Cellular Security Research

- From Specification to Commercial Devices -

Yongdae Kim

SysSec@KAIST

joint work with many of my students and collaborators

Cellular Security Publications (Selected)

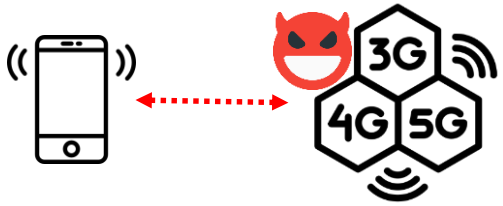
5 NDSS, 4 Usenix Sec, 1 CCS, 1 S&P. 1 Mobicom, 1 EuroS&P, 1 TMC, 1 WISEC

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. BASESPEC: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols, NDSS'21
10. DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices, Usenix Sec'22
11. Watching the Watchers: Practical Video Identification Attack in LTE Networks, Usenix Sec'22
12. Preventing SIM Box Fraud Using Device Fingerprinting, NDSS'23
13. LTESniffer: An Open-source LTE Downlink/Uplink Eavesdropper, ACM WISEC'23
14. BASECOMP: A Comparative Analysis for Integrity Protection in Cellular Baseband Software, Usenix Sec'23
15. Enabling Physical Localization of Uncooperative Cellular Devices, ACM Mobicom'24

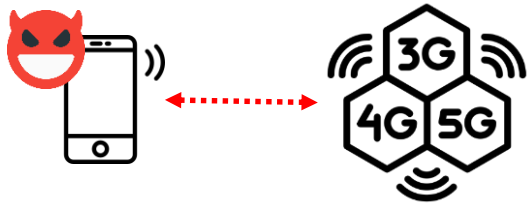
Cellular Security Publications

- New Vulnerabilities/Attacks
  - Location/Identity leaks [NDSS'12, NDSS'18]
  - Accounting bypass [NDSS'14, EuroS&P'17]
  - Signal overshadowing [Usenix Sec'19]
  - Video fingerprinting [Usenix Sec'22]
  - Up-/Down-link sniffer [WISEC'23]
  - Physical Location Tracking [Mobicom'24]
- Test/Measurement
  - VoLTE [CCS'15]
  - Performance bug [TMC'18, Hotmobile'19]
  - Up-/Down-link negative Fuzzer [S&P'19]
  - Stateful Down-link Fuzzer [Usenix Sec'22]
  - UE Fingerprinting [NDSS'23]
- Static Analysis
  - Baseband Static Analysis [NDSS'21, Usenix Sec'23]

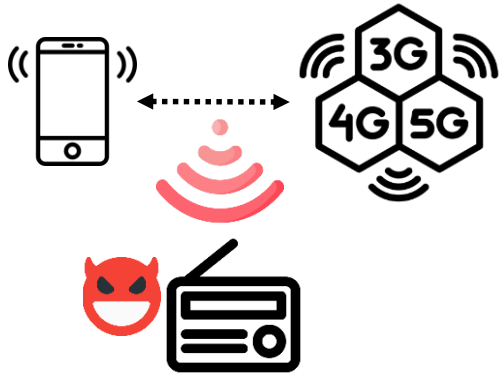
LTE Threat Model.



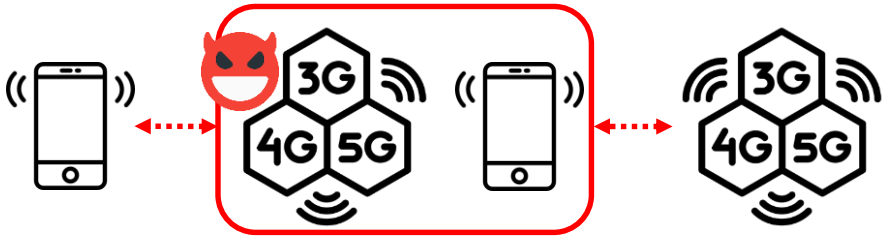
Fake base station
(srseNB/srsEPC)



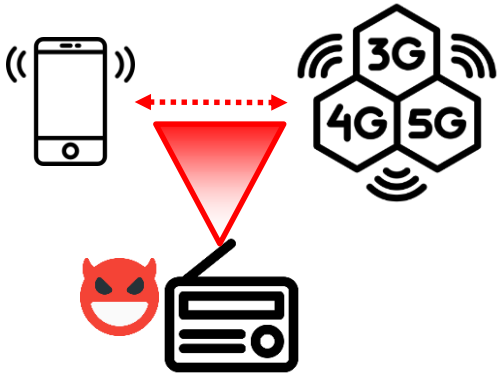
Fake UE
(srsUE)



Sniffer
(LTESniffer)



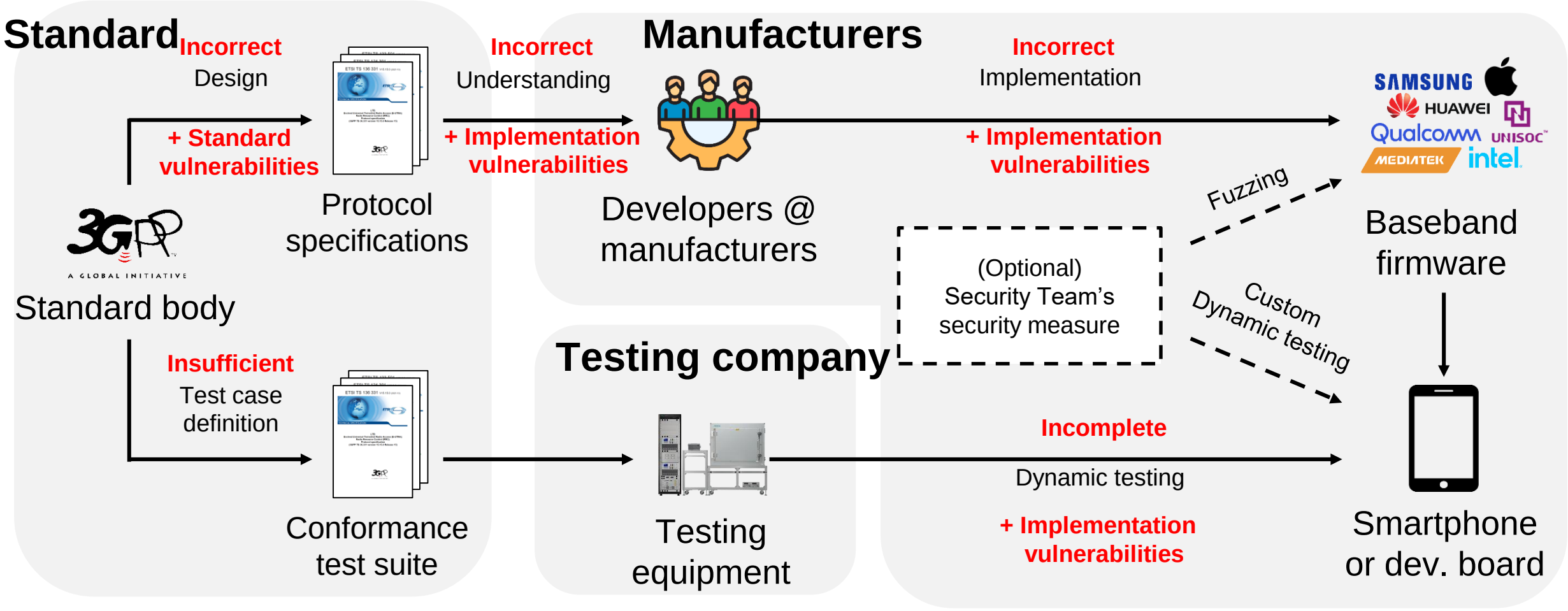
Man-in-the-Middle (MitM)
(srseNB/srsEPC + srsUE) ?



Overshadowing
(SigOver)

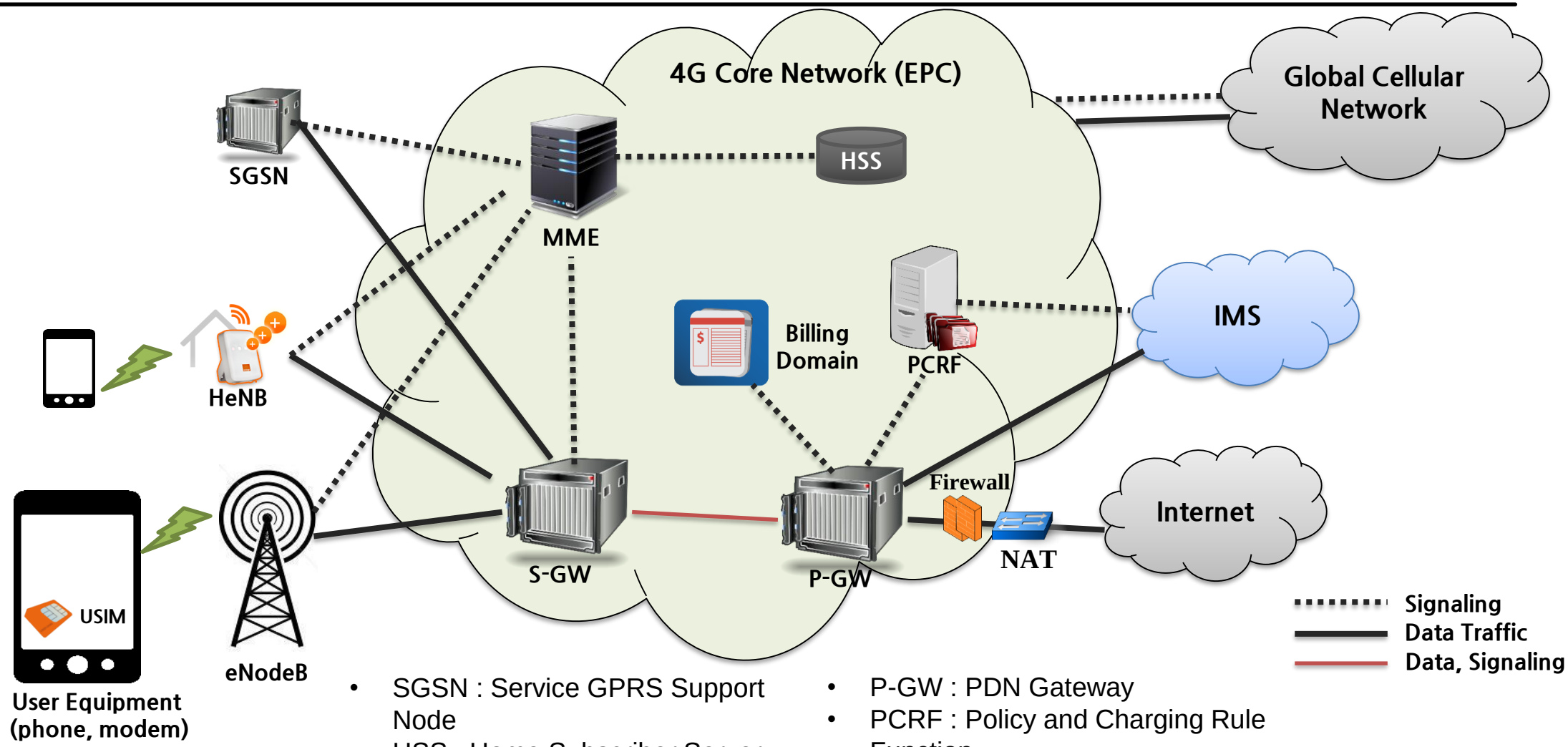
Security problems in baseband (UE)

- Secure specification **does not necessarily lead** to secure implementations



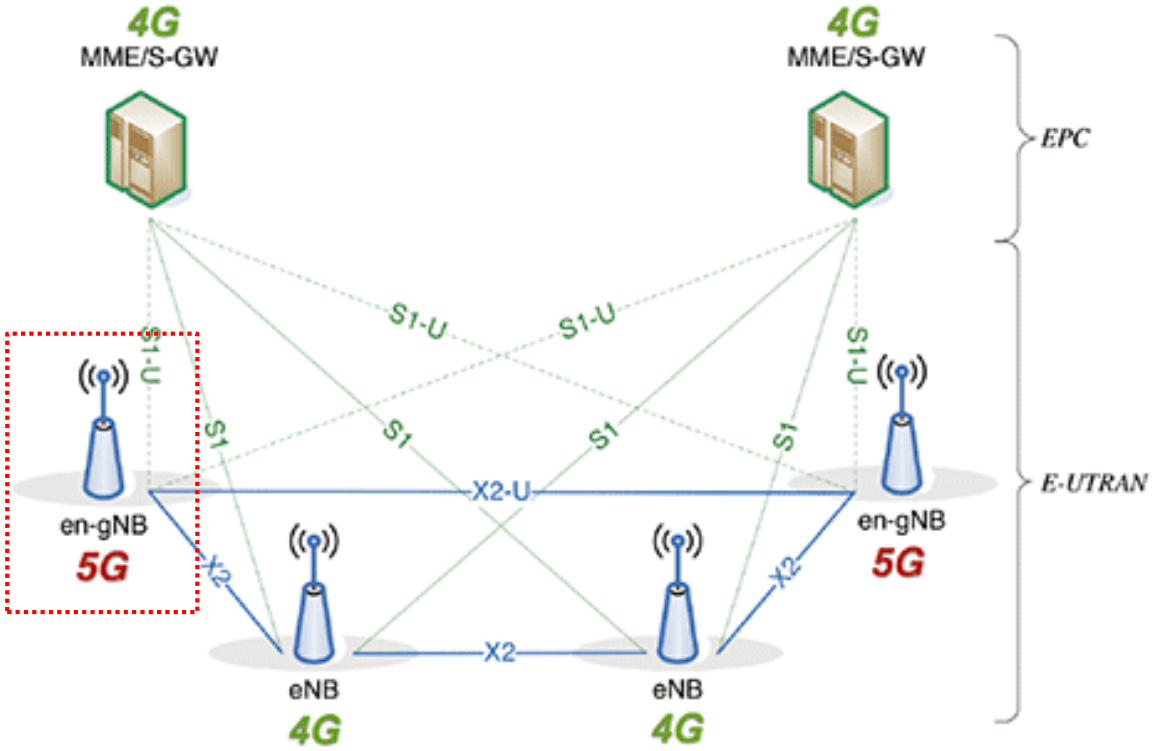
SYSSEC KAIST

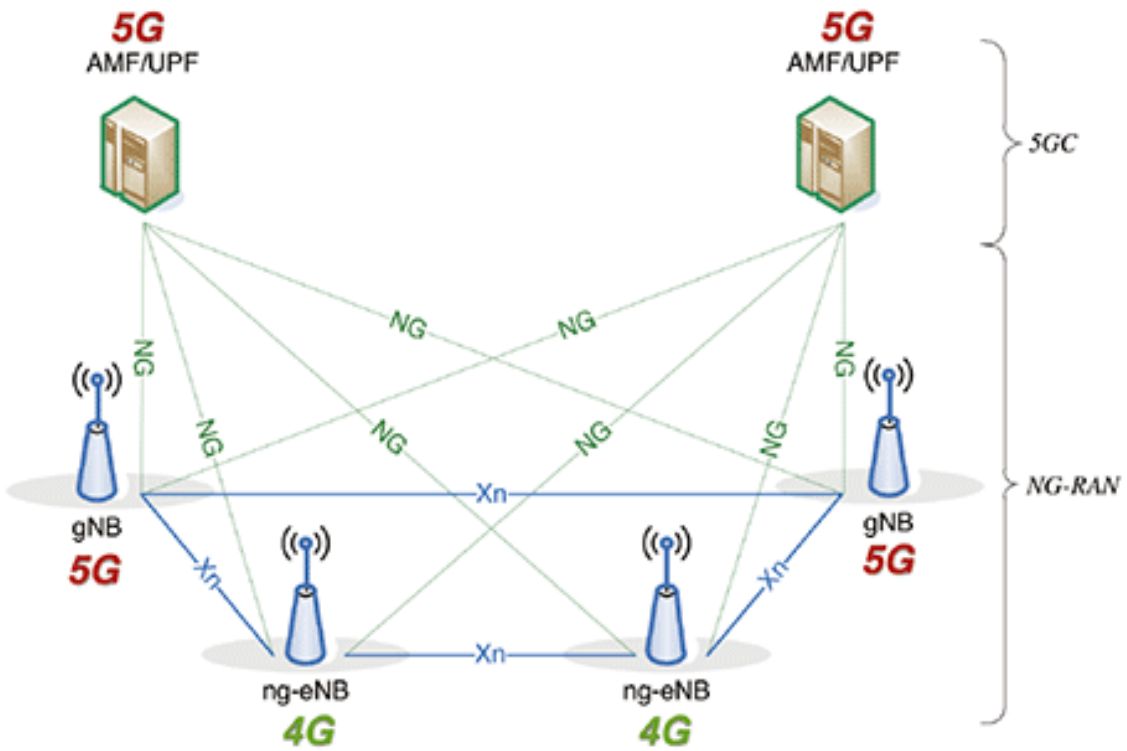
4G LTE Cellular Network Overview



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

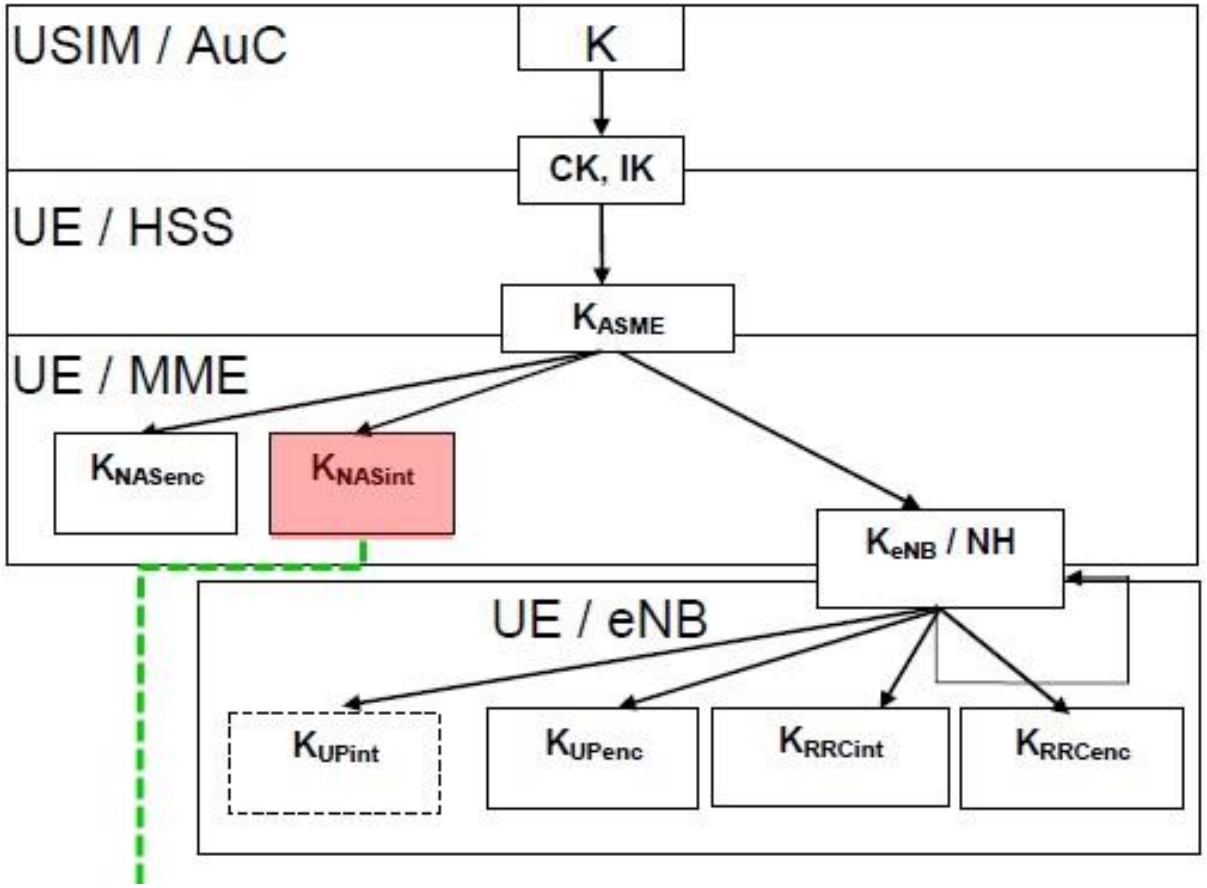
5G NSA vs. 5G SA

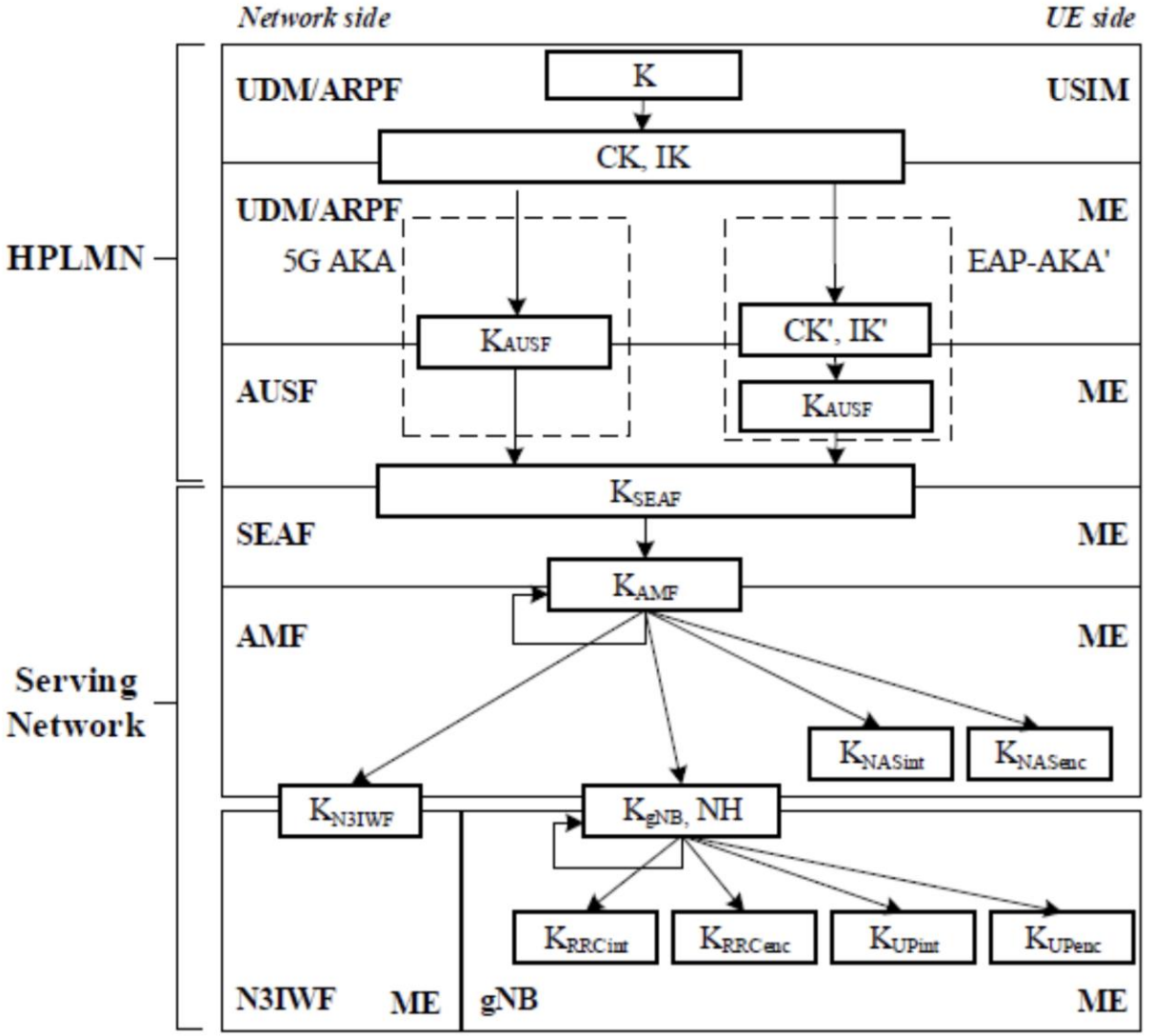




gNB (Next generation NodeB), eNB (Evolved Node B), MME (Mobility Management Entity), SPGW (Serving/Packet data network Gateway), HSS (Home Subscriber Server), IMS (IP Multimedia Subsystem)

Key Hierarchy

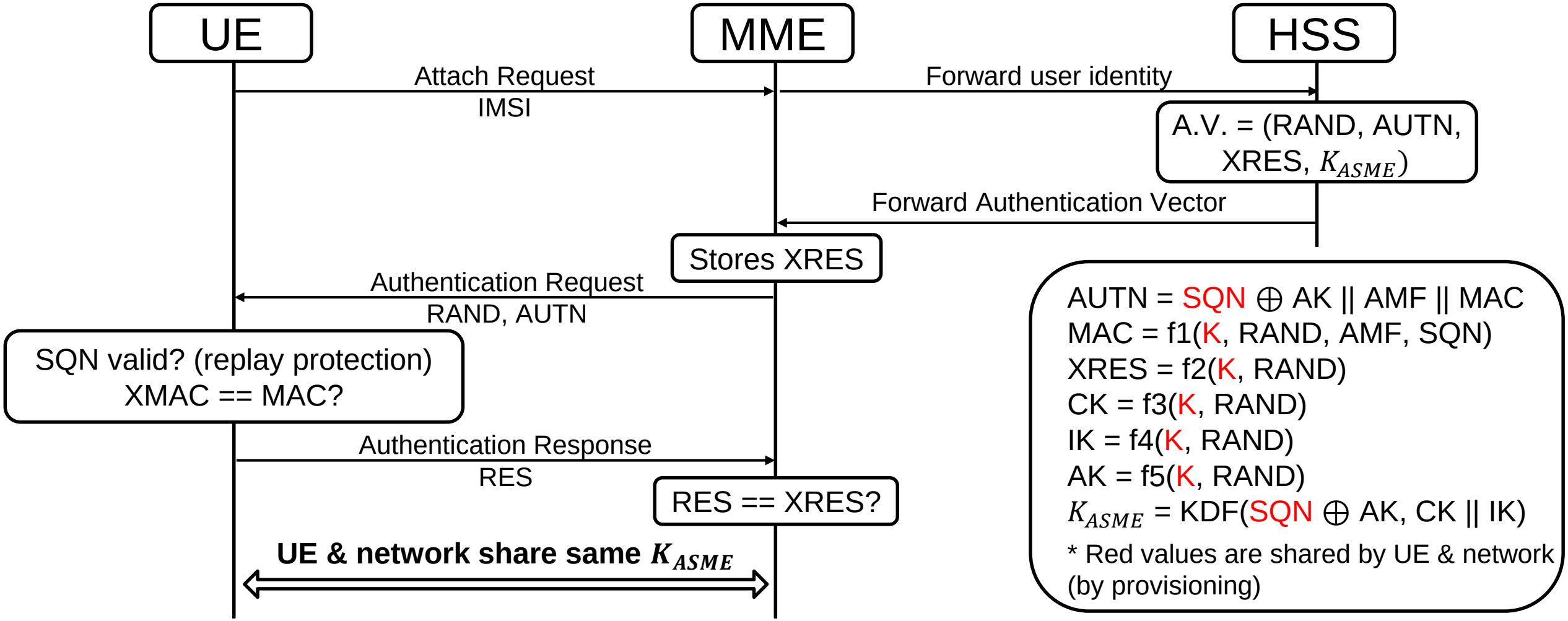




Source: ShareTechNote

SYSSEC KAIST

Authentication



Finally, session keys are derived based on K_{ASME}

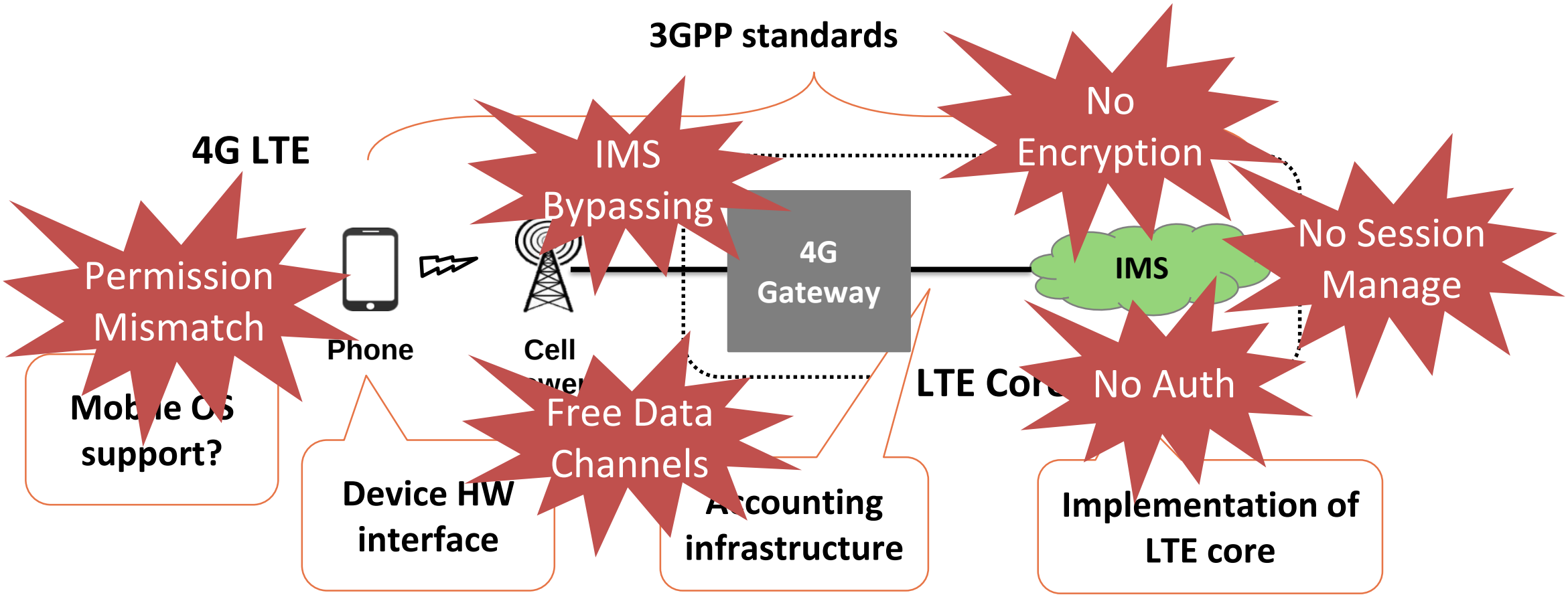
Testing

Why Implementation Vulnerabilities?

- New Generation (Technology) every 10 year
  - New Standards, Implementation, and Deployment ➔ New vulnerabilities
  - Generation Overlap, e.g. LTE CSFB, 5G NSA
- 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.
- Standards are not written in formal languages ➔ Hard for formal analysis
- Leave many implementation details for vendors ➔ Bugs

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

Discussion

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

CERT | Software Engineerin

Vulnerability N

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

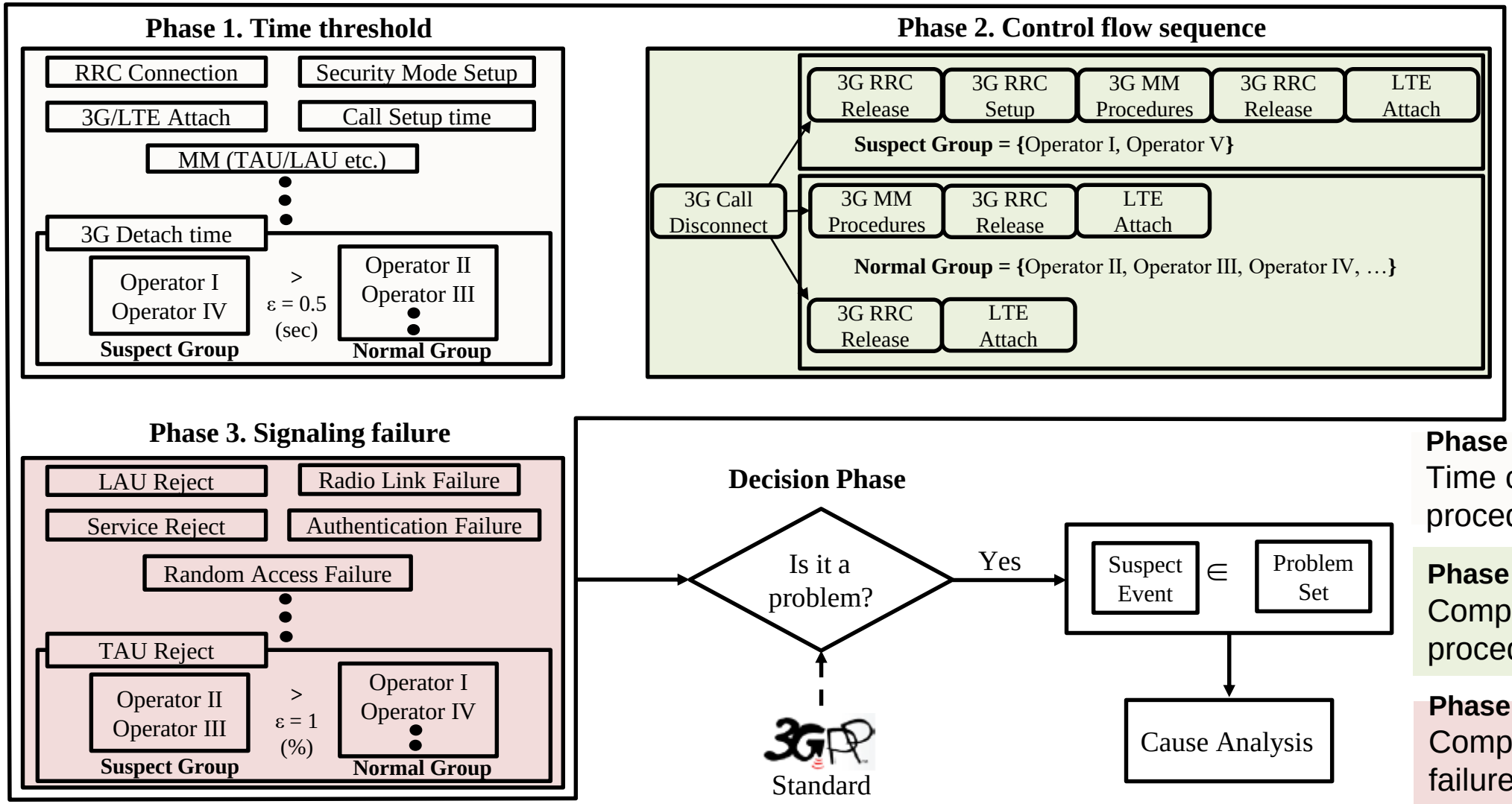
Worldwide Data Collection

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

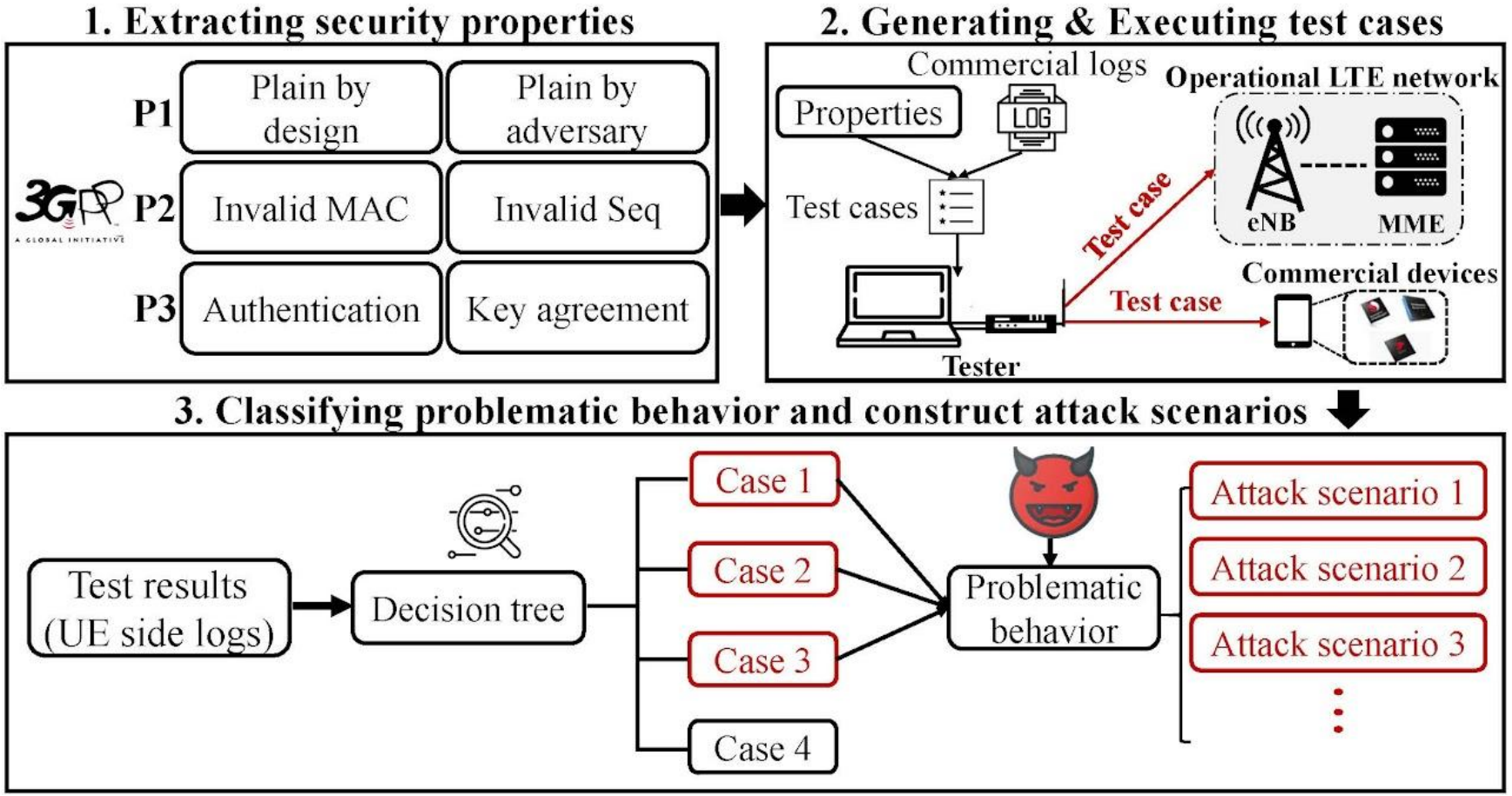
Phase 3
Comparison of signaling failure occurrence probability

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

LTEFuzz

- Stateless Pre-authentication Up-/Down-link Negative Fuzzer



Test messages	Direction	Property 1-1	Property 1-2 (P)	Property 2-1 (I)	Property 2-2 (R)	Property 3	Affected component
NAS							
Attach request (IMSI/GUTI)	UL	B	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

Index

Specification problem

MME vendors

Baseband vendors

Vuln. From different vendors

B: Benign

- : n/a

P: plain

I: Invalid MAC

R: Replay

Attacks exploiting MME

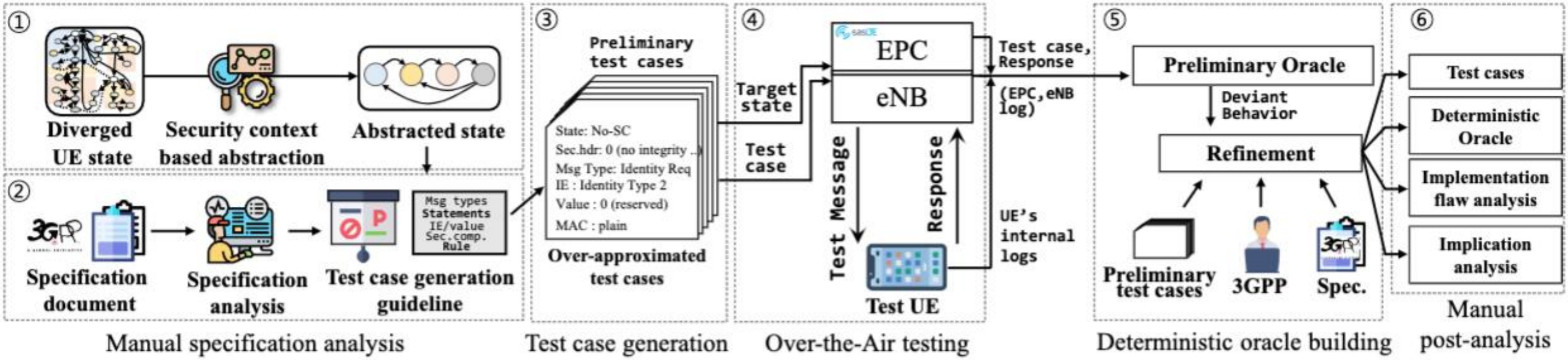
- Result of dynamic testing against different MME types
  - Carrier 1: MME1, MME2, Carrier2: MME3 (MME1 & MME3: the same vendor)

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

DoLTEst

- Stateful In-depth Downlink-only Negative Fuzzer



SYSSEC KAIST

DoLTEst

Protocol	Message	State					Implication	Studied?
		No-SC	**N-SC**	**NR-SC**	**REGI**	All		
RRC	RRCConnectionReconfiguration	I1(2)†, I1		M2		-	AKA bypass (I1), Location leak (I1,M2)	[36], [52]
	RRCConnectionRelease	-		M2		-	Redirection attack (M2)	[41]
	SecurityModeCommand	I2†,I3		-		-	Eavesdropping (I2,I3)	[48]
	UECapabilityEnquiry	-		M2		-	Information leak (M2)	[53]
	CounterCheck	M1		M2		-	Information leak (M2)	-
	UEInformationRequest	M1†		M2		-	Location leak (M1,M2)	[52]
	DLInformationTransfer	-		M2		-	-	-
NAS	Identity Request	I2,I3	-			S1,S2(2)	Information leakage (S1,S2,I2,I3)	[43]
	Security Mode Command	I3	-			-	Eavesdropping (I3)	[48]
	GUTI Reallocation Command	-				S1	Identity spoofing (S1), Denial-of-Service (S1)	[36]
	EMM Information	-	S1			-	NITZ spoofing (S1)	[45]
	Downlink NAS Transport	-			S1	-	SMS phishing (S1)	[43]
	Attach Reject	S2,I2	-			S1	Denial-of-Service (S1,S2,I2)	[52]
	Attach Accept	-				-	-	-

S3

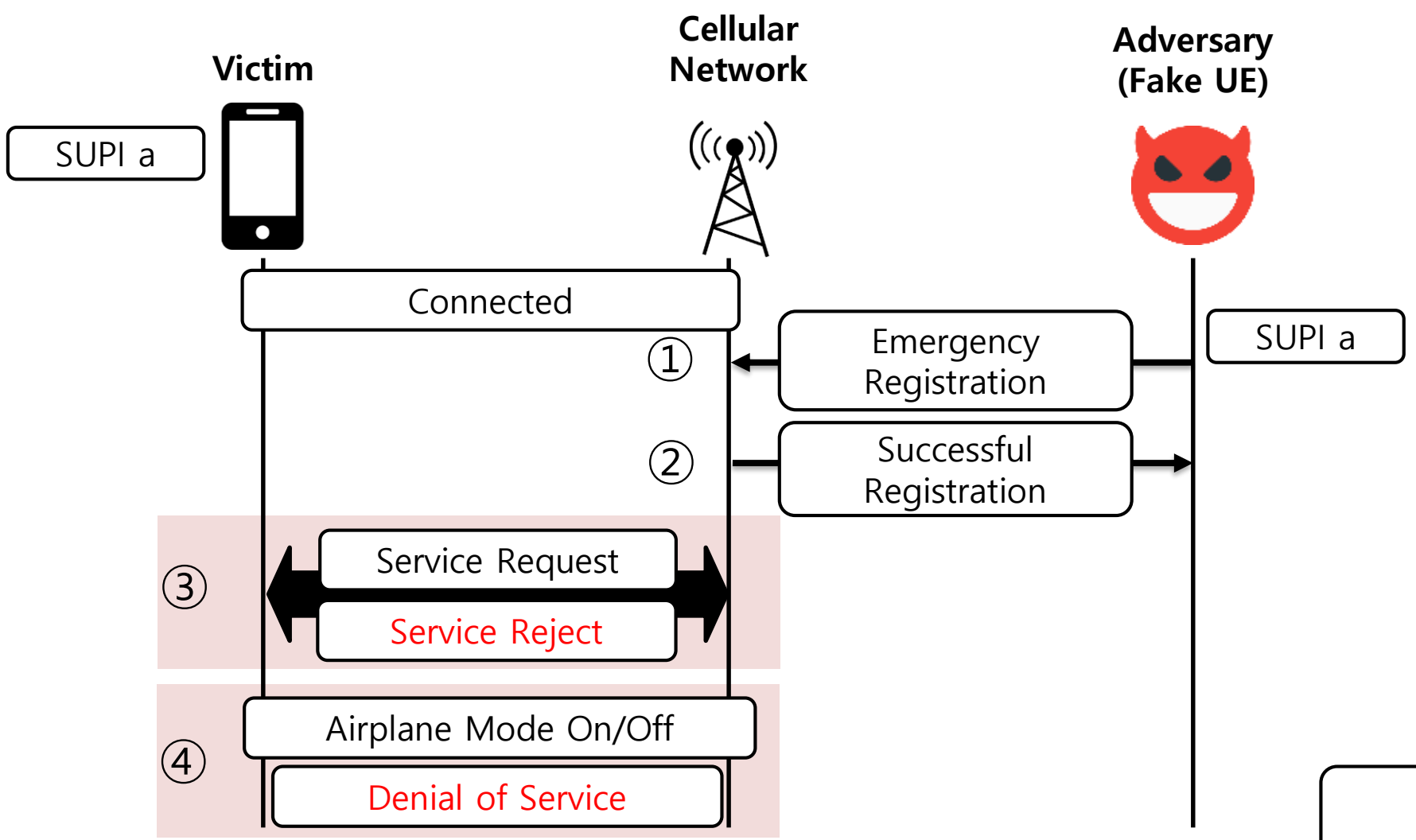
Detecting Undesired Context Transitions

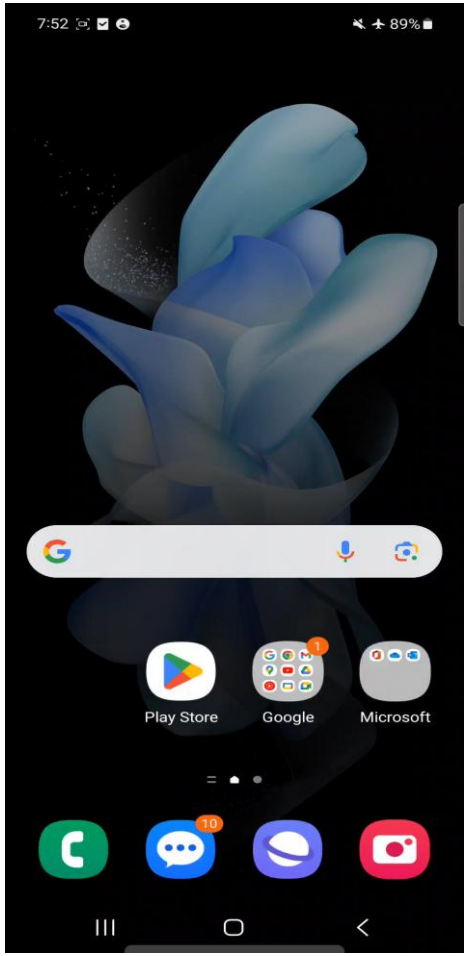
- "If authentication procedure is not successful the MME shall maintain, if any, the EMM-context and EPS security context unchanged" [1, Section 4.4.4.3]

- Attack model: Fake UE
  - Identity spoofing: Impersonates legitimate UE
  - Can send invalid signaling messages to the network
  - Unauthenticated message

[1] 3GPP TS 24.301 Release 18.7.0

Mid-term DoS





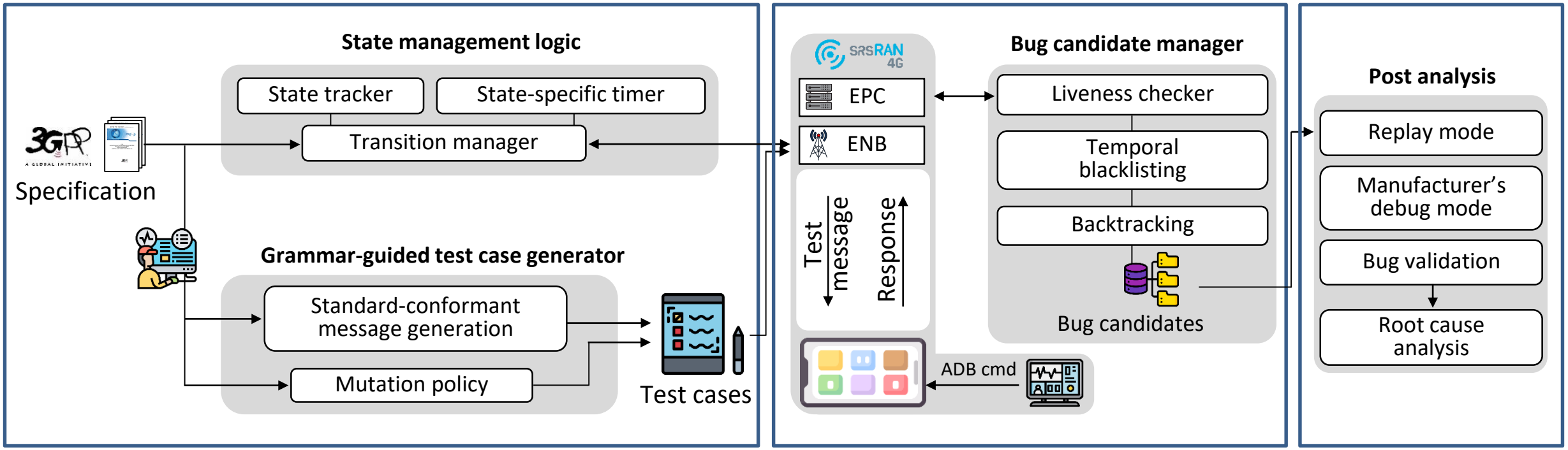
Permanent DoS Demo
(Z Flip + Amari Callbox LTE)

OTA Memory Fuzzer

① Manual specification analysis

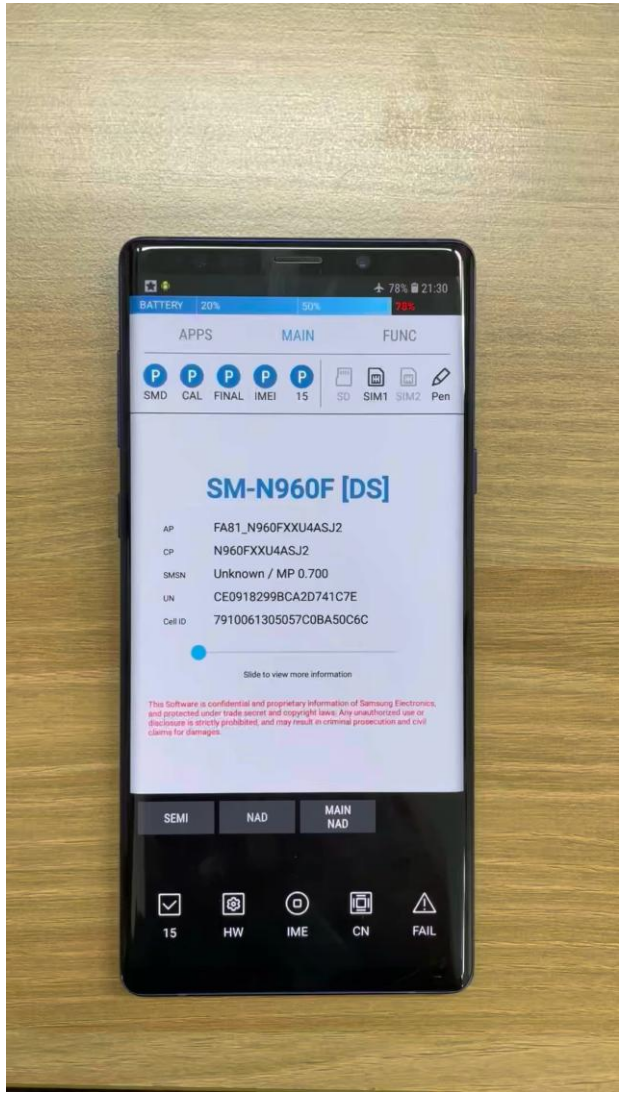
② Over-the-air testing

③ Manual post-analysis



SYSSEC KAIST

Downlink Baseband Memory Fuzzing



Conclusion (Testing)

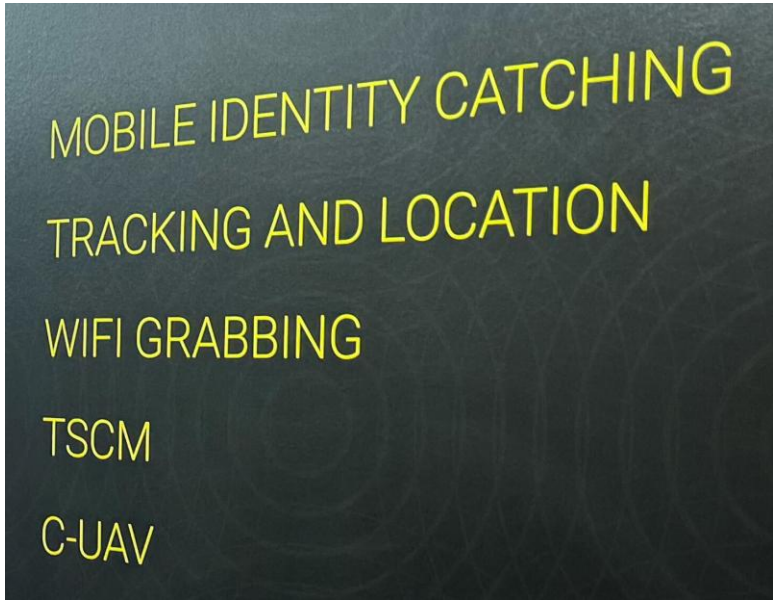
- 5G OTA Downlink/Uplink testing/analysis
  - State-aware Negative Testing for implementation vulnerabilities
  - State-aware Testing for Undesired Context Transitions
  - State-aware Downlink/Uplink Memory Fuzzer

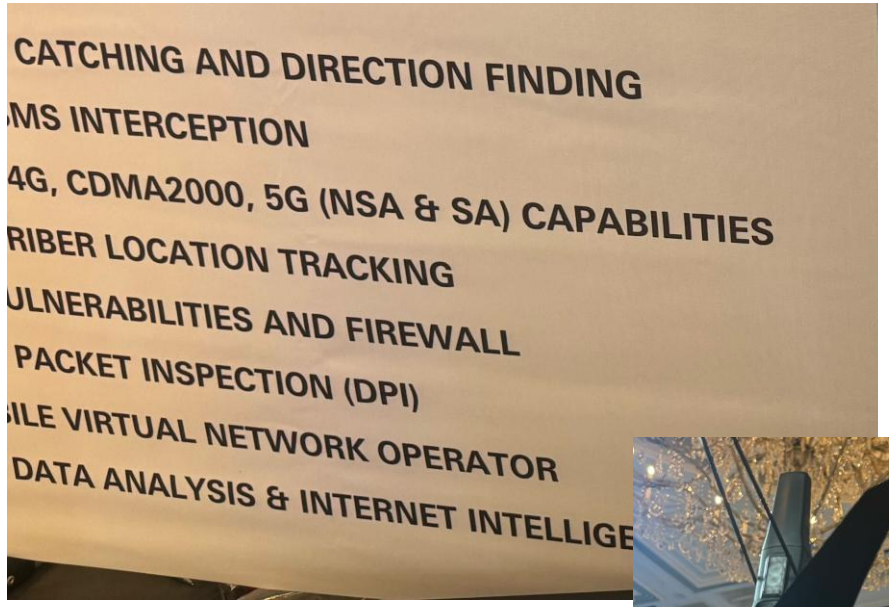
Attacks / Spec Vuln

Why Cellular Design Vulnerabilities Exist?

- New Generation (Technology) every 10 years
  - New Standards, Implementation, and Deployment ➔ New vulnerabilities
  - Backward compatibility: e.g. supporting 2G
- Government > Carrier > Device vendors > Customers ☺
  - Or Government > GSMA > 3GPP > Customers
  - To be standardized, unanimous support is needed.
  - Too expensive, need insecurities, not a big deal, …
- Complicated and huge standards
  - Multiple protocols co-work, but written in separate docs
- No visible attackers so far
- Papers presented, discussed in 3GPP, but forgotten later
  - What are patched/not patched? Why or why not?

Governments are exploiting it!





How can we secure 6G spec?

Cellular Metasploit

Open-source Attacking Tools Exploiting Known or New Vulnerabilities

Private 5G?

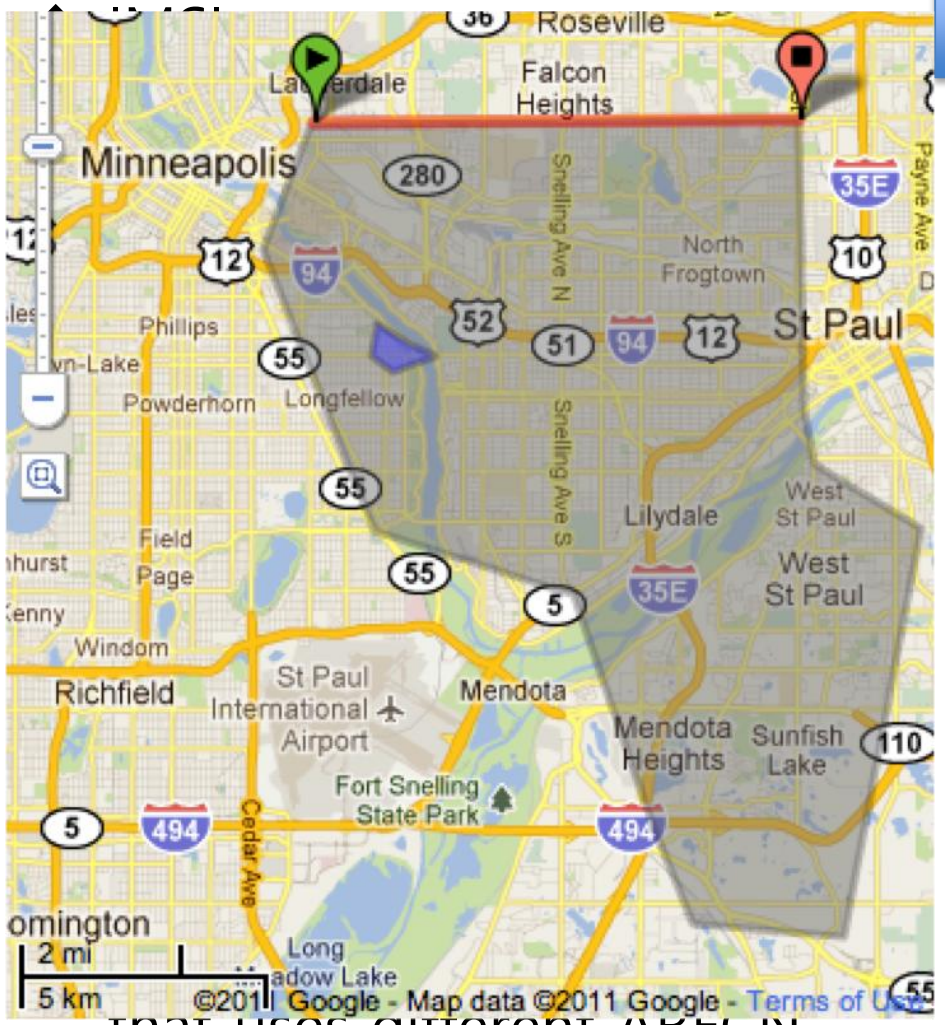
- Definition: a dedicated cellular network deployed for a specific organization or enterprise
- Why private 5G?
  - Dedicated infrastructure, Enhanced security, Customizable, Improved reliability, Lower latency, Higher capacity
- Applications
  - Railroad, Medical, Critical Infrastructure, Defense, …

Considering unpatched vulnerabilities and applications of private 5G,
can private 5G provide sufficient security?

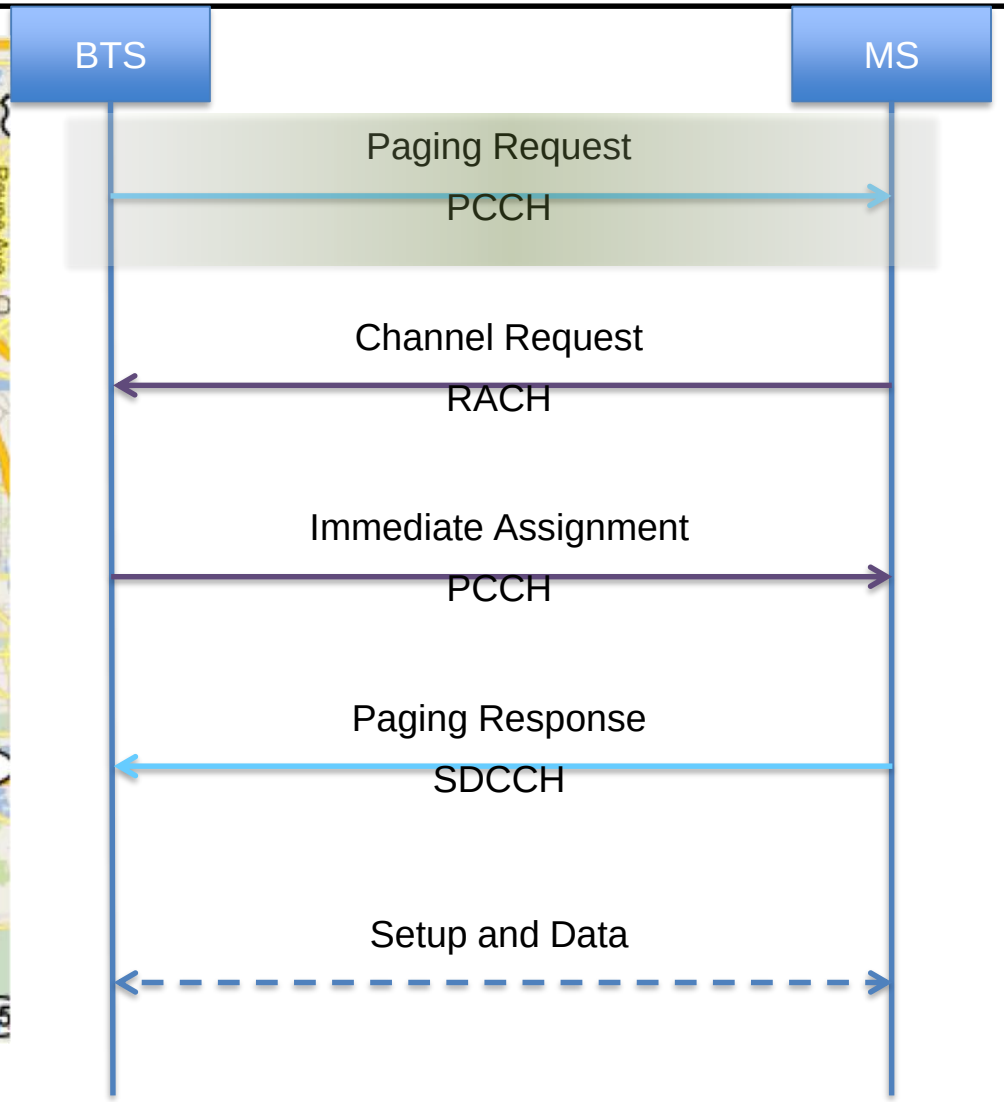
Location Privacy Leaks on GSM

- 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

Location Privacy Leaks on GSM



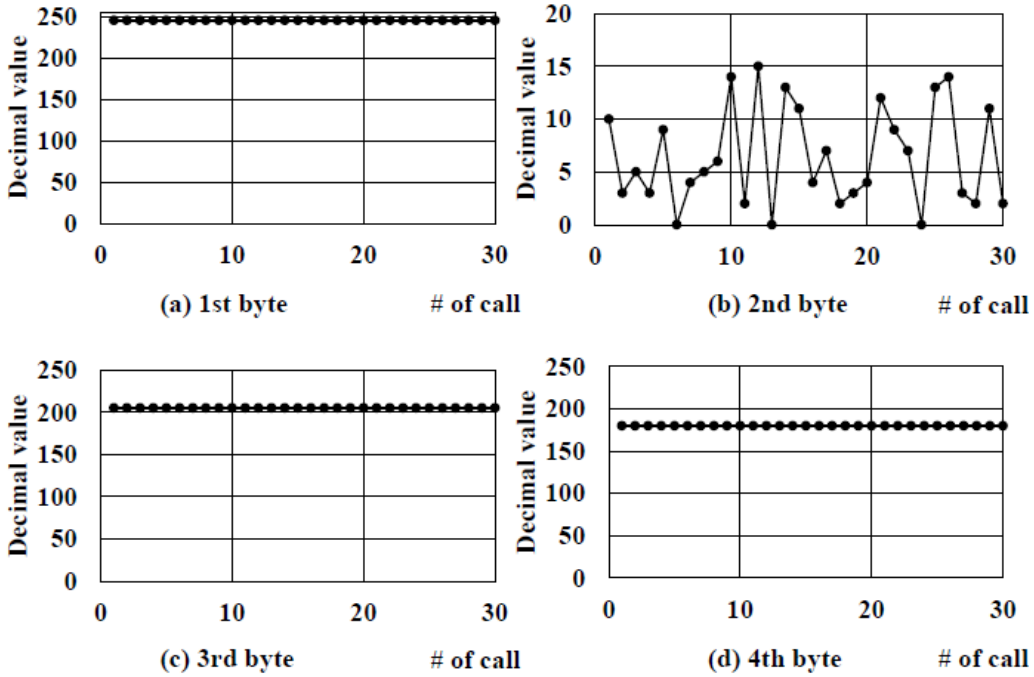
that uses different ARFCN



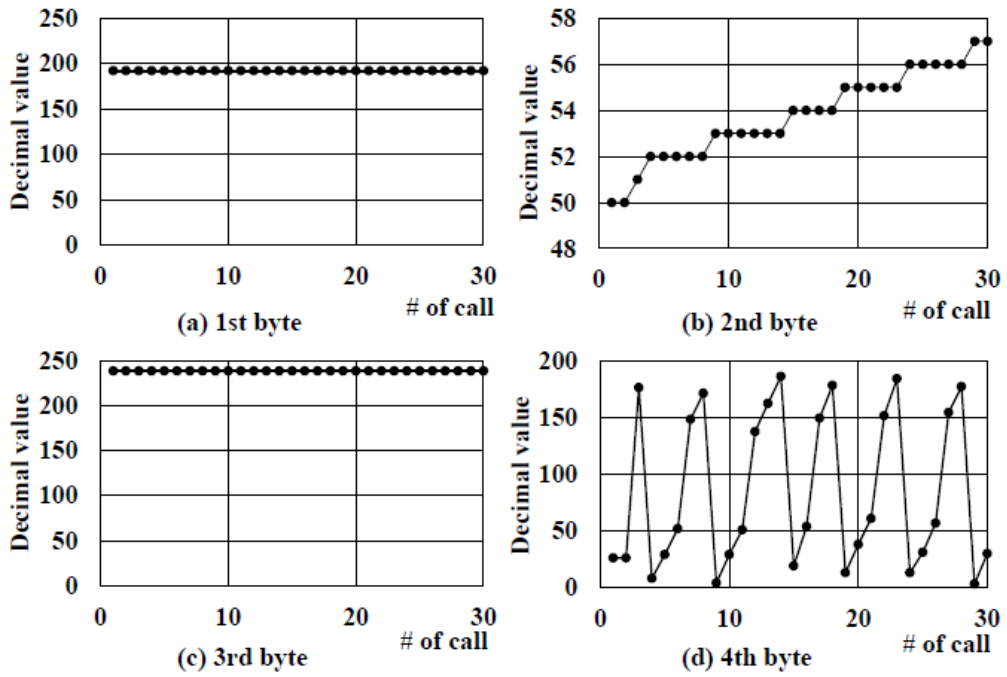
Vulnerabilities in ID Management

- Deployed ID Managements at current ISPs are still vulnerable!
  - They changes GUTI value, But GUTI Pattern in Reallocation shows pattern
    - Fixed bytes in *GUTI Reallocation*

Operator A in Netherlands



Operator B in Belgium



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

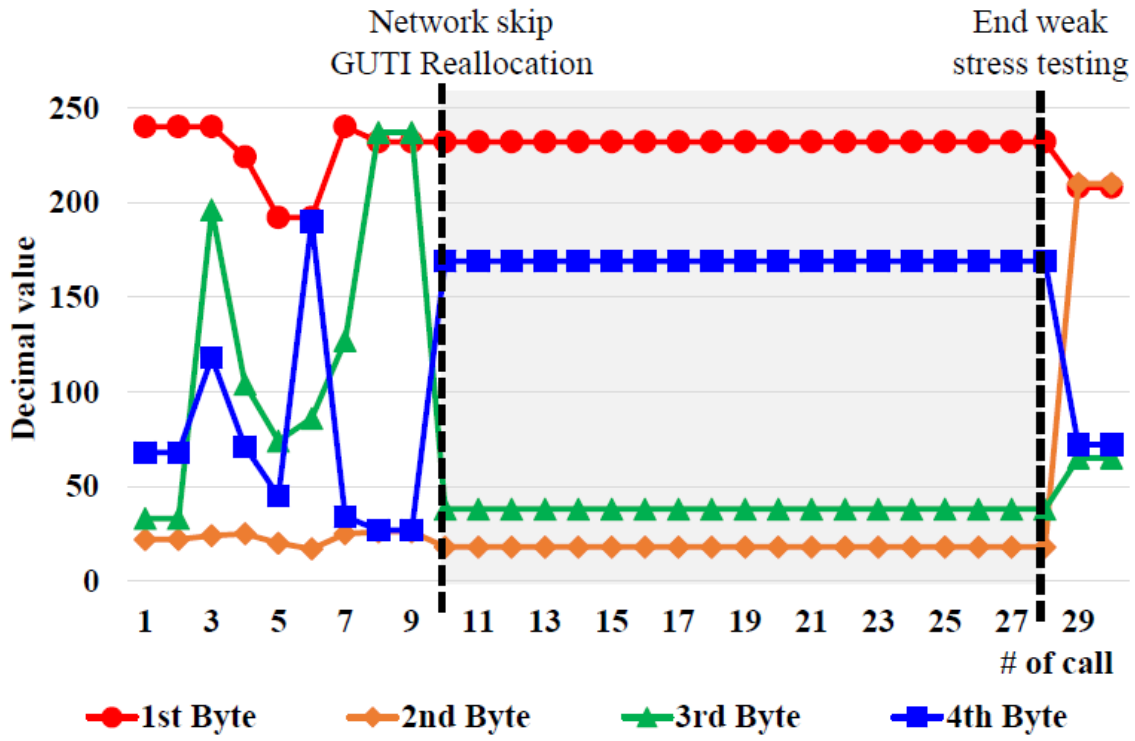
AT: Austria, BE: Belgium, CH: Switzerland, DE: Germany, ES: Spain, FR: France, JP: Japan, NL: Netherlands

Stress Testing

- 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

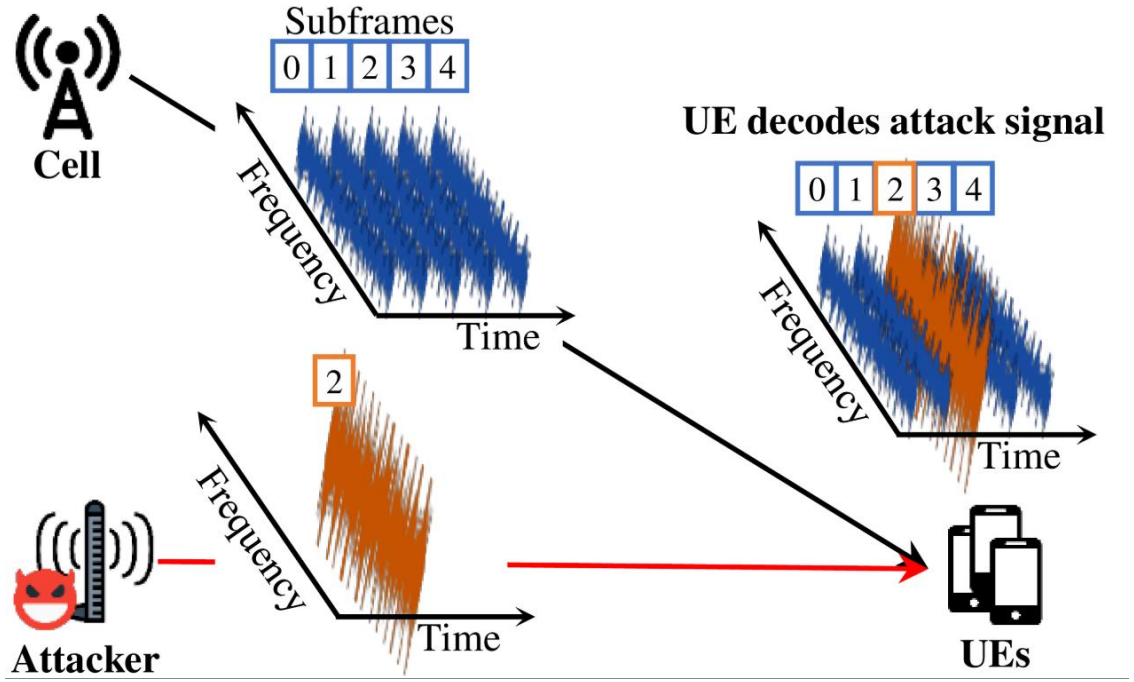
O: Network skips the *GUTI Reallocation*
X: No noticeable change

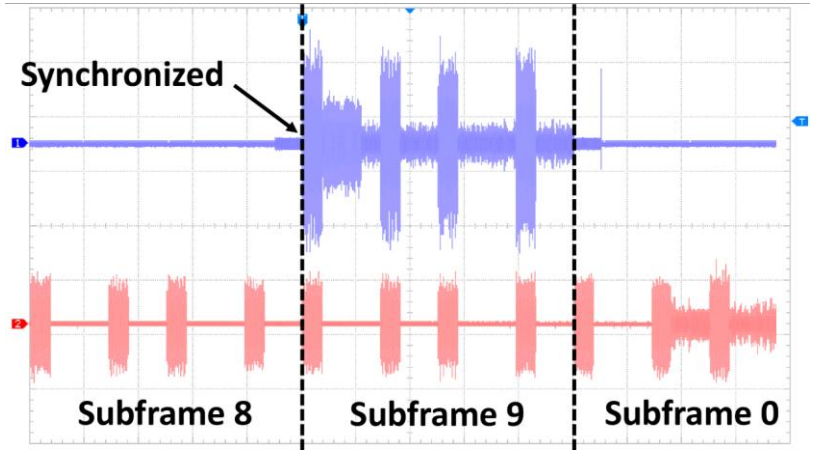


Fake CMAS broadcast attack

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



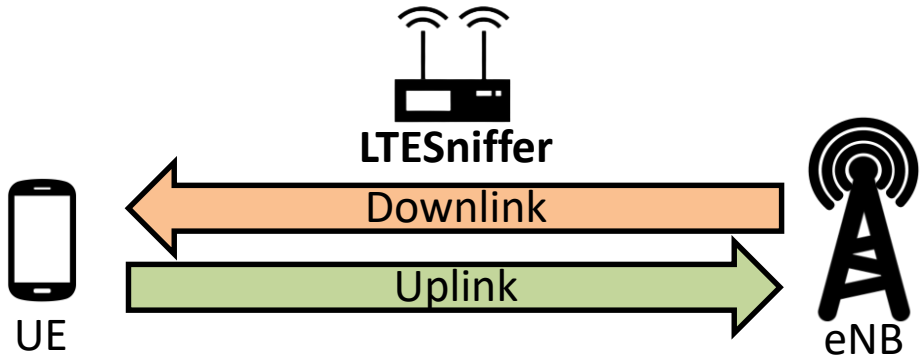


Demonstration of Signal Injection attack

DATA RESTRICTIONS

LTESniffer

- Decoding LTE uplink-downlink control-data channels
  - Downlink: PDCCH, PDSCH (up to 256QAM)
  - Uplink: PUSCH (up to 256QAM)
- Storing decoded packets in Pcap files for further analysis
- Supporting a security API with three functions
  - 1) Identity mapping 2) IMSI collecting 3) UE Capability Profiling
- Open-source*

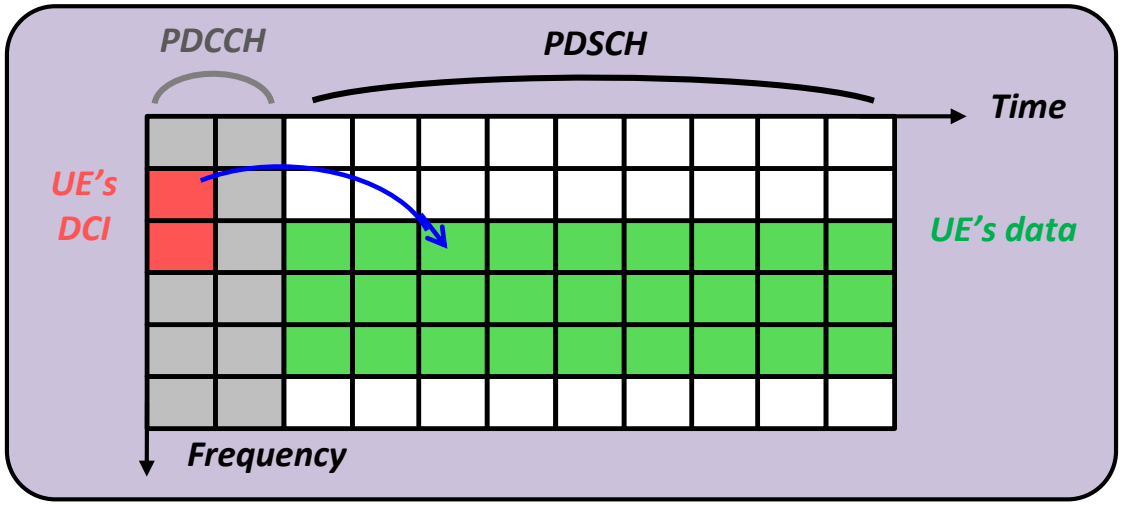


SCAN ME

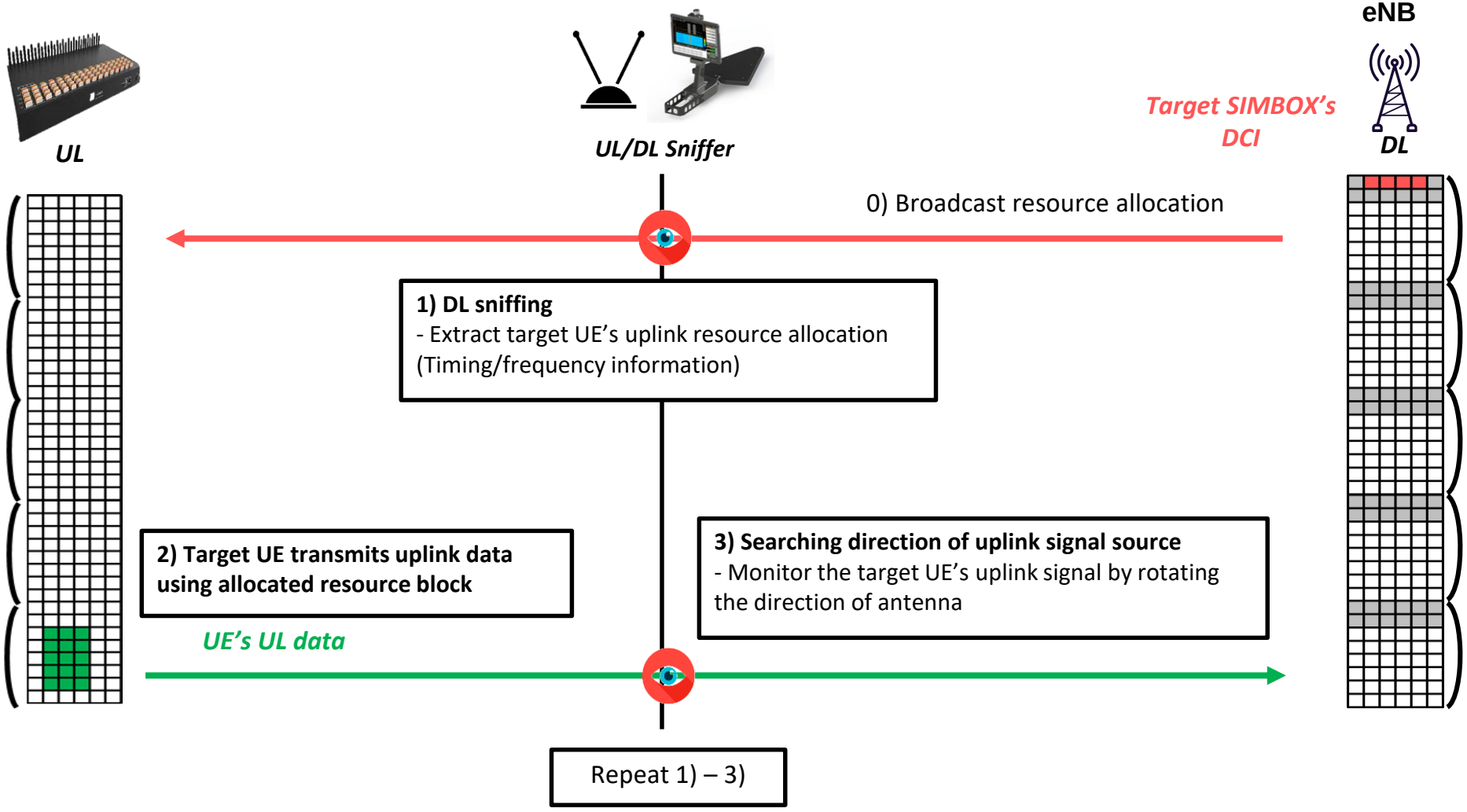
Leaked Downlink Data Transmission Information

- 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




HONDA
HONDA

Unauthorized Localization in Wild

- Korean police plans to do unauthorized localization to defeat vishing
  - Track and seize illegal devices used in vishing fraud
  - Without control to UE and eNB
  - Using vehicle-mounted location tracker

Catching Voice Phisher's UE

Conclusion (Attack+Specification)

- Unpatched Design Vulnerabilities in 5G
  - 5G Sniffer, 5G Sigover, 5G FBS/MitM, …
  - Cellular Metasploit ➔ Used for IDS R&D
  - Attacks possible against private 5G application domains
  - Fixing them in 6G?
  - Developing applications utilizing design vulnerabilities (e.g. Location tracking)

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

This presentation was supported and funded by the Korean National Police Agency.
(Project Name: Tracking and identifying devices and call traffic in voice phishing ecosystem / Project Number: PR10-03-020-22)