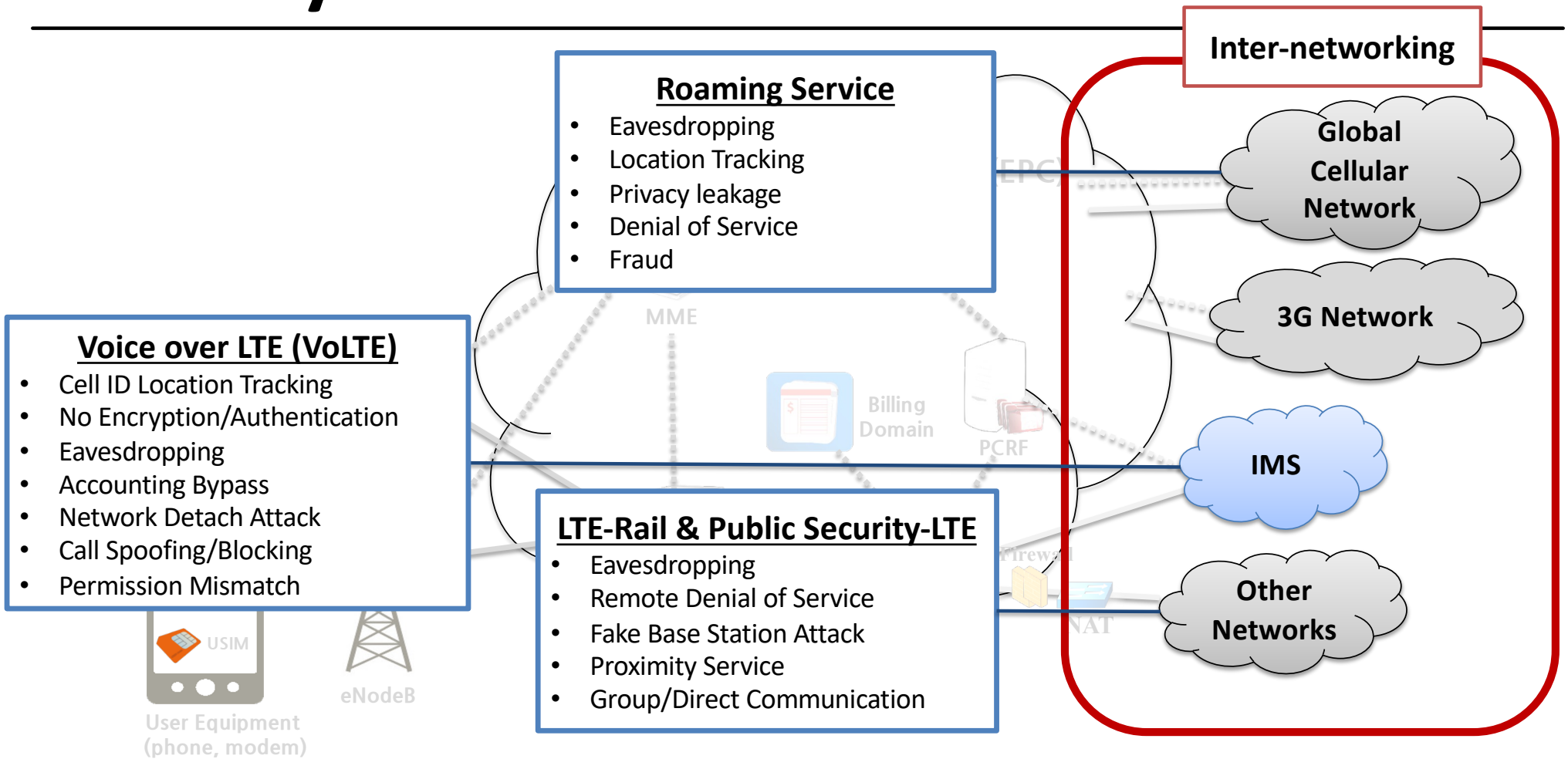


Charging policy
- Overbilling
- Free riding
  - ✓ Zero rating protocol
  - ✓ TCP Retransmission

NAT
- NAT Public IP Disabling
- NAT Resource Exhaustion

Firewall
- TCP-RST DoS
- Overbilling
- DDoS
- Scanning
- Fingerprinting

Security Issues in Services



Cellular vs. Network Security: Why Difficult?

- New Generation (Technology) every 10 year
  - New Standards, Implementation, and Deployment ➔ New vulnerabilities
- Generation Overlap, e.g. LTE CSFB, 5G NSA
  - CSFB: 3G, LTE and CSFB vulnerabilities
- Cellular networks are different from each carrier, manufacturer, operator in terms of implementations and configurations
  - Therefore, vulnerabilities are different ➔ Need for global measurement
- Walled Garden
  - Carriers (smartphone vendors) don't talk to each other.
  - One vulnerability from a carrier will appear in other carriers.

Cellular Security: Special Circumstances

- Governance: 3GPP, GSMA, Government
  - Device manufacturers tend to follow carrier's requirement.
- Very few experts who know Cellular Technology and Security
- Complicated and huge standards ➔ Hard to find bugs, need large group
- Standards are not written in formal languages ➔ Hard for formal analysis
- Leave many implementation details for vendors ➔ Bugs
- Most of the cellular security analyses have been manual.
- New HW/SW tools are needed for each generation.
  - Slow/imperfect open-source development. Thank you, SRS!

Security Problems in Standard

Signaling System No. 7 (SS7) for roaming service

- SS7
  - Protocol suite used by most cellular operators throughout the world to talk to each other
  - When it was designed, there were only few operators
  - Closed and trusted, no authentication built in
- Getting an access to SS7 is easier than ever
  - Bought from operators or roaming hubs for a few hundred euros a month
  - Some operators are reselling roaming agreements
  - Unsecured equipment on the Internet
- Diameter for 4G LTE

Results of Security Measurement

MAP message	Threat Category	Target	Prerequisites
updateLocation	**DoS, Interception**	**All the subscriber**	**IMSI**
cancelLocation	DoS	Roaming subscriber	IMSI
purgeMS	DoS	Roaming subscriber	IMSI
insertSubscriberData deleteSubscriberData	DoS	Roaming subscriber	IMSI and MSISDN
restoreData	Leak, DoS	Roaming subscriber	IMSI
sendIMSI	Leak	Roaming subscriber	MSISDN
provideSubscriberInfo	Tracking	Roaming subscriber	IMSI

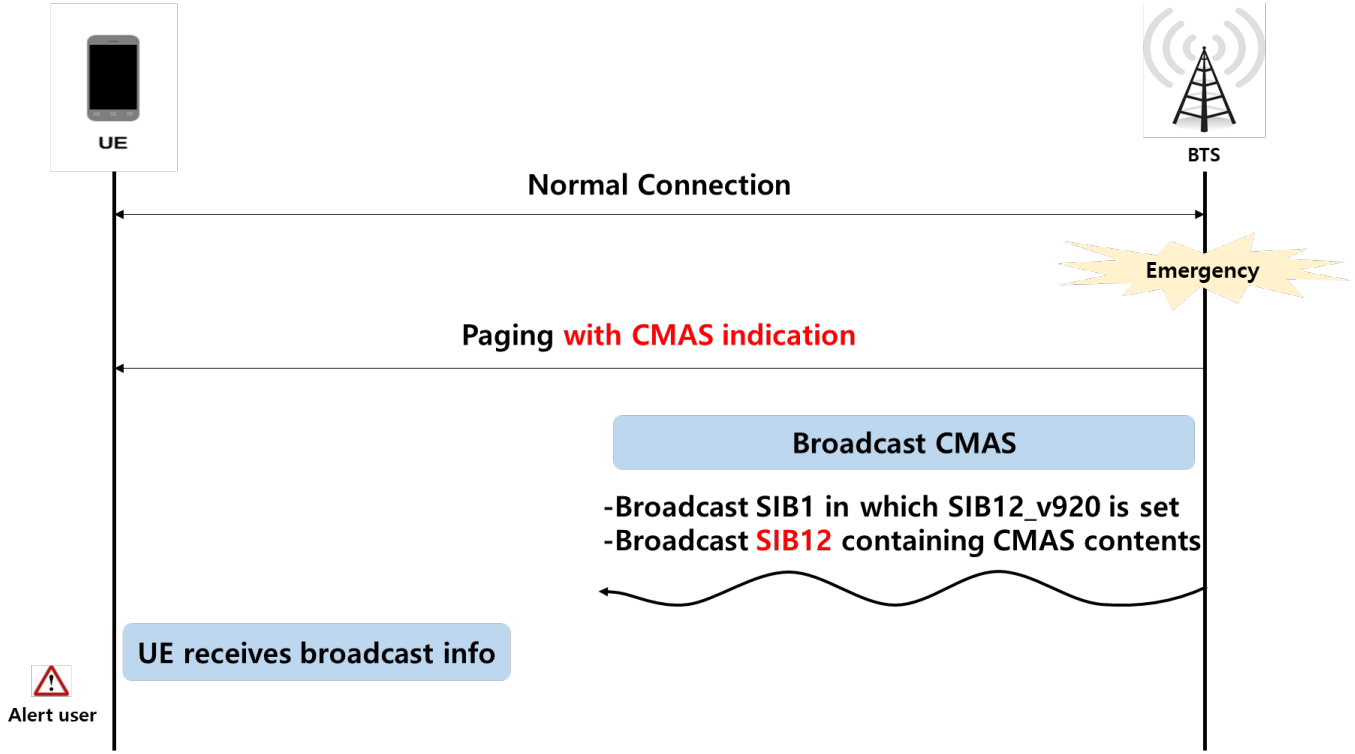
Eavesdropping Phone Calls

Unprotected Broadcast Channel

- eNB broadcasts System Information (SI) periodically
  - Master Information Block (MIB)
    - SIB scheduling information, most frequently used
  - System Information Block (SIB)
    - Various system info (e.g. information needed for UE's cell selection)
    - Might include emergency alert
  - Paging Message
    - Tell Idle/Inactive UE about existing downlink data

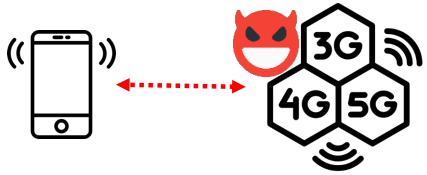
- No authentication whatsoever

CMAS Protocol

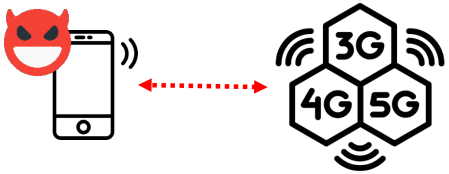


Fake CMAS broadcast attack

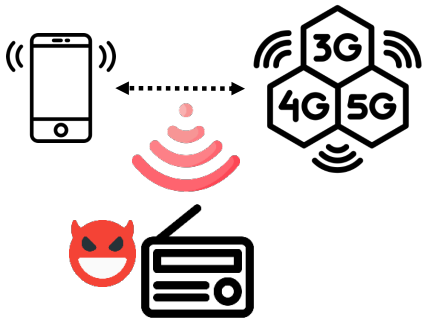
Threat Model



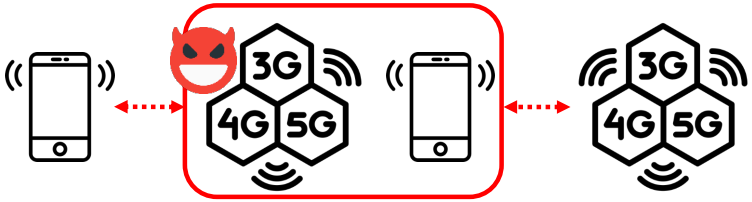
Fake base station



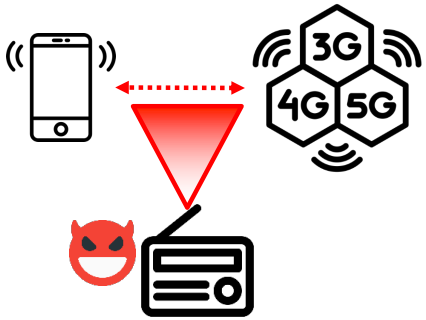
Fake UE



Sniffer



Man-in-the-Middle (MitM)

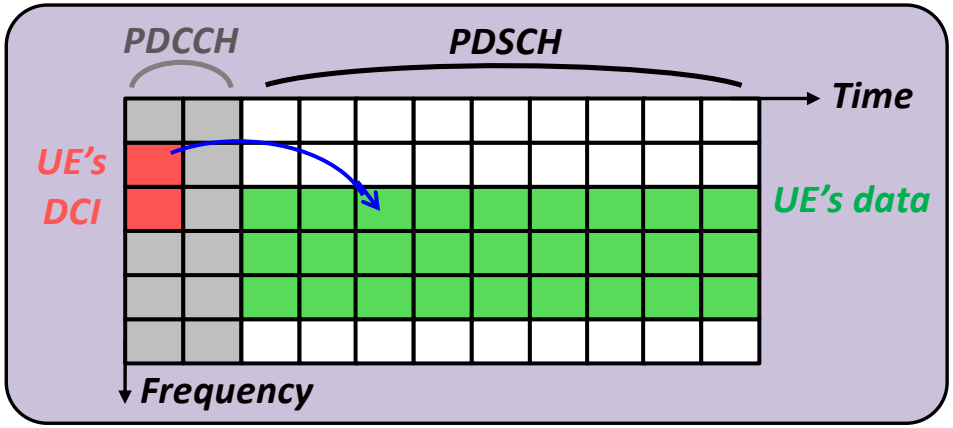


SigOver (Overshadowing)

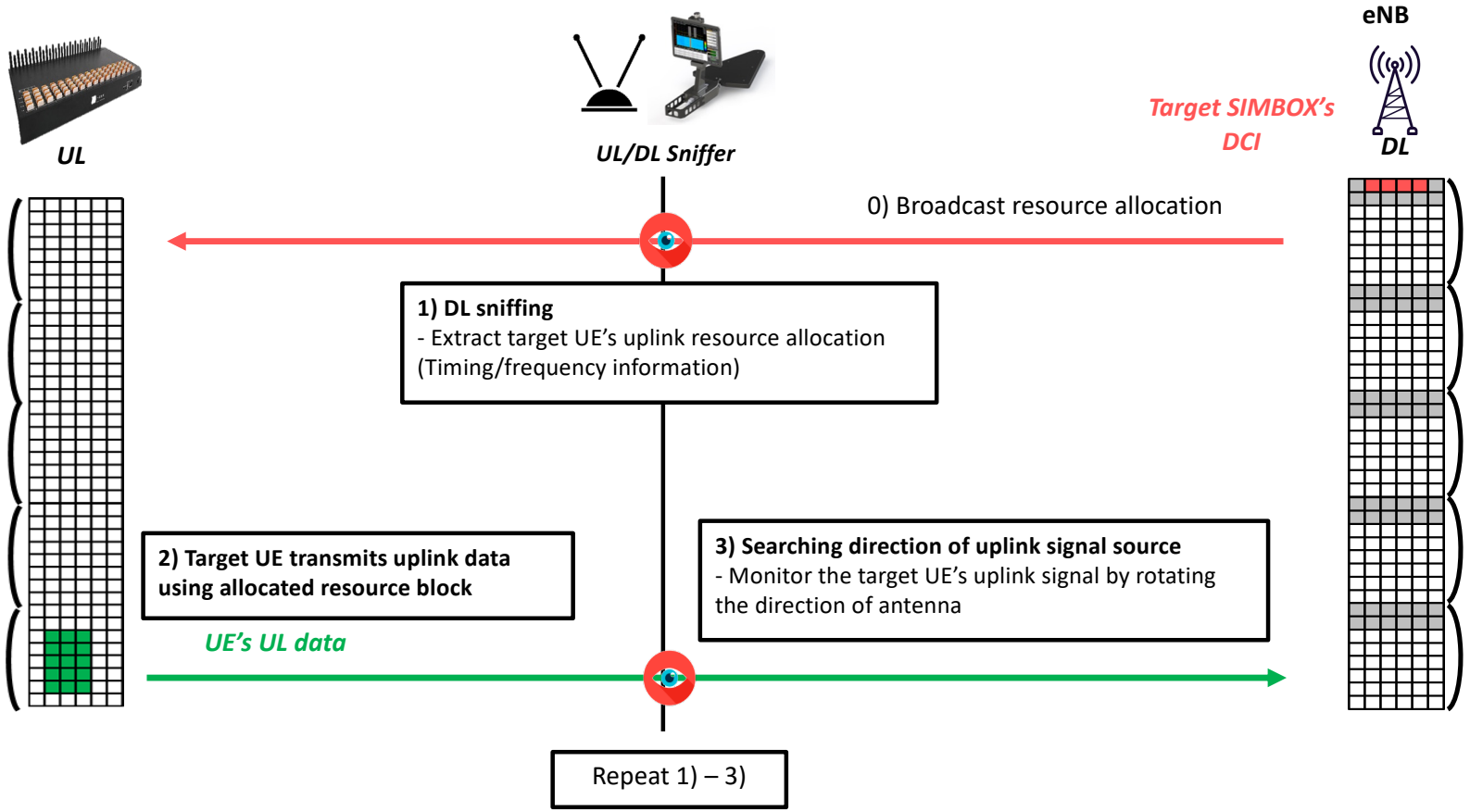
Downlink Data Transmission Information is Leaked

- eNB (base station) controls DL data transmission by broadcasting DCI
- Downlink Control Indicator (DCI)
  - Descriptions about DL data transmitted to the UE
    - Data volume, modulation scheme, allocated resource blocks (RB)
  - Distinguished by RNTI

This information is broadcast in plain text

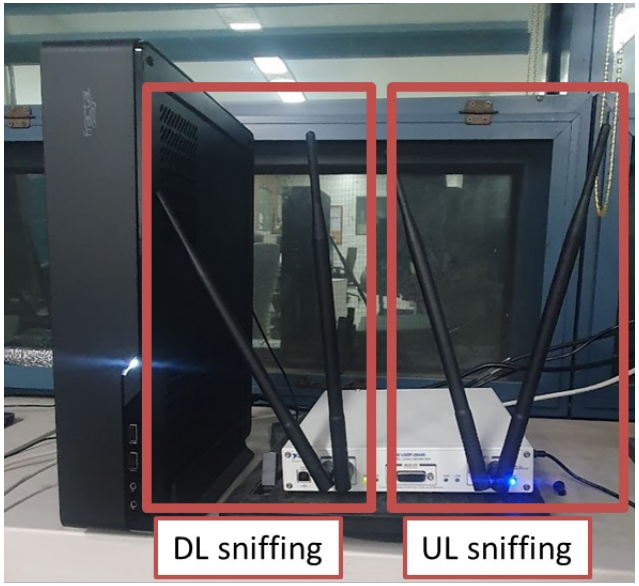


Localization



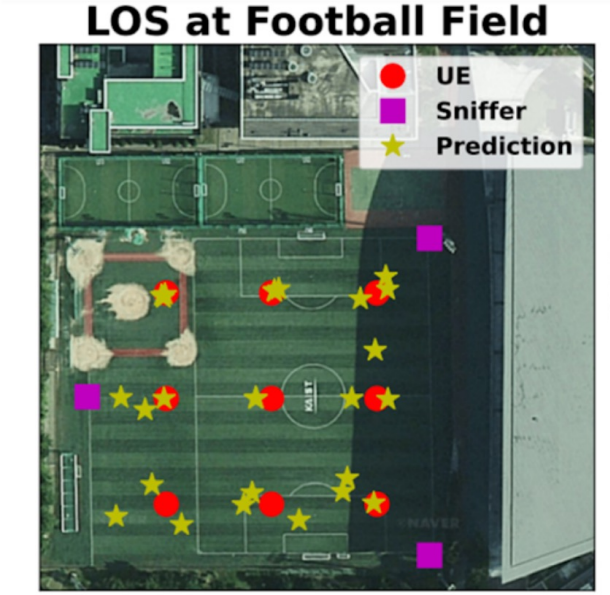
Implementation

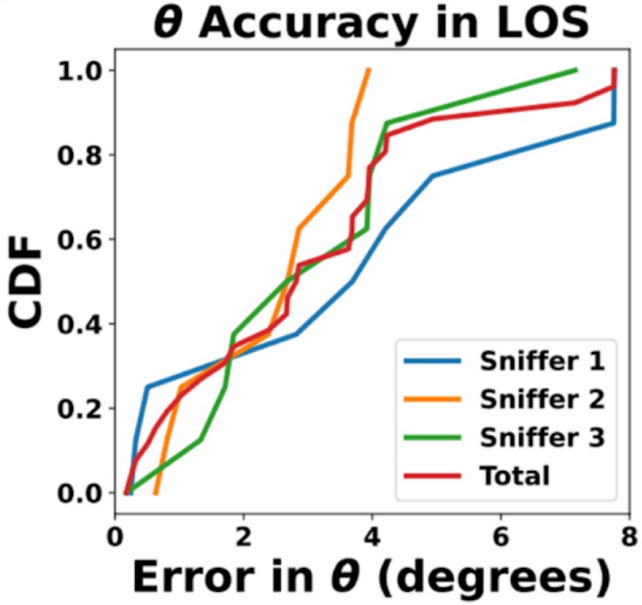
- UL Sniffer
  - Operate with Single USRP X310
    - Capture uplink/downlink signal simultaneously
      - Octoclock is not needed
    - Sync with DL signal from eNB
  - Operate in real time
    - Modify/Add ~1K LoC of C++ FALCON (open-source DL sniffer)
      - Match with monitored UL
      - Compute signal strength
    - Optimize to UL resource allocation extraction

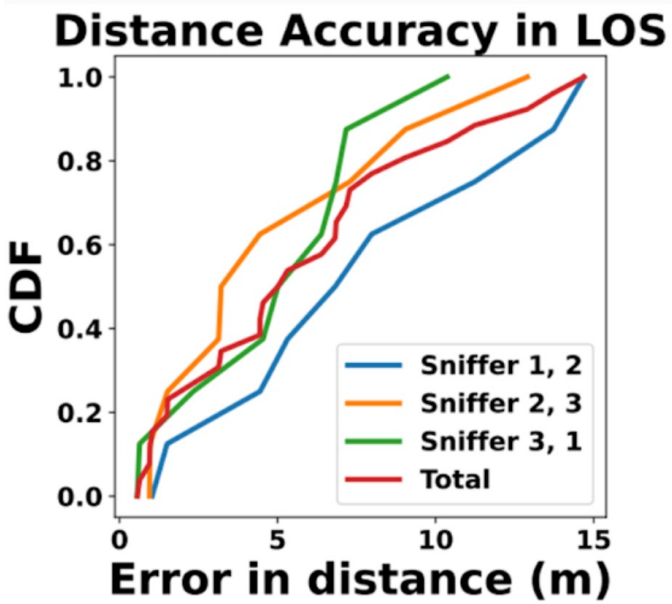


- RF frontend
  - Directional antenna (Various gain/beam width)

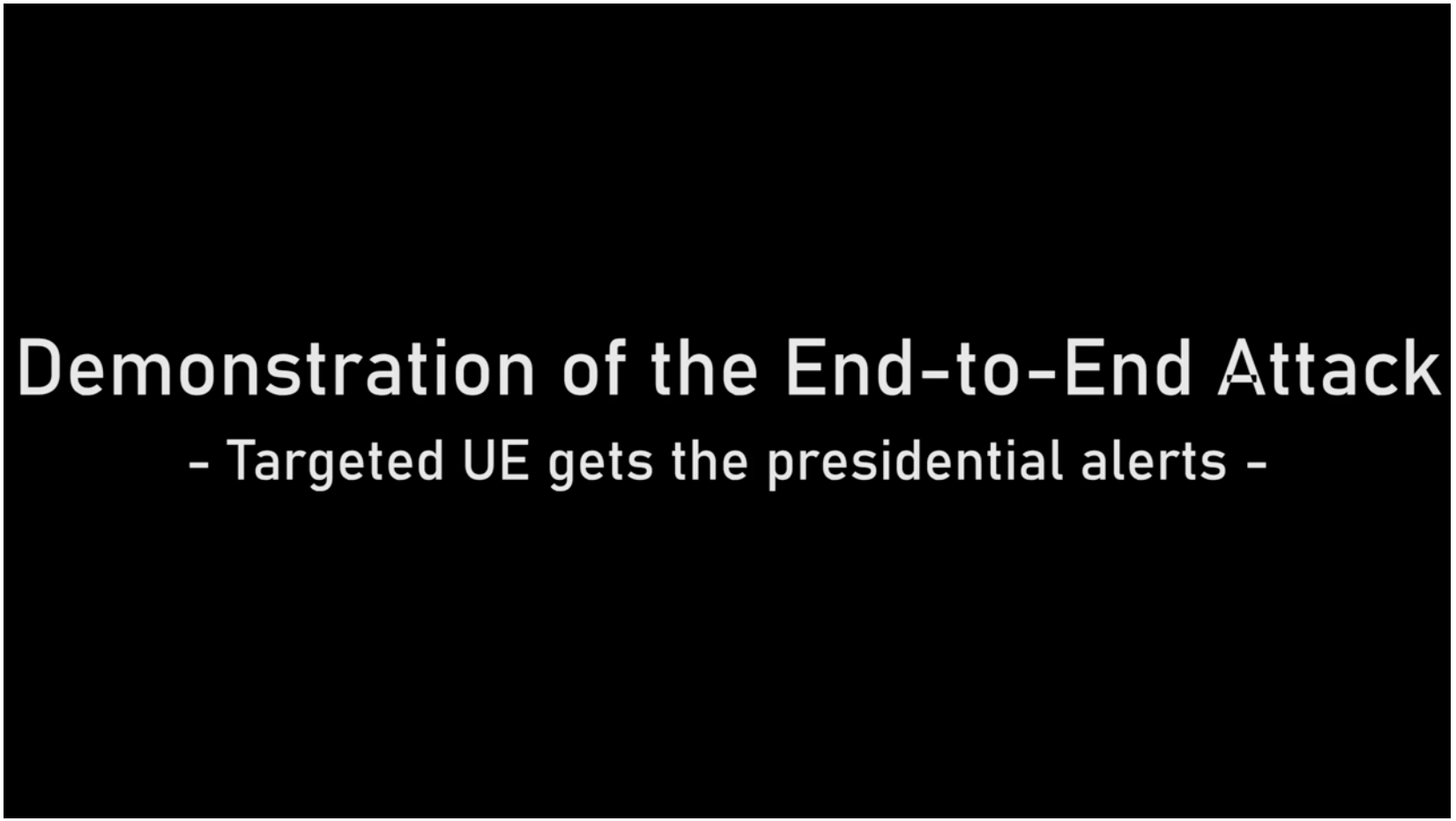
LoS Experiment







Unencrypted DCI + Unprotected Unicast



Cellular Insecurity in Standard

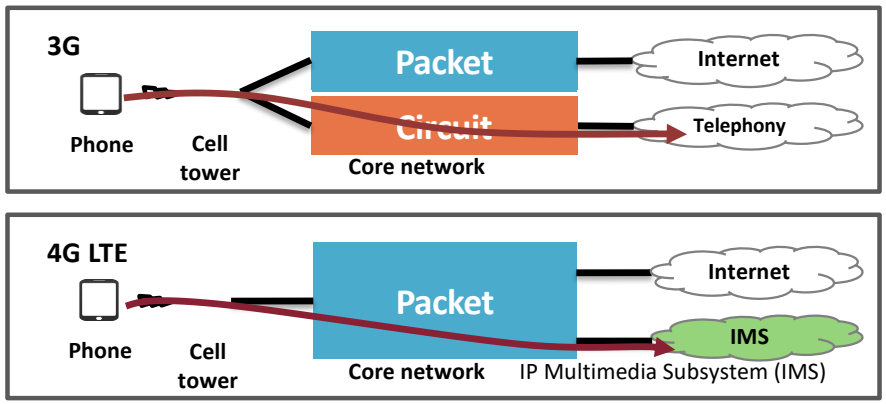
- Roaming Network such as SS7 and Diameter
- Unprotected Broadcast/Unicast Channel
- Unprotected Control Channel
- Trackable Temporary Identities
- No voice encryption
- Lawful Interception
- Still symmetric key-based key management

- These need to be fixed in 6G

Security of New Systems

VoLTE = Voice over LTE

- Implementation of VoIP on LTE
- 3G network
  - Data and voice are separated

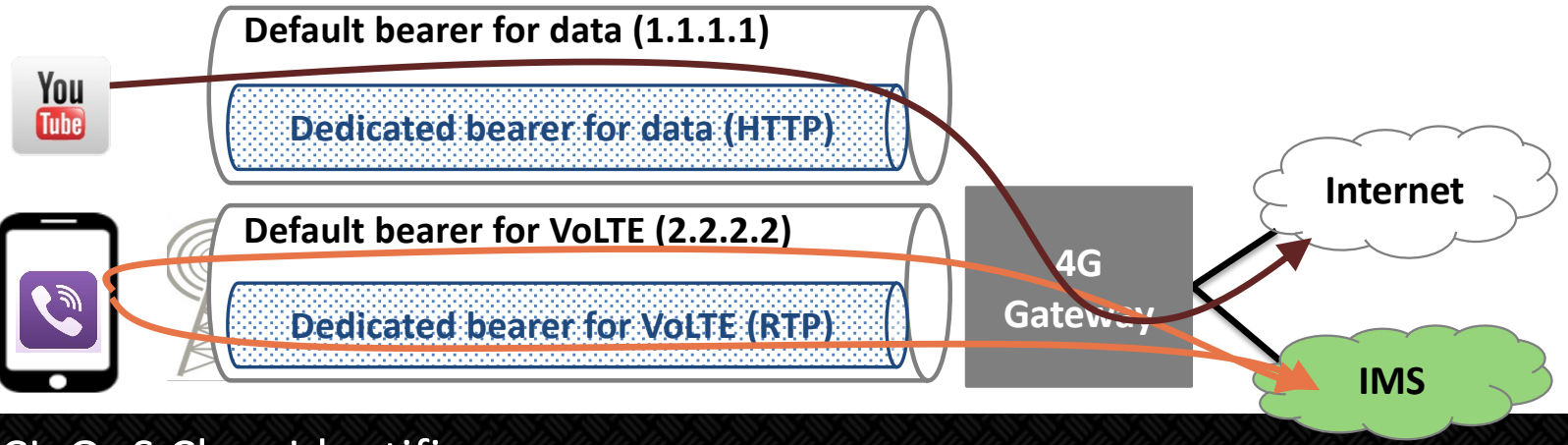


- 4G LTE network : All-IP based Network
  - Both data and voice are delivered as data-flow

- Advantages on VoLTE
  - **For users**: high voice quality, faster call setup, better battery life.
  - **For operators**: increase usability, reduce cost, rich multimedia services

Each service is delivered by bearer

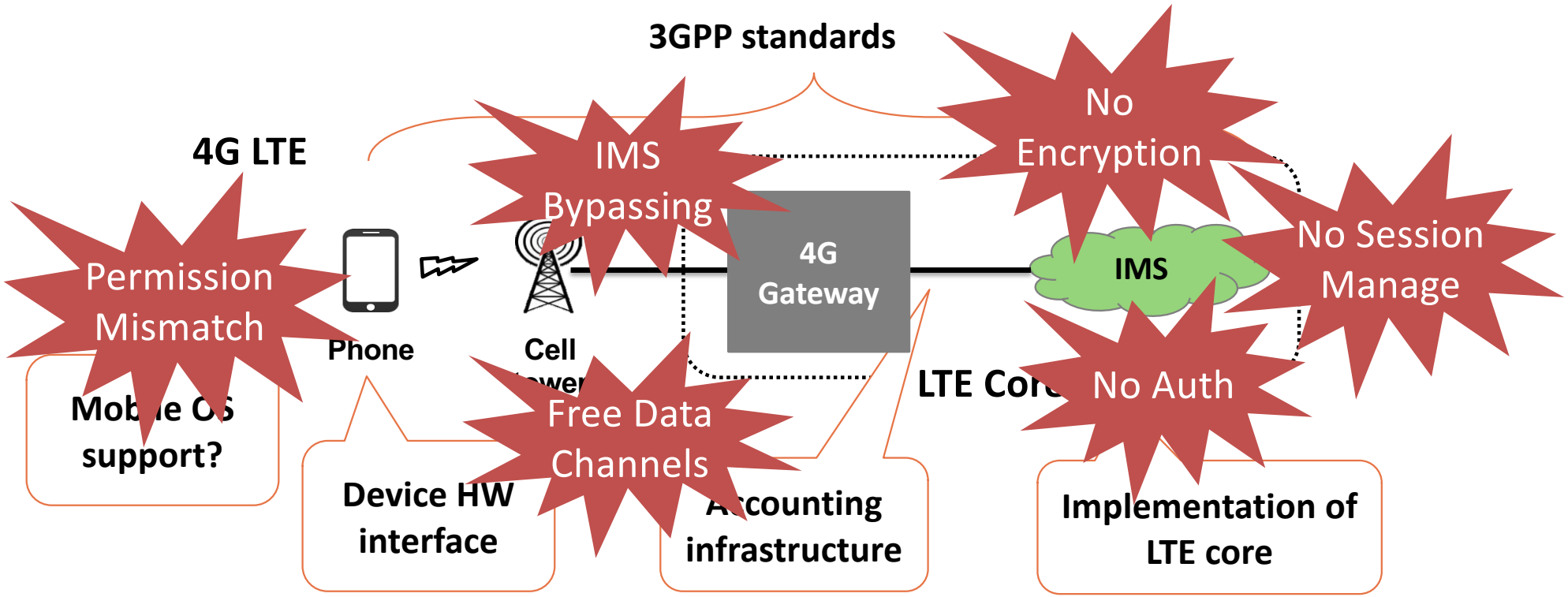
- In LTE, all services are delivered data channels, called “bearers”
  - Data, Voice, Video, …
- **Bearer**: a virtual channel with below properties
  - Based on **QCI*** value, it determines bandwidth, loss rate, latency (QoS)
  - **Default bearer**: Non Guaranteed Bit rate
  - **Dedicated bearer**: Guaranteed Bit rate



*QCI: QoS Class Identifier

VoLTE makes cellular network more complex

- Let's check potential attack vectors newly introduced in VoLTE

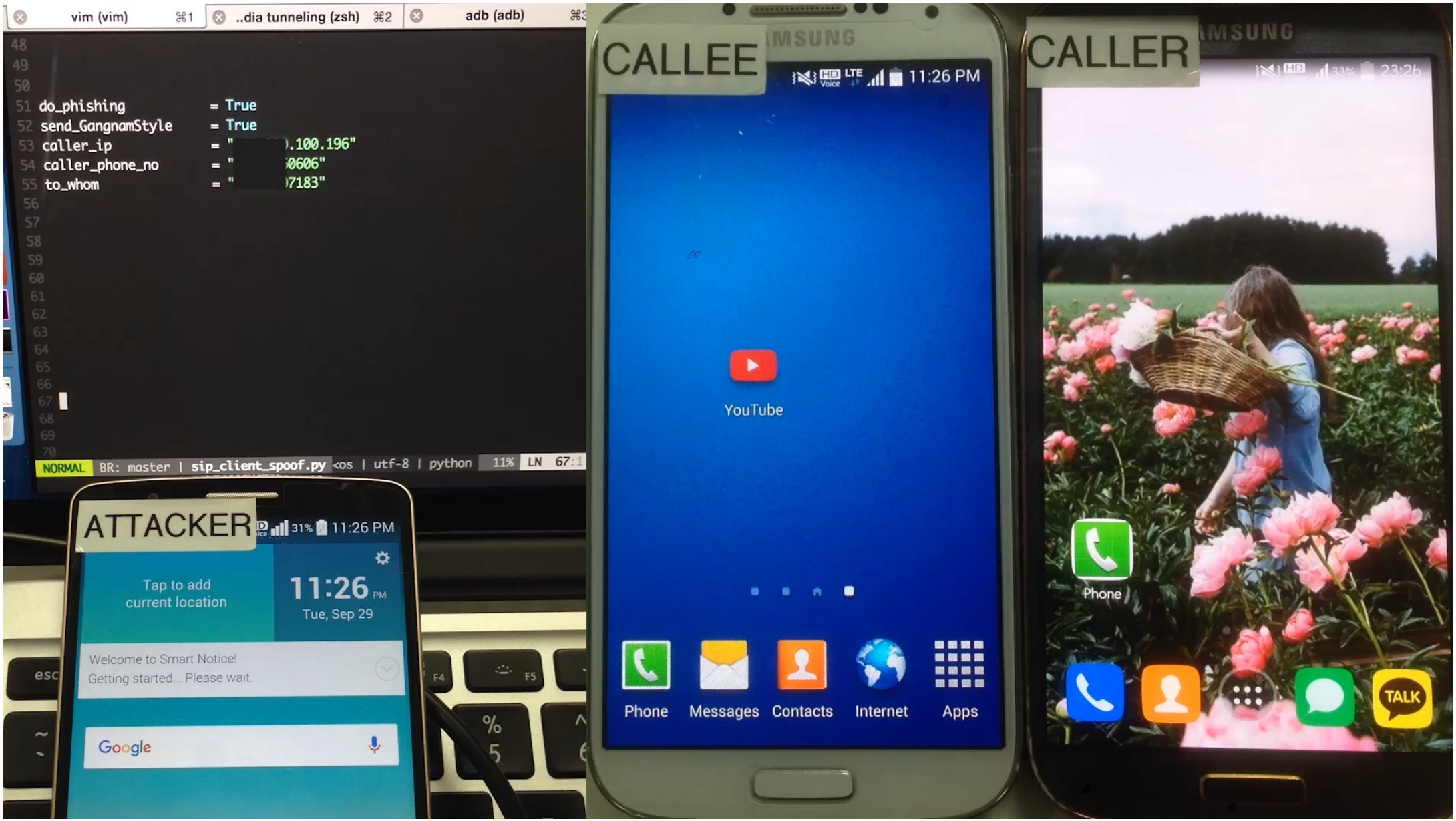


Free Data Channels	Free Channel	US-1	US-2	KR-1	KR-2	KR-3
Using VoLTE Protocol	SIP Tunneling	✓	✓	✓	✓	✓
	Media Tunneling	✓	✓	✓	✓	✓
Direct Communication	Phone to Phone	✓	✗	✓	✗	✗
	Phone to Internet	✗	✓	✓	✗	✗

Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
IMS	No SIP Encryption						Message manipulation
	No Voice Data Encryption						Wiretapping
	No Authentication						Caller Spoofing
	No Session Management						Denial of Service on Core Network
4G-GW	IMS Bypassing						Caller Spoofing
Phone	Permission Mismatch	Vulnerable for all Android					Denial of Service on Call, Overbilling

 : Vulnerable  : Secure

SysSec System Security Lab


vim (vim) ⌘1
..dia tunneling (zsh) ⌘2
adb (adb)
do_phishing = True
send_GangnamStyle = True
caller_ip = "
.100.196"
caller_phone_no = "
0606"
to_whom = "
7183"
NORMAL BR: master | sip_client_spoof.py <os | utf-8 | python 11% LN 67:1
ATTACKER
31% 11:26 PM
Tap to add current location
11:26 PM
Tue, Sep 29
Welcome to Smart Notice!
Getting started... Please wait.
Google
CALLEE
11:26 PM
YouTube
Phone
Messages
Contacts
Internet
Apps
CALLER
Phone
TALK

Discussion

www.kb.cert.org/vuls/id/943167

CERT | Software Engineering

Vulnerability No

Advisory

DATABA

Vulne

Voice

Original R

CWE-732

CWE-284

CWE-287

CWE-384

Elevation Of Privilege Vulnerability in Telephony

A vulnerability in the Telephony component that can enable a local malicious application to pass unauthorized data to the restricted network interfaces, potentially impacting data charges. It could also prevent the device from receiving calls as well as allowing an attacker to control

Acknowledgements

We would like to thank these researchers for their contributions:

- Abhishek Arya, Oliver Chang and Martin Barbella, Google Chrome Security Team: CVE-2015-6608
- Daniel Micay (daniel.micay@copperhead.co) at Copperhead Security: CVE-2015-6609
- Dongkwan Kim of System Security Lab, KAIST (dkay@kaist.ac.kr): CVE-2015-6614
- Hongil Kim of System Security Lab, KAIST (hongilk@kaist.ac.kr): CVE-2015-6614
- Jack Tang of Trend Micro (@jacktang310): CVE-2015-6611
- Peter Pi of Trend Micro: CVE-2015-6611
- Natalie Silvanovich of Google Project Zero: CVE-2015-6608
- Qidan He (@flanker_hqd) and Wen Xu (@antlr7) from KeenTeam (@K33nTeam, http://k33nteam.org/): CVE-2015-6612
- Seven Shen of Trend Micro: CVE-2015-6610

Conclusion

- Newly adopted VoLTE has
  - A complex (legacy time-based) accounting
  - Delegated voice signal (previously done by CP) to AP
- We analyzed the security of VoLTE for 5 operators, and found
  - Four free data channels
  - Five security problems
- All related parties have problems
  - 3GPP, telcos, IMS providers, mobile OSes, and device vendors
- More and more reliance on cellular technology
  - Automobiles, power grid, traffic signal, ...

Holistic re-evaluation of security for VoLTE?

ISPs don’t talk to each other!

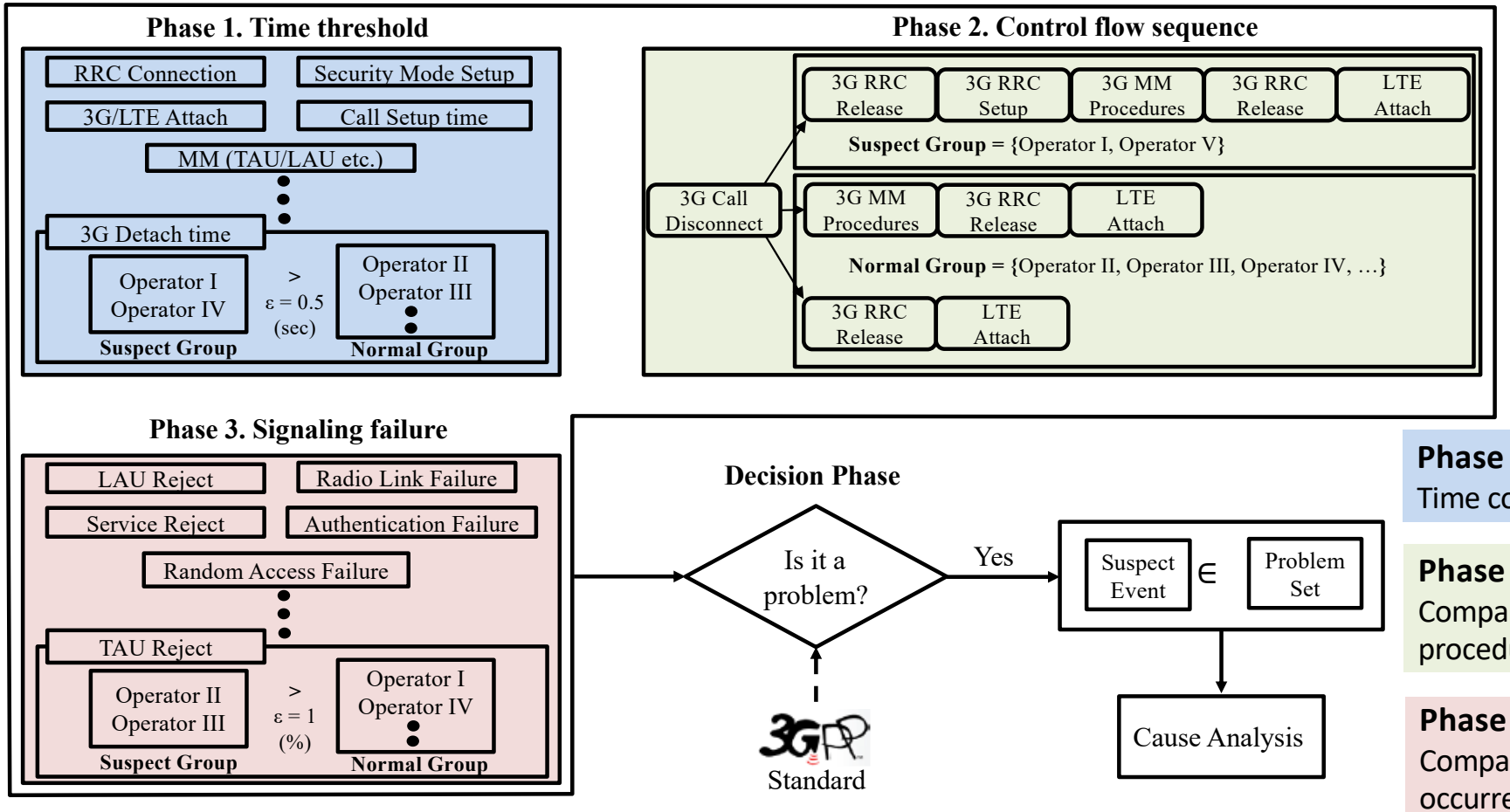
Worldwide Data Collection

Country	# of OP.	# of signalings	Country	# of OP.	# of signalings
U.S.A	3	763K	U.K.	1	41K
Austria	3	807K	Spain	2	51K
Belgium	3	372K	Netherlands	3	946K
Switzerland	3	559K	Japan	1	37K
Germany	4	841K	South Korea	3	1.7M
France	2	305K			

Data summary

of countries: **11**
# of operators: **28**
# of USIMs: **95**
# of voice calls: **52K**
# of signalings (control-plane message): **6.4M**

Problem Diagnosis Overview



Phase 1
Time comparison by procedure

Phase 2
Comparison of signaling procedure sequence

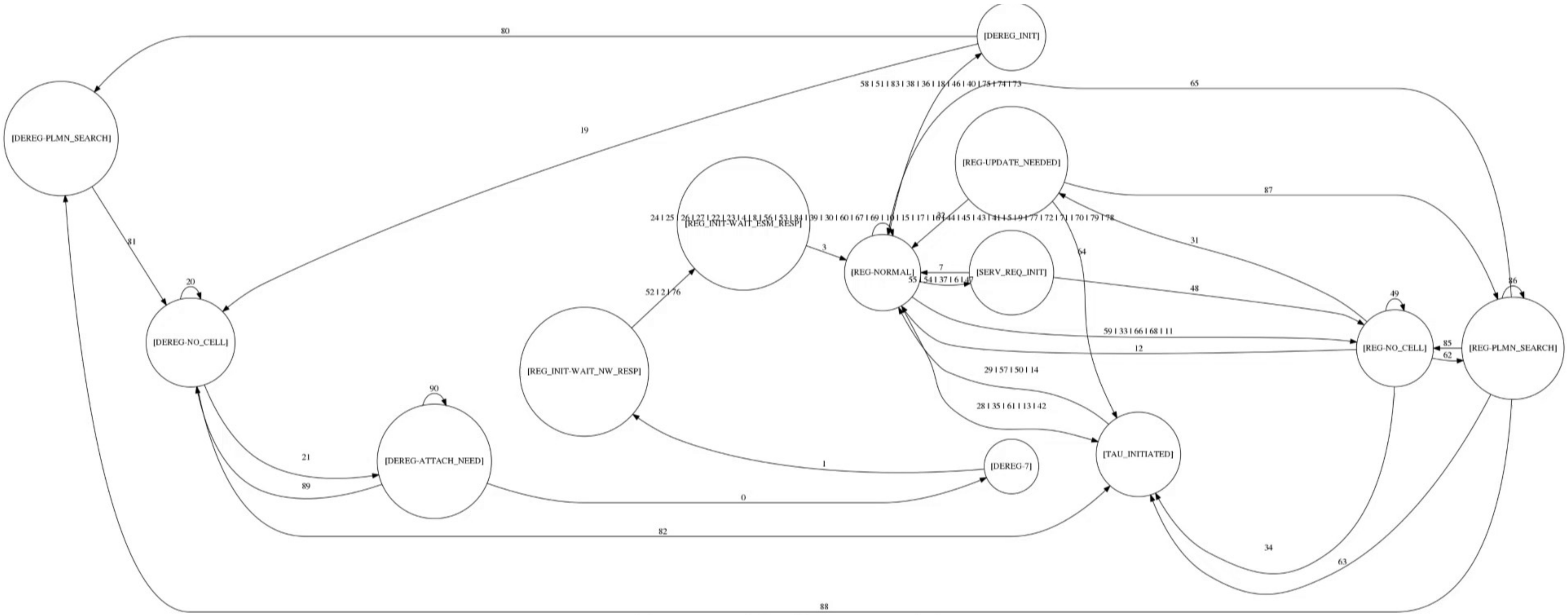
Phase 3
Comparison of signaling failure occurrence probability

Identified Problems

Problem	Observation	Operator
LTE location update collision	**Out-of-service** about **11 sec**.	US-II
Mismatch procedures	Delay of 3G detach. Worst case: **10.5 sec.**	US-I, DE-I. DE-II, FR-I, FR-II
Allocation of incorrect frequency	**Out-of-service 30 sec**. and **stuck in 3G for 100 sec.**	DE-I
Redundant location update	Delay of LTE attach or call setup. Worst case: **6.5 sec.**	US-I, DE-I, DE-III, FR-II
Redundant authentication	Delay of CSFB procedures for 0.4 sec.	FR-I, FR-II, DE-I, DE-III, FR-II
Security context sharing error	Out-of-service 1.5 sec.	ES-I
Core node handover misconfiguration	Delay of LTE attach (0.4 sec.)	US-II

Automated Protocol/System Analysis

- Our solution: **analysis with state machine**
  - Generate *analyzable/comparable* **state machine**
    - Manipulate the state machine described in 3GPP standards
      - But, represent the interactions between RRC, EMM, and ESM layer
    - Analyze the transmitted control plane messages during state transition
      - Include sufficient information such as timing, detailed values in each signaling msg
  - Inferring & Comparing state machines between multiple carriers
- Possible Usages
  - Protocol optimization: Find relatively slow procedures and root causes
  - Discover misconfigurations: Find undesired/suspicious operations
  - Find vendor specific implementation or procedure
  - Find security holes


[DEREG_INIT]
80
58 | 51 | 83 | 38 | 36 | 18 | 46 | 40 | 75 | 74 | 73
65
[DEREG-PLMN_SEARCH]
19
[REG-UPDATE_NEEDED]
87
[REG_INIT-WAIT_ESM_RESP]
24 | 25 | 26 | 27 | 22 | 23 | 4 | 8 | 56 | 53 | 84 | 39 | 30 | 60 | 67 | 69 | 10 | 15 | 17 | 16 | 44 | 45 | 43 | 41 | 5 | 9 | 77 | 72 | 71 | 70 | 79 | 78
32
81
3
64
31
[REG-NORMAL]
7
[SERV_REQ_INIT]
55 | 54 | 37 | 6 | 47
20
52 | 2 | 76
48
49
86
[DEREG-NO_CELL]
59 | 33 | 66 | 68 | 11
[REG-NO_CELL]
85
[REG-PLMN_SEARCH]
12
62
[REG_INIT-WAIT_NW_RESP]
29 | 57 | 50 | 14
28 | 35 | 61 | 13 | 42
90
21
[DEREG-ATTACH_NEED]
[DEREG-7]
[TAU_INITIATED]
1
89
0
82
34
63
88

Fuzzing LTE Core and Baseband

Touching the Untouchables - Dynamic Security Analysis of the LTE Control Plane -

H Kim, J Lee, E Lee, Y Kim

2019 IEEE Symposium on Security and Privacy (SP)

Fundamental Problems in cellular network

- Description of standard (3GPP) is ambiguous
  - The 3GPP specifications are based on natural language
  - Standard leave implementation (exact behavior) details to the vendors
  - There are conformance test specs…
    - But, no security testing specs

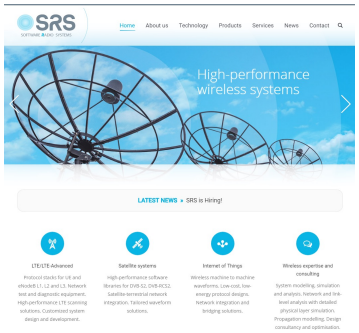
- Mobile network operators & vendors rarely communicate with each other
  - Different carriers with different device vendors suffer from different vulnerabilities

Goal of this paper

- **Goal:** Investigate potential problems of the control plane procedures
  - **Rooted from either**
    - Design flaws
    - Implementation mistakes
    - Configurations issues
  - **How?** Comprehensive dynamic testing against LTE components
- **Challenges in dynamic network testing**
  1. Hard to control the behaviors of commercial baseband
  2. Carrier networks are closed system
  3. Transmitting radio signals to an operational network might not be allowed

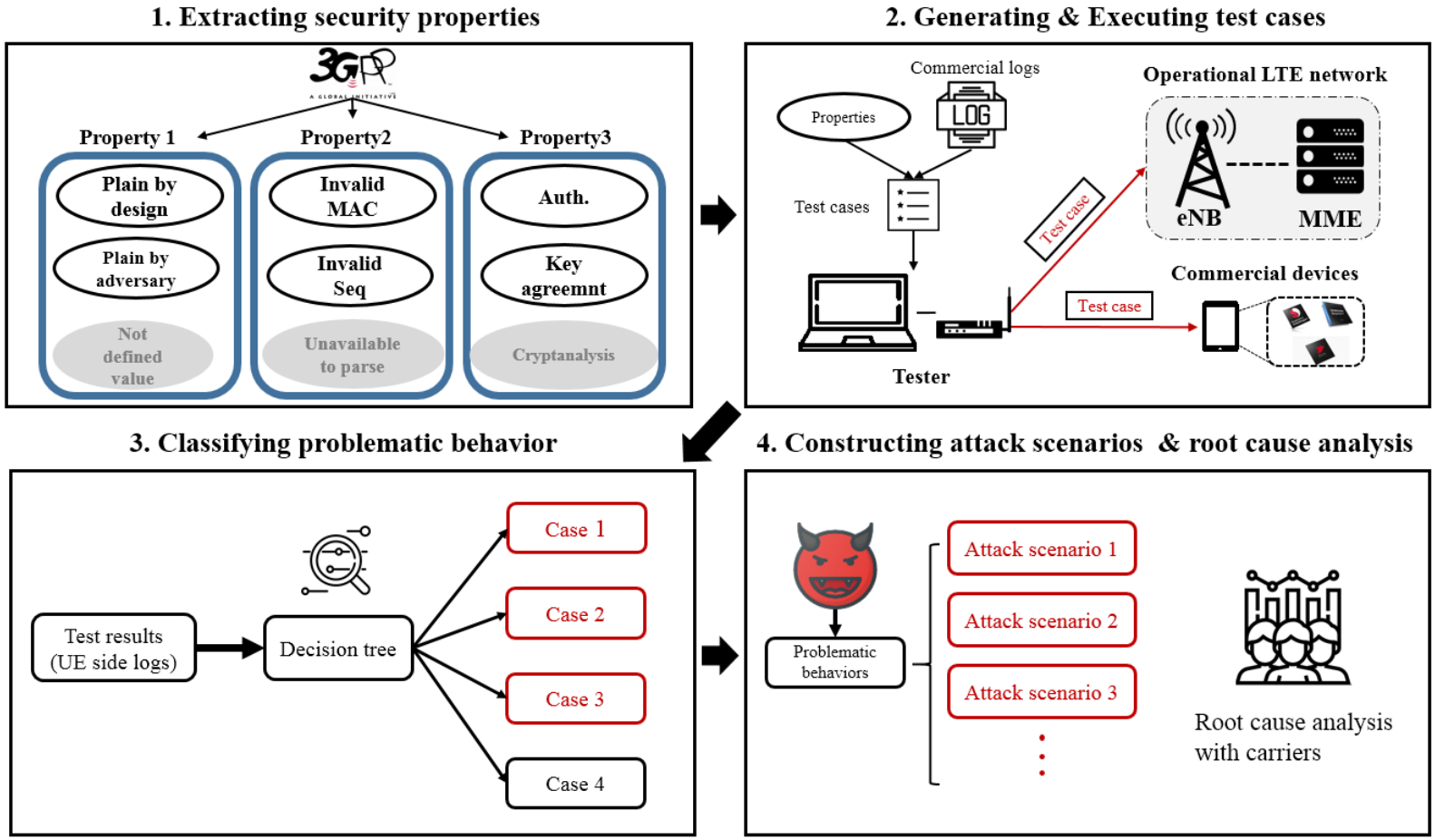
Approach

- To overcome the challenges,
  1. **Utilized open source LTE stack called srsLTE**
     - Provides fully controllable baseband and core network functions
     - Transmit LTE signals using SDR (Software Defined Radio) device



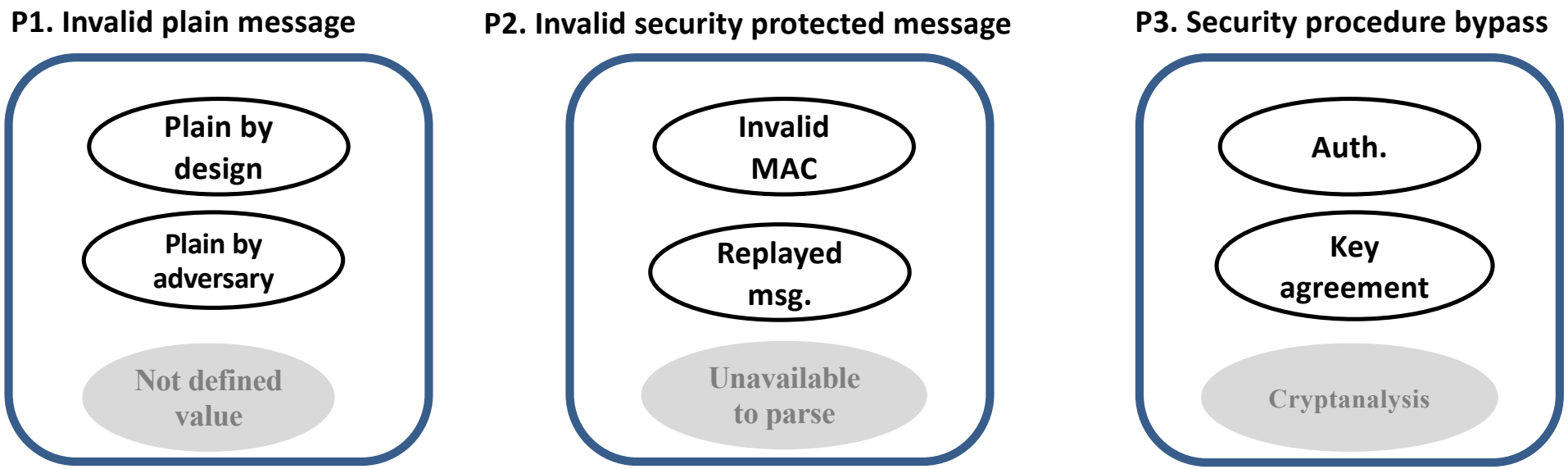
  2. **Detect problematic behaviors by only monitoring the UE side logs**
     - LTEFuzz (details in the next slide)
  3. **Cooperate with the carriers**
     - Confirmation of the results
     - Detailed root cause analysis

Overview of our approach



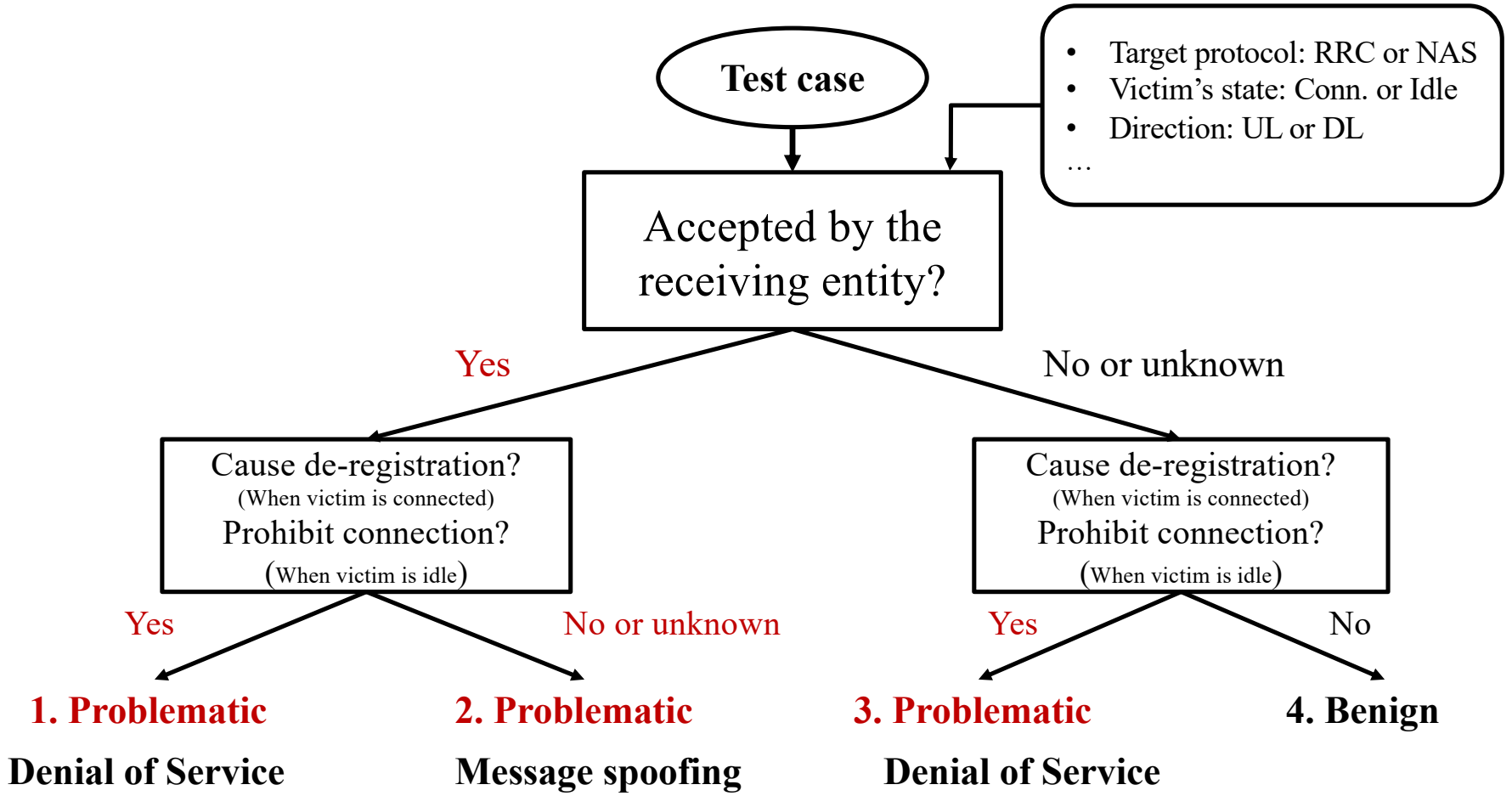
Generating test cases

- **Target protocol**: *RRC and NAS*



- For P1 and P2
  - Mandatory fields are mutated from the collected commercial logs

Classifying the problematic behavior



Attacks exploiting MME

- Result of dynamic testing against different MME types
  - Carrier 1: MME1, MME2, Carrier2: MME3 (MME1 & MME3: the same vendor)

Exploited NAS Messages	Implications		
	MME_1	MME_2	MME_3
Attach Request	DoS (**P**, **I**, **R**)	×	DoS (**P**, **I**, **R**)
TAU Request	DoS (**P**, **I**, **R**)	×	DoS (**I**), False location update (**R**)
Uplink NAS Transport	DoS (**P**, **I**), SMS phishing (**R**)	SMS phishing (**P**, **I**, **R**)	-
PDN Connectivity Request	DoS (**I**)	×	DoS, DosS (**R**)
PDN Disconnect Request	DoS (**I**), DosS (**R**)	×	DosS (**R**)
Detach Request	DoS (**P**, **R**)	DoS (**P**, **I**, **R**)	DoS (**P**, **I**, **R**)

DosS: Denial of selective Service, **P:** Plain, **I:** Invalid MAC, **R:** Replay

Test messages	Direction	Property 1-1	Property 2-1 (I)	Property 2-2 (R)	Property 3	Affected component
NAS						
Attach request (IMSI/GUTI)	UL	-	DoS	DoS	DoS	-	Core network (MME)
Detach request (UE originating detach)	UL	-	DoS [1]	DoS	DoS	-	Core network (MME)
Service request	UL	-	-	B	Spoofing	-	Core network (MME)
Tracking area update request	UL	-	DoS	DoS	FLU and DoS	-	Core network (MME)
Uplink NAS transport	UL	-	SMS phishing and DoS	SMS phishing and DoS	SMS replay	-	Core network (MME)
PDN connectivity request	UL	B	B	DoS	DoS	-	Core network (MME)
PDN disconnect request	UL	-	B	DoS	selective DoS	-	Core network (MME)
Attach reject	DL	DoS [2]	DoS [3]	-	-	-	Baseband
Authentication reject	DL	DoS [4]	-	-	-	-	Baseband
Detach request (UE terminated detach)	DL	-	DoS [4]	-	-	-	Baseband
EMM information	DL	-	Spoofing [5]	-		-	Baseband
GUTI reallocation command	DL	-	B	B	ID Spoofing	-	Baseband
Identity request	DL	Info. leak [6]	B	B	Info. leak	-	Baseband
Security mode command	DL	-	B	B	Location tracking [4]	-	Baseband
Service reject	DL	-	DoS [3]	-	-	-	Baseband
Tracking area update reject	DL	-	DoS [3]	-	-	-	Baseband
RRC						
RRCConnectionRequest	UL	DoS and con. spoofing	-	-	-	-	Core network (eNB)
RRCConnectionSetupComplete	UL	Con. spoofing	-	-	-	-	Core network (eNB)
MasterInformationBlock	DL	Spoofing	-	-	-	-	Baseband
Paging	DL	DoS [4] and Spoofing	-	-	-	-	Baseband
RRCConnectionReconfiguration	DL	-	MitM	DoS	B	-	Baseband
RRCConnectionReestablishment	DL	-	Con. spoofing	-	-	-	Baseband
RRCConnectionReestablishmentReject	DL		DoS			-	Baseband
RRCConnectionReject	DL	DoS	-	-	-	-	Baseband
RRCConnectionRelease	DL	DoS [2]	-	-	-	-	Baseband
RRCConnectionSetup	DL	Con. spoofing	-	-	-	-	Baseband
SecurityModeCommand	DL	-	B	B	B	MitM	Baseband
SystemInformationBlockType1	DL	Spoofing [4]	-	-	-	-	Baseband
SystemInformationBlockType 10/11	DL	Spoofing [4]	-	-	-	-	Baseband
SystemInformationBlockType12	DL	Spoofing [4]	-	-	-	-	Baseband
UECapabilityEnquiry	DL	Info. leak	-	Info. leak	Info. leak	-	Baseband

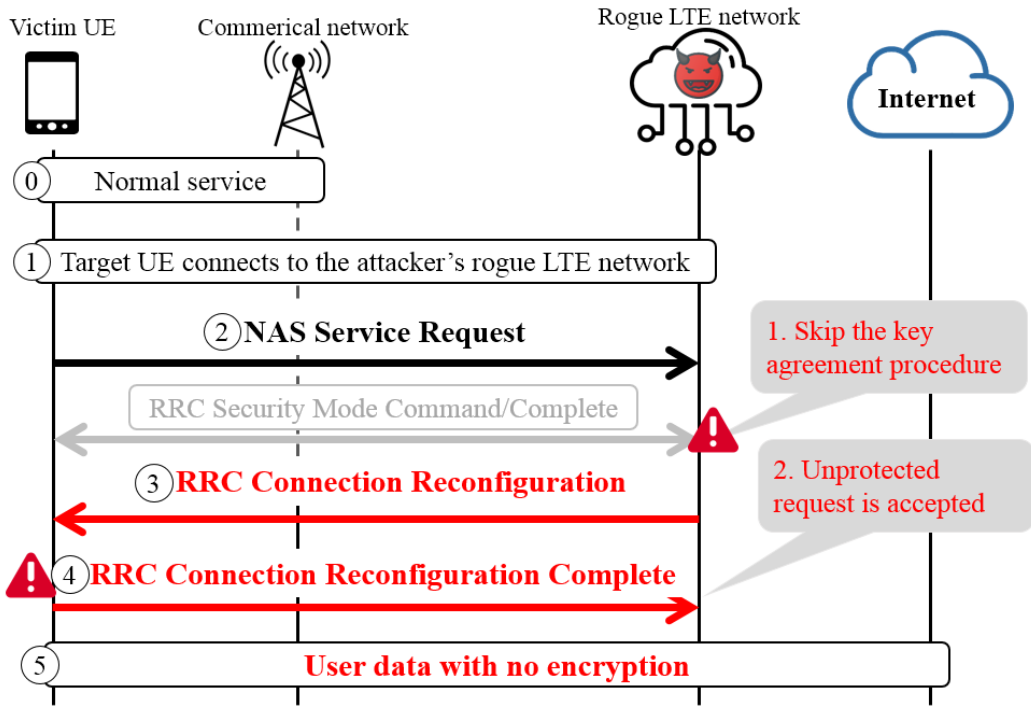
Specification issues

Vendor issues

AKA Bypass attack

- Exploits 2 vulnerabilities
  - **RRC SMC** can be bypassed
  - **RRC Connection Reconfiguration**

  is not security protected.
- Implications
  - Eavesdropping user data traffic
  - Steal user credentials by Phishing
  - Redirecting to fake online payment websites
- Validation
  - LG G2, Samsung Galaxy S4, S5
    - Basebasnd: Qualcomm chipsets



Conclusion

- We have implemented LTEFuzz
  - A semi-automated dynamic testing tool for both network equipments and devices
- LTEFuzz uncovered 51 vulnerabilities
  - New: 36, Previously known: 15
  - Specification problem: 16, Implementation & configuration problem: 35
  - two network devices from a single manufacturer (but in two carriers) has different vulnerabilities.
- Responsible disclosure
  - Carriers, Network vendors, Qualcomm, Huawei, Apple

Best Questions

- Kyungmook Kim
  - What are needed to test the LTE network?
- DAVY Guillaume
  - How can we make the FBS has higher signal strength than the commercial?
- Sumin Cho
  - How to reduce the errors that complex deployments make?

Interesting questions

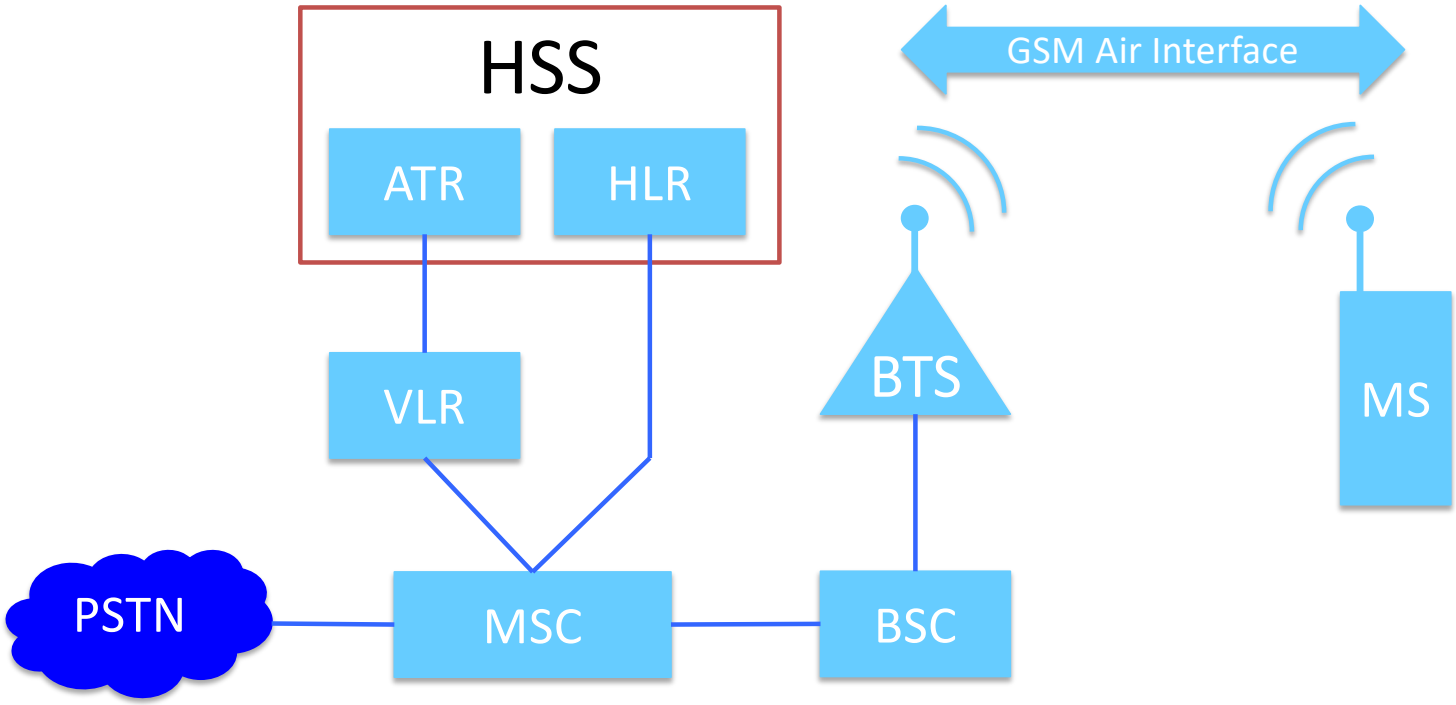
- Sangmin Woo
  - Test LTEFuzz in other carriers and vendors?
  - Successfully extended to stateful fuzzing?
- Kyungmook Kim
  - Commercial mobile devices capable of generating arbitrary messages?
  - How was the set of control plane log data from commercial networks collected worldwide?
  - A reason to simplify the decision tree?
  - Can unprotected control plane message be handled by software?
- DAVY Guillaume
  - Why do companies not apply these mandatory security procedures?
- Sumin Cho
  - What did you focus on when setting up the test cases?
- Junyoung Park
  - Would it be possible to target other parts of the LTE network?
  - Which technical challenges exist for stateful fuzzing?
- Hyung Chan Kim, WonYoung Jung
  - Testing in 5G?

Location Tracking

Location Privacy Leaks on GSM

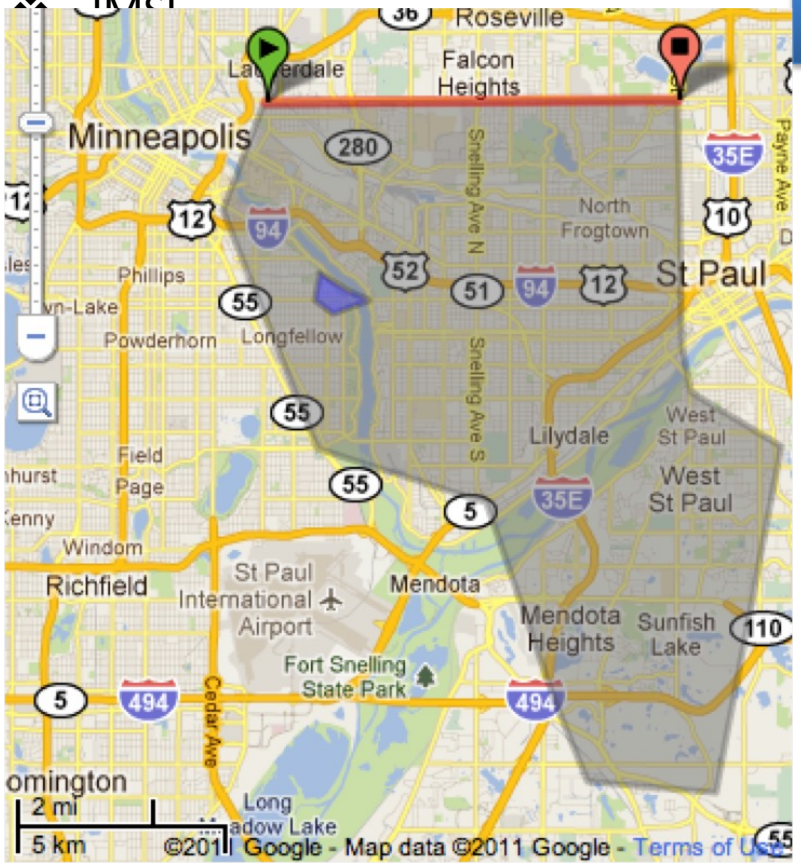
- We have the victim's mobile phone number
- Can we detect if the victim is in/out of an area of interest?
  - Granularity? 100 km^2? 1km^2? Next door?
- No collaboration from service provider
  - i.e. How much information leaks from the HLR over broadcast messages?
- Attacks by passively listening
  - Paging channel
  - Random access channel

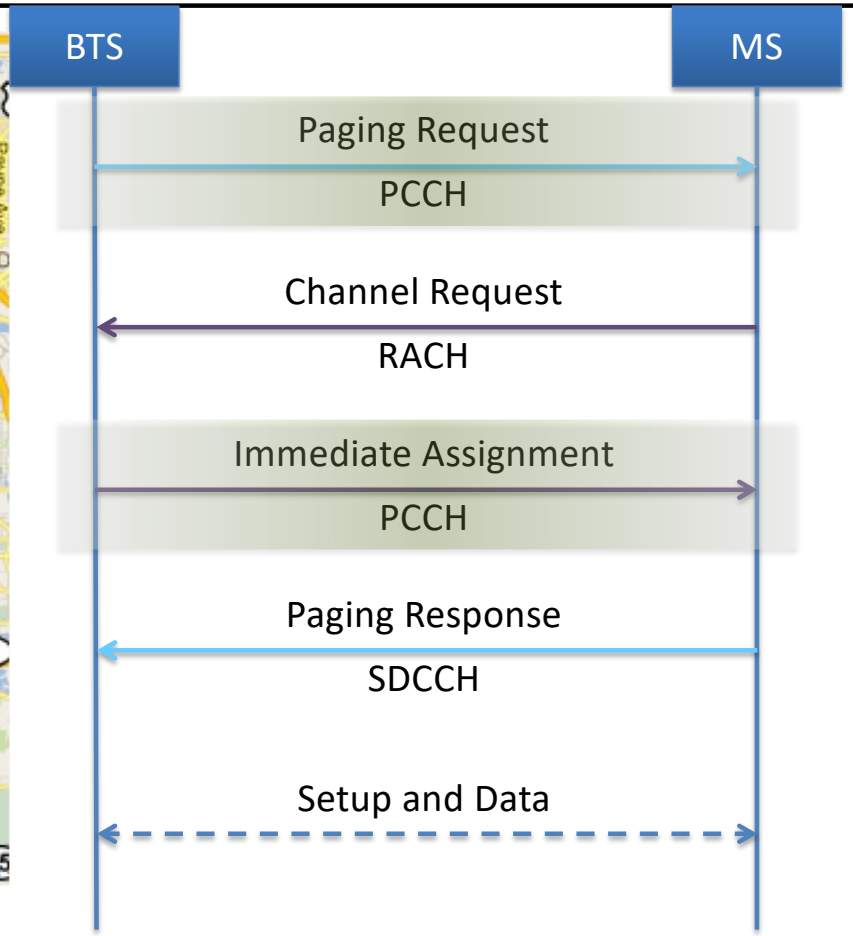
Cellular Network



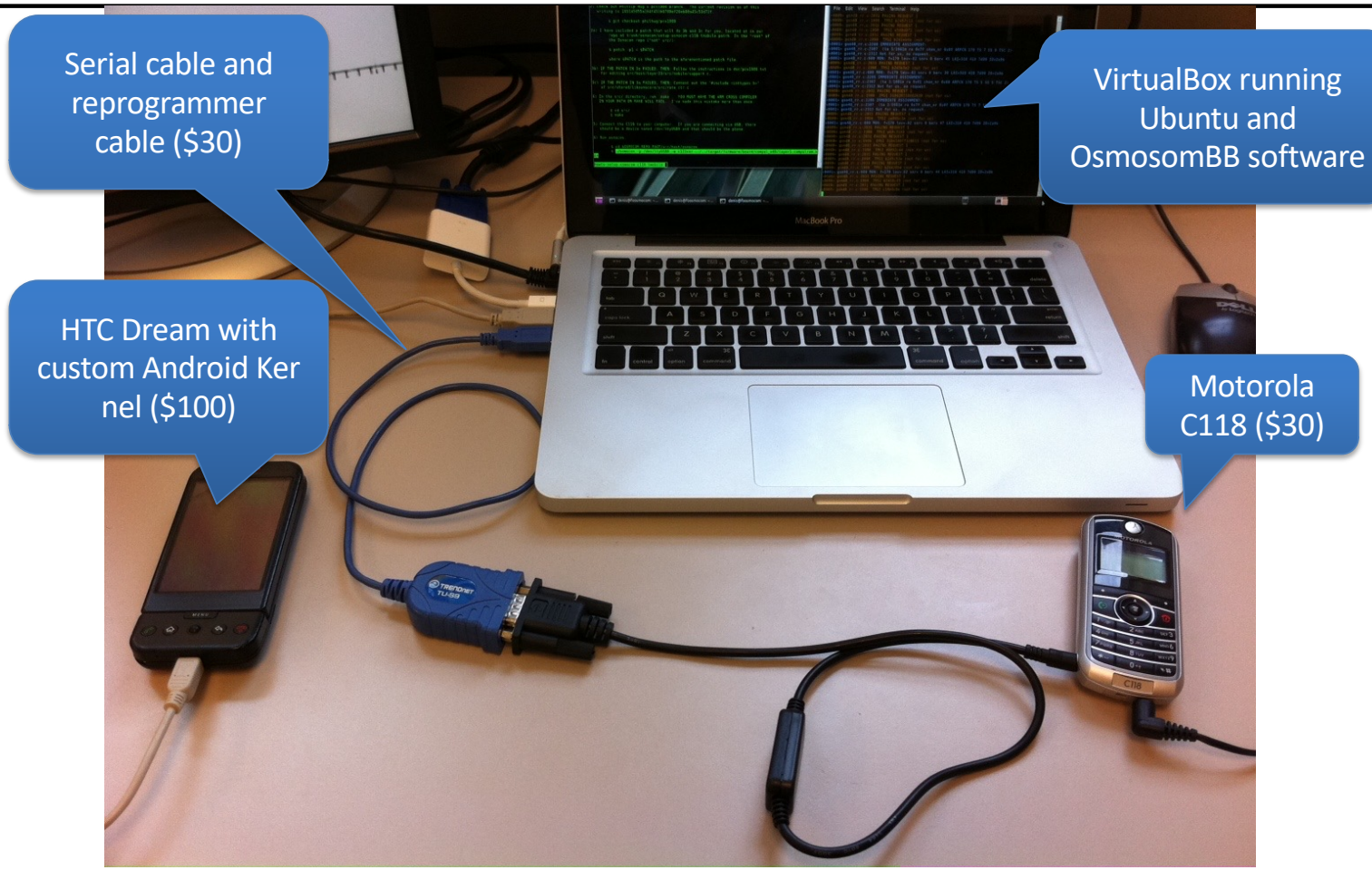
Location Leaks on Cellular Network

- IMSI

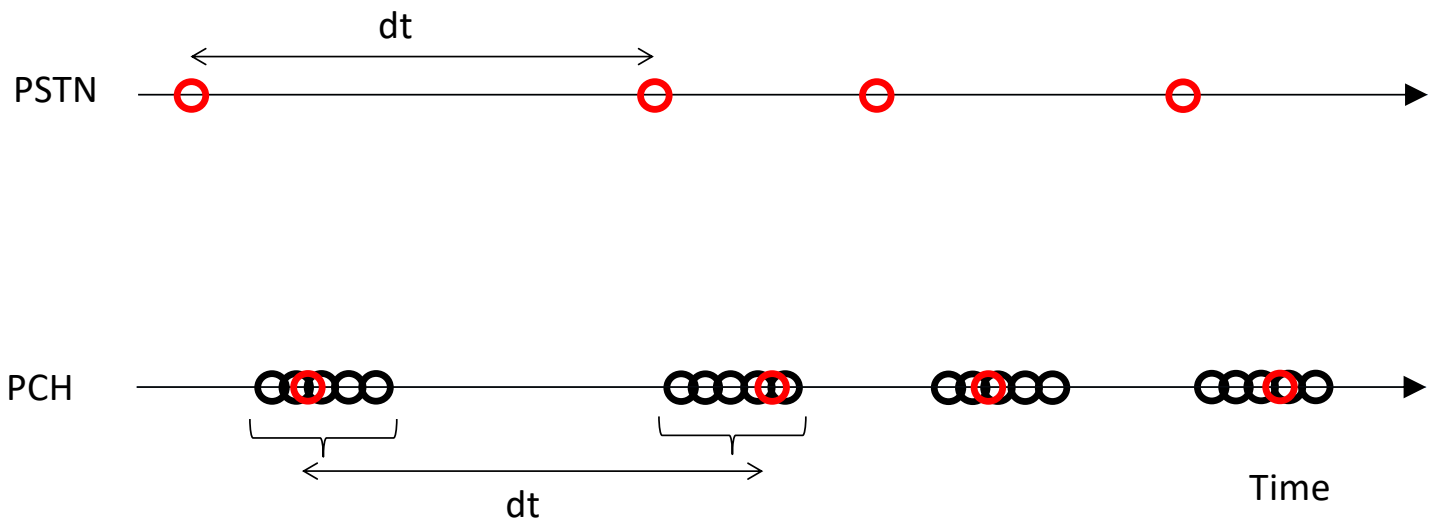




Platform

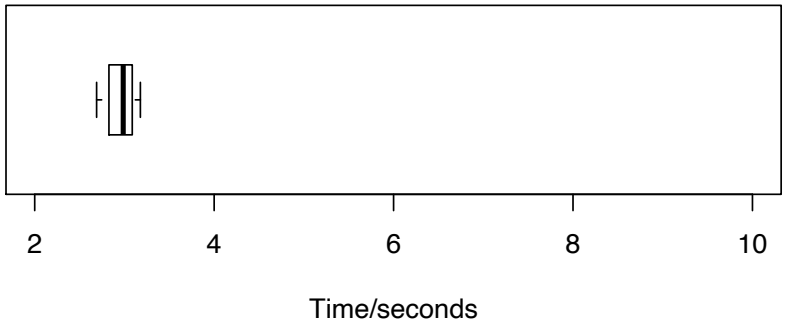

Serial cable and reprogrammer cable ($30)
VirtualBox running Ubuntu and OsmosomBB software
HTC Dream with custom Android Ker nel ($100)
Motorola C118 ($30)

Phone number-TMSI mapping

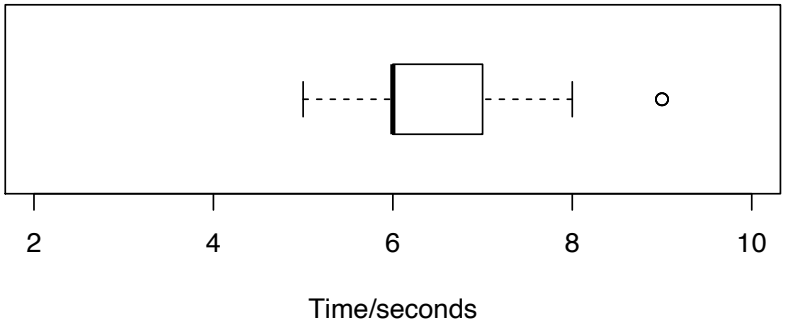


Silent Paging

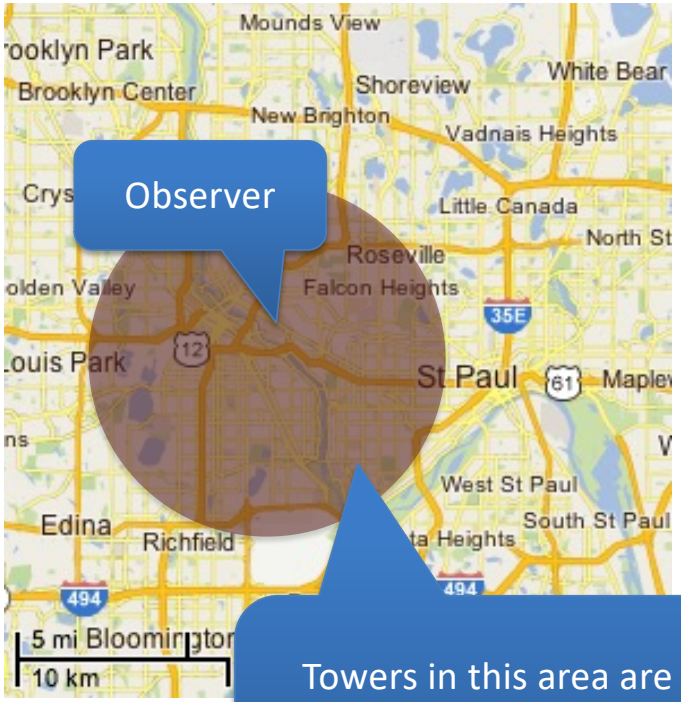
- Delay between the call initiation and the paging request: 3 sec



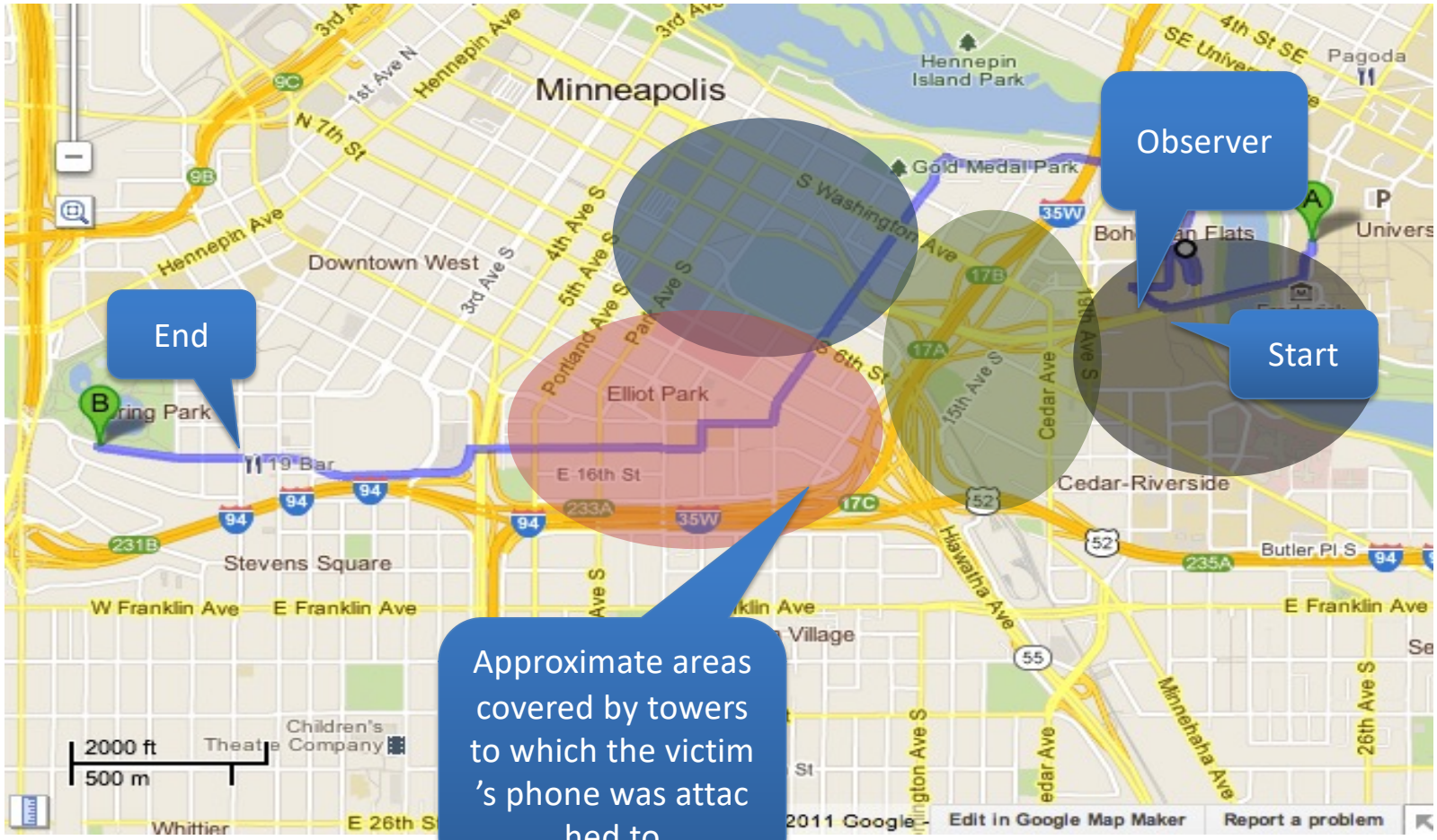
- Median delay between call initiation and ring: 6 sec



Coverage area with 1 antenna



Following a walking person



Identifiers in Cellular Networks

- Permanent/Unique identifier
  - IMSI (International Mobile Subscriber Identity)
    - Provisioned in the SIM card
- Temporary identifier
  - Used to **hide** subscriber
    - **TMSI** (Temporary Mobile Subscriber Identity)
      - Used in 2G/3G
    - **GUTI** (Globally Unique Temporary Identity)
      - Used in LTE

Worldwide Data Collection

Country	# of OP.	# of USIM	# of signalings	Country	# of OP.	# of USIM	# of signalings
U.S.A	3	22	763K	U.K.	1	1	41K
Austria	3	3	807K	Spain	2	2	51K
Belgium	3	3	372K	Netherlands	3	3	946K
Switzerland	3	3	559K	Japan	1	2	37K
Germany	4	19	841K	South Korea	3	14	1.7M
France	2	6	305K				

Data summary

Collection Period: **2014. 11. ~ 2017. 7.**

# of countries: **11** # of operators: **28** # of USIMs: **78** # of voice calls: **58K** # of signalings: **6.4M**

※ OP: operator, USIM: Universal Subscriber Identity Module, Signaling: control plane message

Same vs. Fingerprintable IDs

NDSS'12, '16: Same ID → Location Tracking!!

This work: ID Fingerprinting → Location Tracking!!

Fixed Bytes in *GUTI Reallocation*

- 19 operators have fixed bytes

Allocation Pattern	Operators
Assigning the same GUTI	BE-III, DE-II, FR-II, JP-I
Three bytes fixed	CH-II, DE-III, NL-I, NL-II
Two bytes fixed	BE-II, CH-I, CH-III, ES-I, FR-I, NL-III
One bytes fixed	AT-I, AT-II, AT-III, BE-I, DE-I

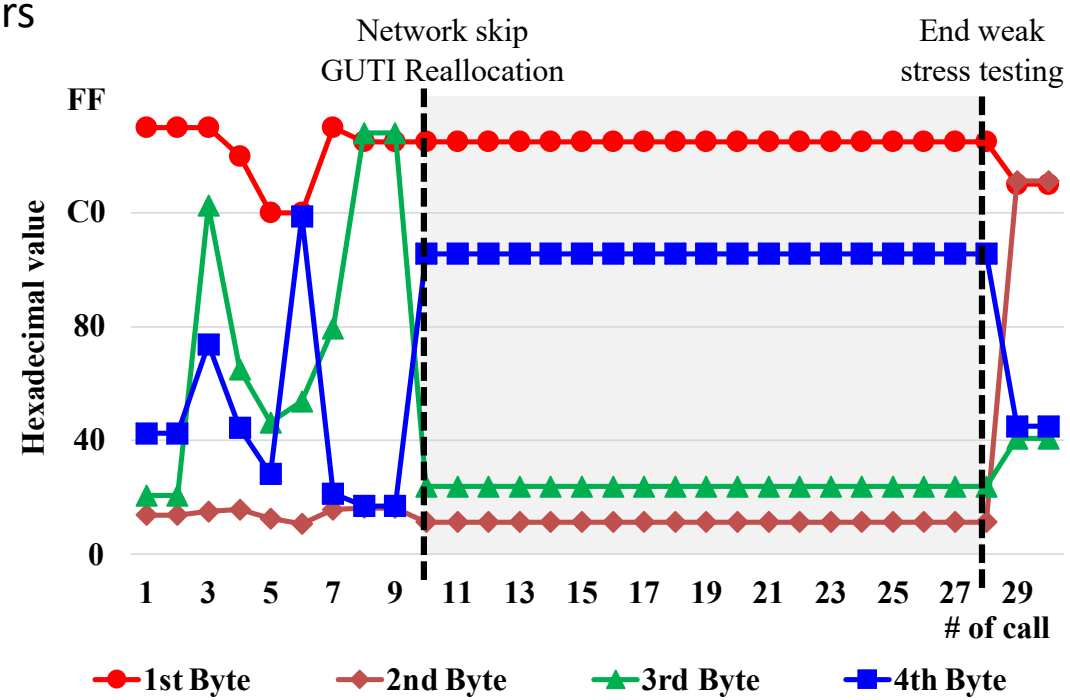
AT: Austria, BE: Belgium, CH: Switzerland, DE: Germany, ES: Spain, FR: France, JP: Japan, NL: Netherlands

Stress Testing Result

- Force the network to skip the *GUTI reallocation*
  - Perform experiments on US and Korean operators
    - Two US and two Korean operators

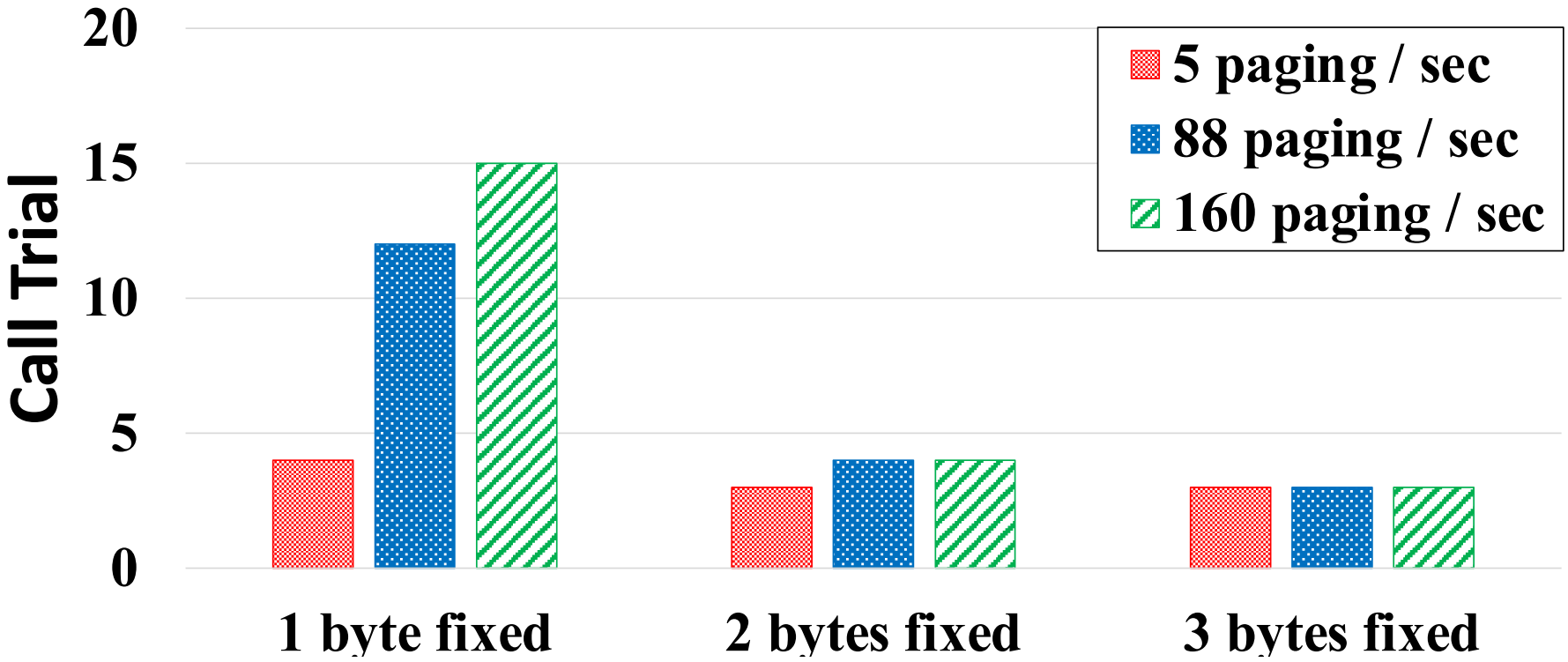
Operator	Weak Stress Testing	Hard Stress Testing
KR-I	O	O
KR-II	X	O
US-I	X	O
US-II	O	O

O: Reuse *GUTI*
X: No noticeable change



Success Rate of our Attack

- Required number of calls covering 99% success rate



Location Tracking with GUTI

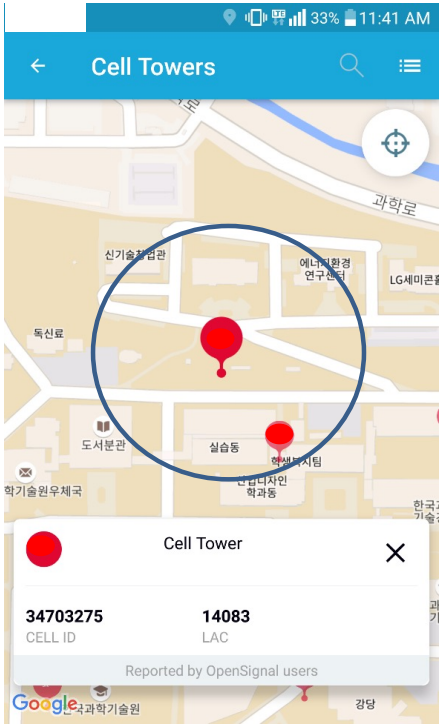
- Observation of broadcast channels after call invocation
  - Pattern matching (fixed bytes, assigning same GUTI)
  - Location tracking (Tracking Area, Cell)

EXTENDED_SERVICE_REQUEST:
SecurityHeaderType: 0
ServiceType: 1 (mobile terminating CS fallback or 1xCS fallback)
NASKeySetIdentifier:
TSC: 0 (native security context)
NASKeySetId: 2
MTMSI: Identity:
IdentityDigit:
01: 200 = 0xC8
02: 22 = 0x16
03: 66 = 0x42
04: 93 = 0x5D

(a) M-TMSI monitored by Device

```
6027 106.479617    LTE RRC PCCH    22 Paging (1 PagingRecords)
6028 106.489716    LTE RRC PCCH    22 Paging
6029 106.500101    LTE RRC PCCH    33 Paging (3 PagingRecords)
▸ LTE Radio Resource Control (RRC) protocol
  ▸ PCCH-Message
    ▸ message: c1 (0)
      ▸ c1: paging (0)
        ▸ paging
          ▸ pagingRecordList: 3 items
            ▸ Item 0
              ▸ PagingRecord
                ▸ ue-Identity: s-TMSI (0)
                  ▸ s-TMSI
                      mmec: 07 [bit length 8, 0000 0111 deci
                      m-TMSI: c816425d [bit length 32, 1100
```

(b) Paging Message in Broadcast Channel (USRP)



OpenSignal (at KAIST)

Best Questions

- Haein Lee
  - After leaking temporal ID, are there any attacks with the information
- Olav Lamberts
  - Any explicit standardization changes?
- Sujin Han
  - Why can’t we encrypt paging messaging packets?

Interesting Questions

- Haein Lee
  - the impact of this paper?
- Olav Lamberts
  - A time-delta based side-channel? ??
  - Detection of Silent calls?
  - VoIP takeover?
  - A constant internet connection affec ts the ability to track?
  - Any attack against Hash_DRBG?
- Sujin Han
  - How to compute the probability that a UE receive the same number of call s as the attacks?
  - How low-cost should the GUTI reallo cation algorithm be?
- Weonji Choi
  - 5G solved all privacy problems?
  - Can one enforce the standard compli ance?
  - SKT? KT? LG U+?
  - How big are the cells and TAs?
  - The emergency message determines the recipient based on the ‘cell’?
  - Receivers alerted for silent calls?
- TaiSic Yun
  - The attack range seems a little wide?
  - Any standard for GUTI reallocation?
- Min Woo Baek
  - Side-channel leaks for GUTI?

Lessons Learned from 4G/5G Security

- A lot of systematic problems from cellular industry

- Standard has a lot of security problem itself.
- Device vendors are making a lot of mistakes.
- Cellular ISPs are making a lot of mistakes.
- New generation deployment for every 10 years
  - New system deployment for every 3-4 years.
- ISPs don’t talk to each other. They don’t respond to public scrutiny.
  - Vendors don’t talk to each other.

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"