Cellular Security Overview + LTEFuzz

Yongdae Kim

KAIST
SysSec Lab

* A revised presentation from QPSS’19 presentation

Cellular Security Publications (Selected)

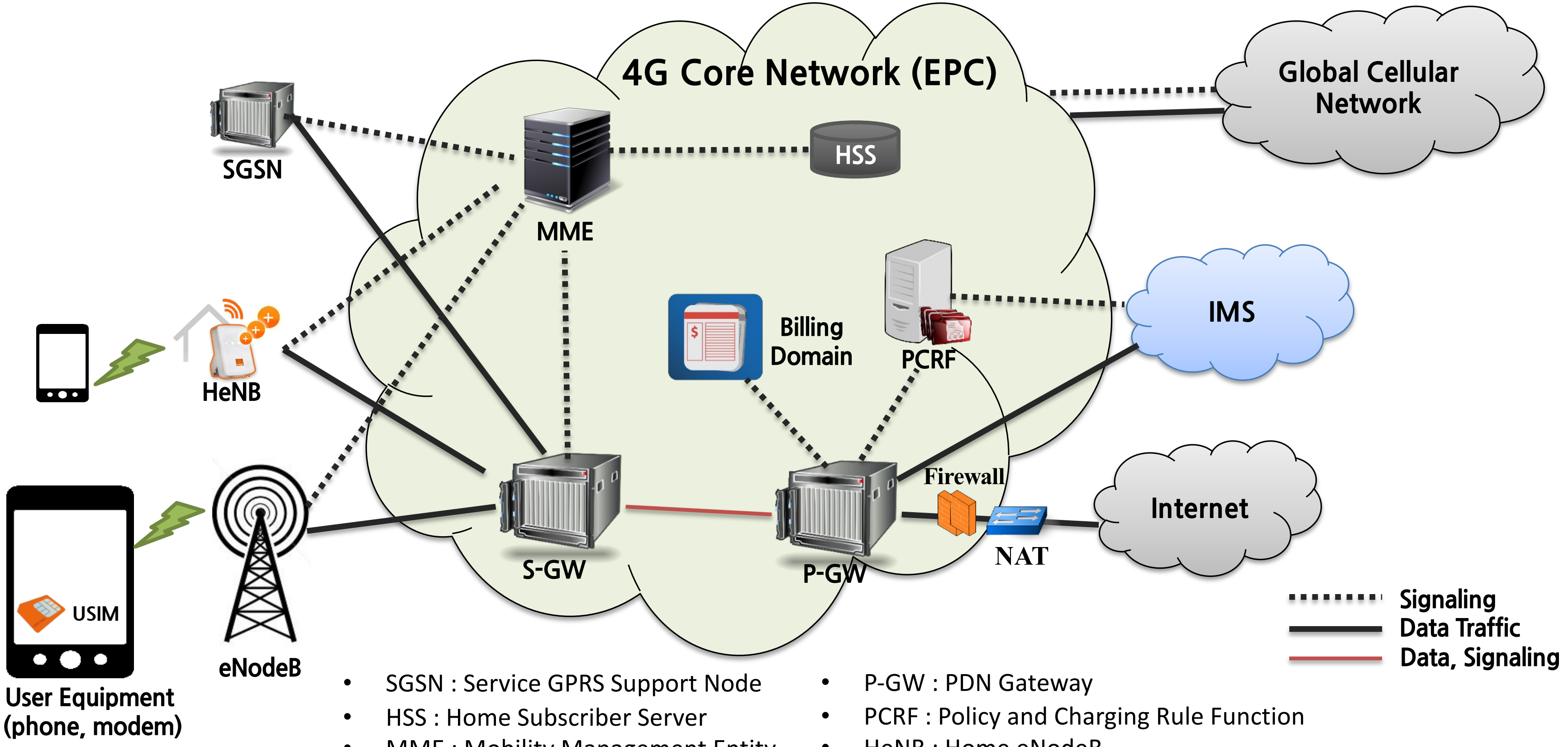
5 NDSS, 4 Usenix Sec, 1 CCS, 1 S&P. 1 EuroS&P, 1 TMC, 1 WISEC

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

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]
  - LTESniffer: Up-/Down-link sniffer [WISEC’23]
- Test/Measurement
  - VoLTE [CCS’15]
  - Performance bug [TMC’18, Hotmobile’19]
  - LTEFuzz: Up-/Down-link negative Fuzzer [S&P’19]
  - DoLTEst: Stateful Down-link Fuzzer [Usenix Sec’22]
  - UE Fingerprinting [NDSS’23]
- Static Analysis
  - Baseband Static Analysis [NDSS’21, Usenix Sec’23]

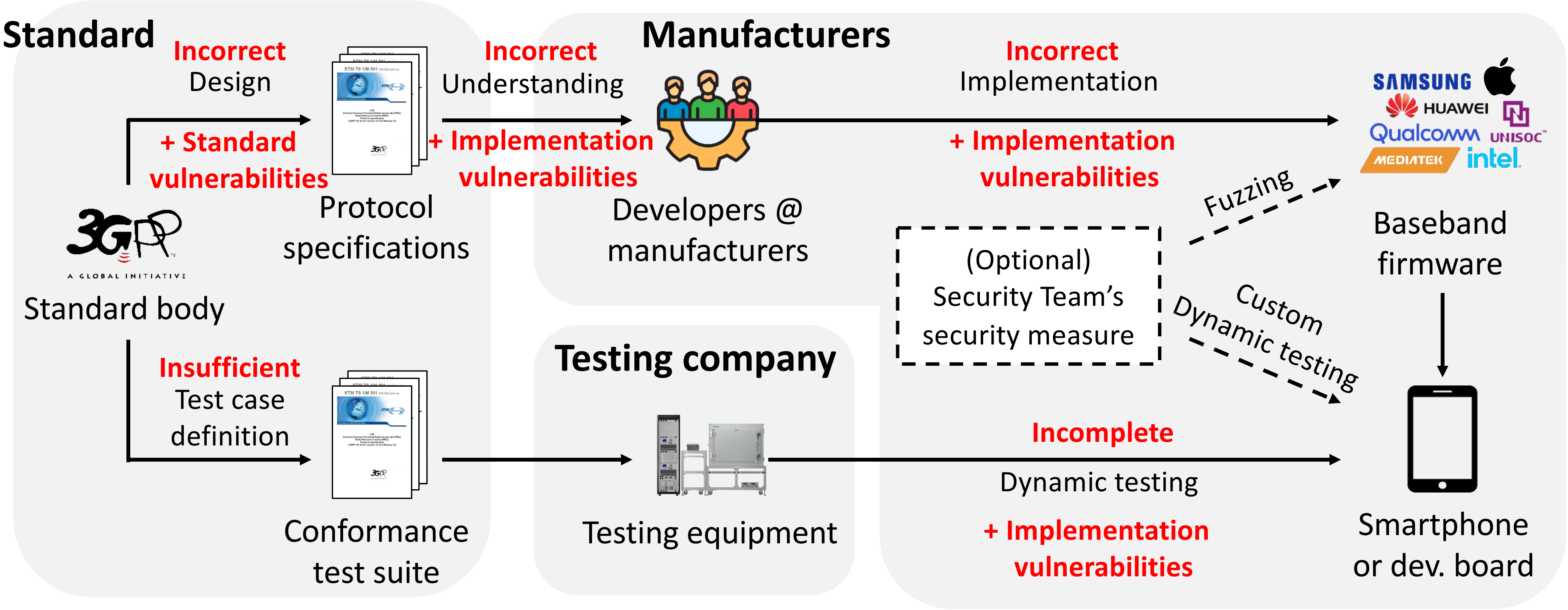
4G LTE Cellular Network Overview



- 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

Security problems in baseband (UE)

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



Why Cellular Implementation vulns Exist?

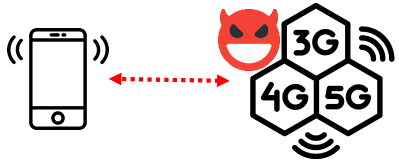
- New Generation (Technology) every 10 years
  - New Standards, Implementation, and Deployment ➔ New vulnerabilities
- Generation overlap: e.g. 3G, LTE and CSFB vulnerabilities in CSFB
- Government > Carrier > Device vendors > Customers ☺
- Walled Garden
  - Carriers and vendors don't talk to each other.
  - Carriers: (Mostly) No response to responsible disclosure
- Complicated and huge standards ➔ Hard to find bugs, need a large group
  - Multiple protocols co-work, but written in separate docs
- Standards are written ambiguously
  - Misunderstanding by vendors and carriers
  - Leave many implementation details for vendors
- Cellular networks/devices could be different from each carrier and vendor
- Conformance testing standard, but (almost) no security testing standard

Why Cellular Design Vulnerabilities Exist?

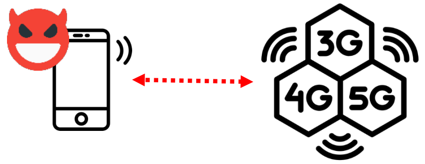
- New Generation (Technology) every 10 years
  - New Standards, Implementation, and Deployment ➔ New vulnerabilities
- Backward compatibility: e.g. supporting 2G
- Government > Carrier > Device vendors > Customers ☺
  - Or Government > GSMA > 3GPP > Customers
  - To become standard, one needs unanimous support.
  - Too expensive, need insecurities, not a big deal, …
- Complicated and huge standards ➔ Hard to find bugs, need a large group
  - Multiple protocols co-work, but written in separate docs
- No visible attackers so far
- Papers presented, featured in newspapers, discussed in 3GPP, but forgotten later

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

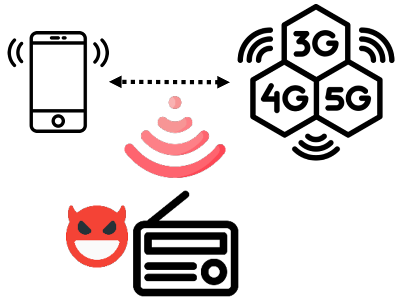
Threat Models



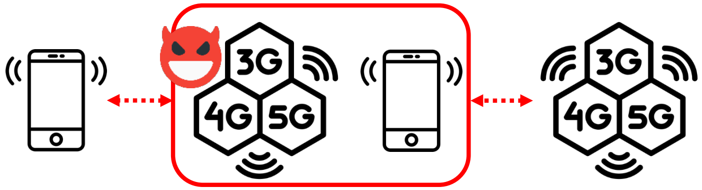
Fake base station



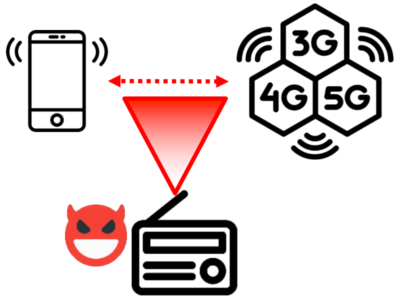
Fake UE



Sniffer



Man-in-the-Middle (MitM)



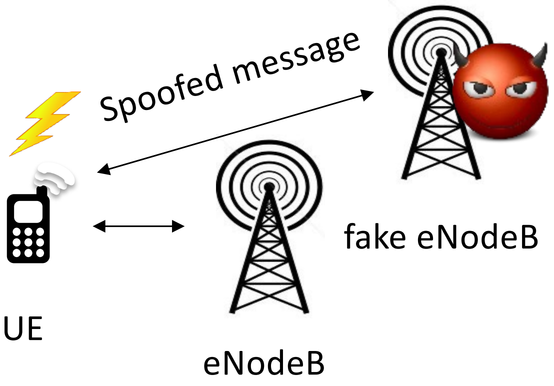
SigOver (Overshadowing)

Unpatched Design Vulnerabilities

Fake CMAS broadcast attack

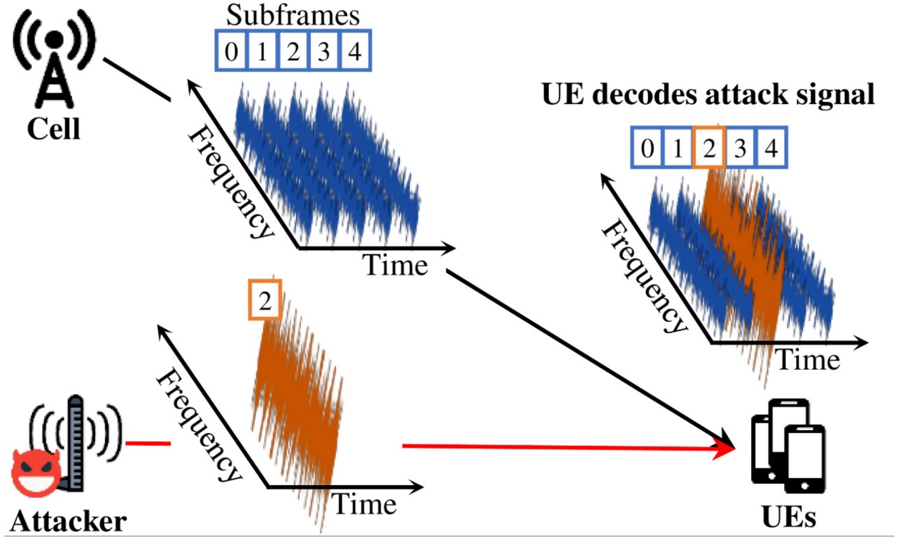
Attacks using SDR based “Fake BTS”

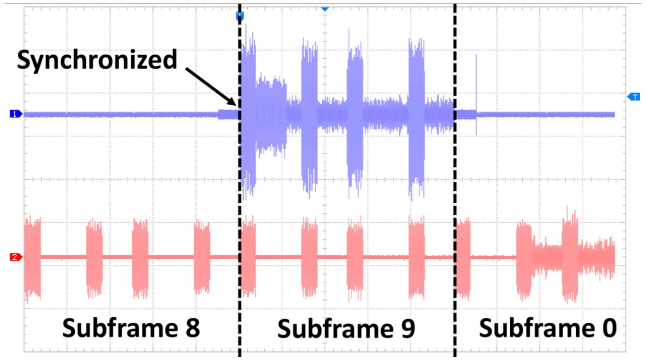
- Exploit physical layer procedure
  - Fake BTS synchronizes with a benign eNodeb, and send spoofed signal to UEs or receive uplink signal from UEs
    - Selective Jamming
    - Malicious data injection
      - e.g. warning message (Emergency SMS), detach message
- Exploit unprotected RRC, NAS Procedure
  - DoS: Attach/TAU/Service Reject
  - Privacy leak: Identity request



Signal Overshadowing: SigOver Attack

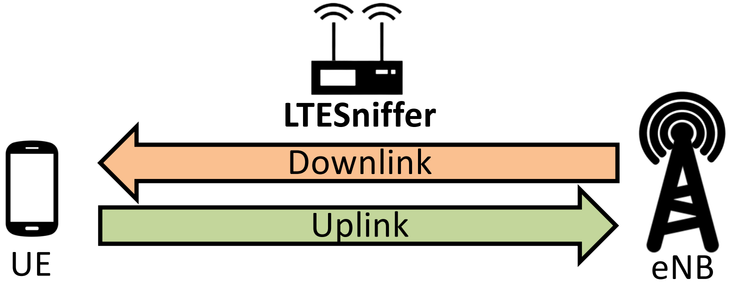
- Signal injection attack exploits broadcast messages in LTE
  - Broadcast messages in LTE have never been integrity protected!
- Transmit time- and frequency-synchronized signal





LTESniffer

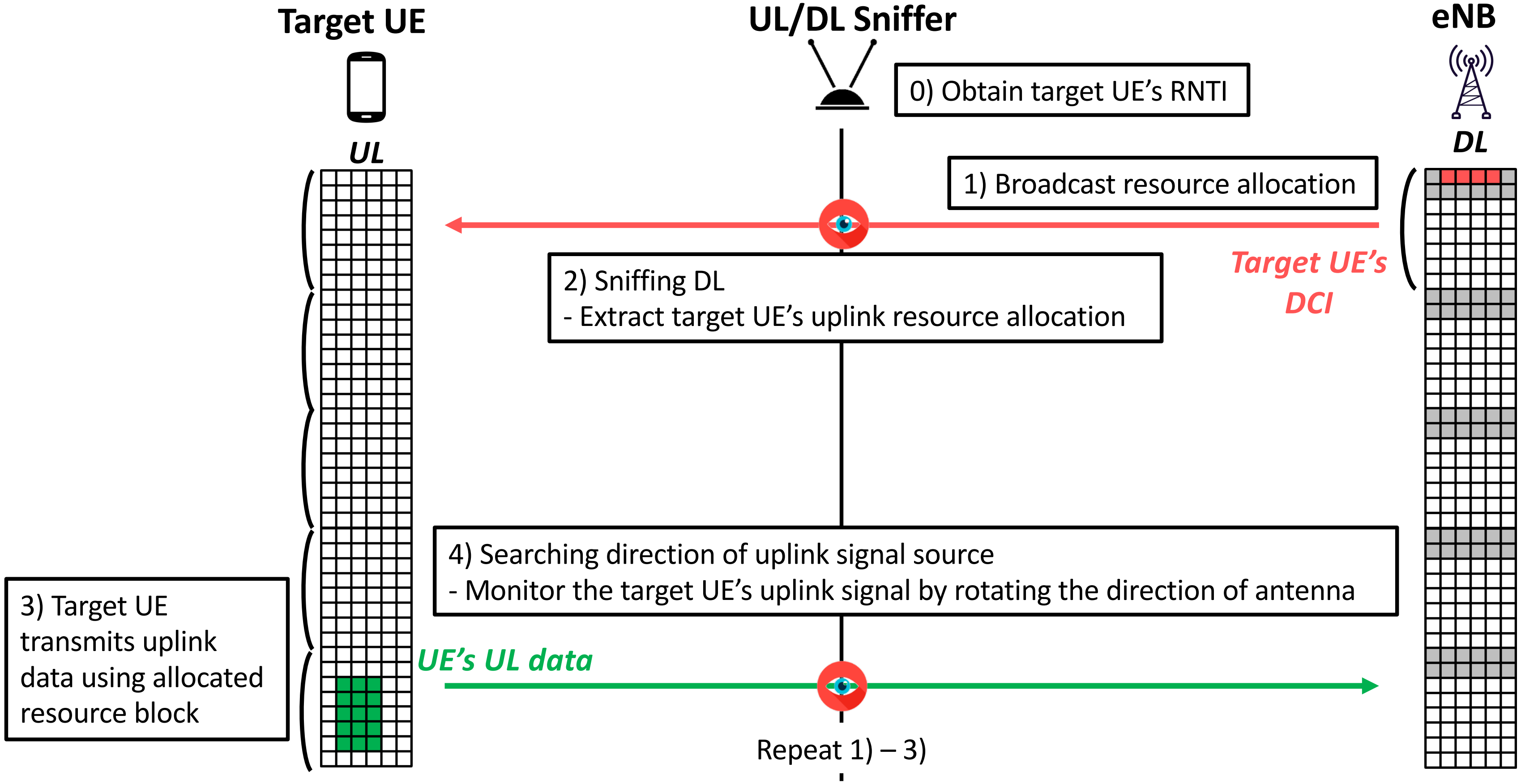
- ❖ Decoding LTE uplink-downlink control-data channels
  - – Downlink: PDCCH, PDSCH (up to 256QAM)
  - – Uplink: PUSCH (up to 256QAM)
- ❖ Storing decoded packets in Pcap files for further analysis
- ❖ Supporting a security API with three functions
  - – 1) Identity mapping 2) IMSI collecting 3) UE Capability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



SCAN ME

LTESniffer: An Open-source LTE Downlink/Uplink Eavesdropper, WISEC'23, https://github.com/SysSec-KAIST/LTESniffer

Unauthorized Localization of LTE Devices



0) Obtain target UE's RNTI

1) Broadcast resource allocation

2) Sniffing DL
- Extract target UE's uplink resource allocation

3) Target UE transmits uplink data using allocated resource block

4) Searching direction of uplink signal source
- Monitor the target UE's uplink signal by rotating the direction of antenna

Repeat 1) – 3)

Cellular Insecurity in Standard

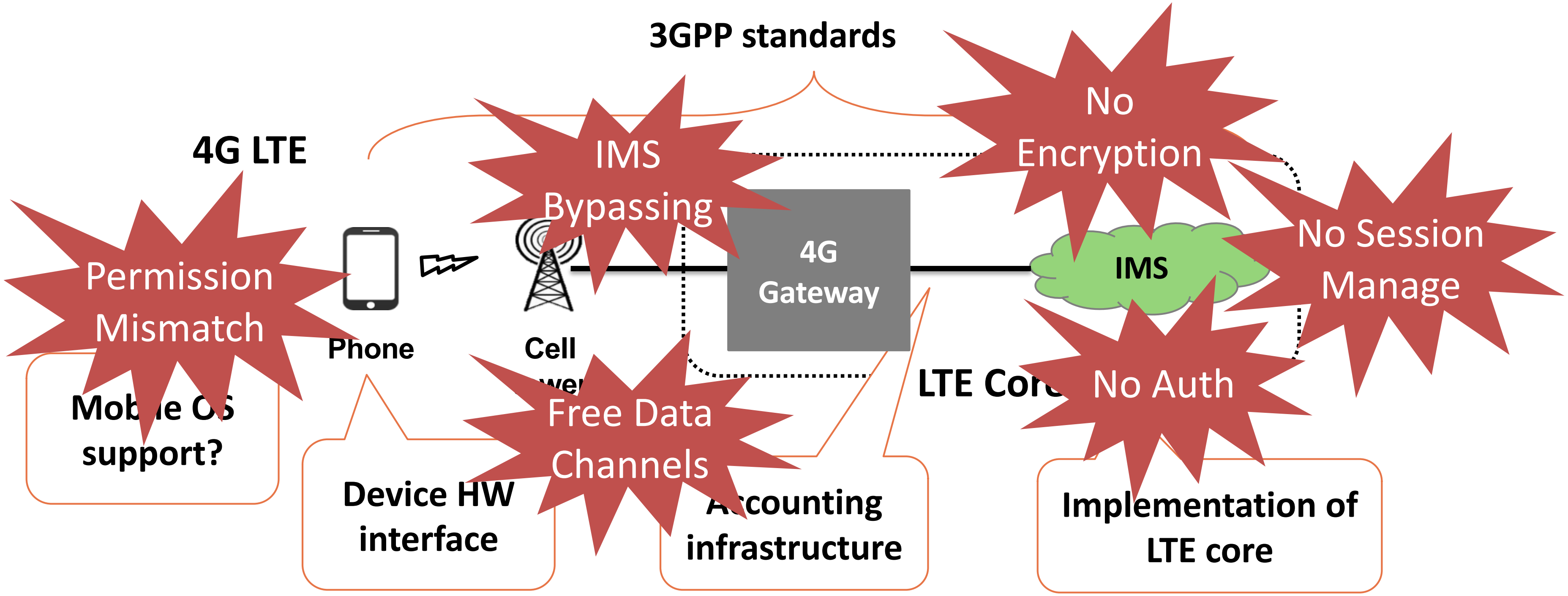
- Unauthenticated broadcast channel
- Roaming networks such as SS7 and Diameter
- Unauthenticated initial messages
- No voice encryption
- No MAC layer protection
- Lawful Interception
- Still symmetric key-based key management

- Suppose you implement cellular network (e.g. 6G) from scratch, would you design with these insecurities?

Security of New Systems

VoLTE makes cellular network more complex

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

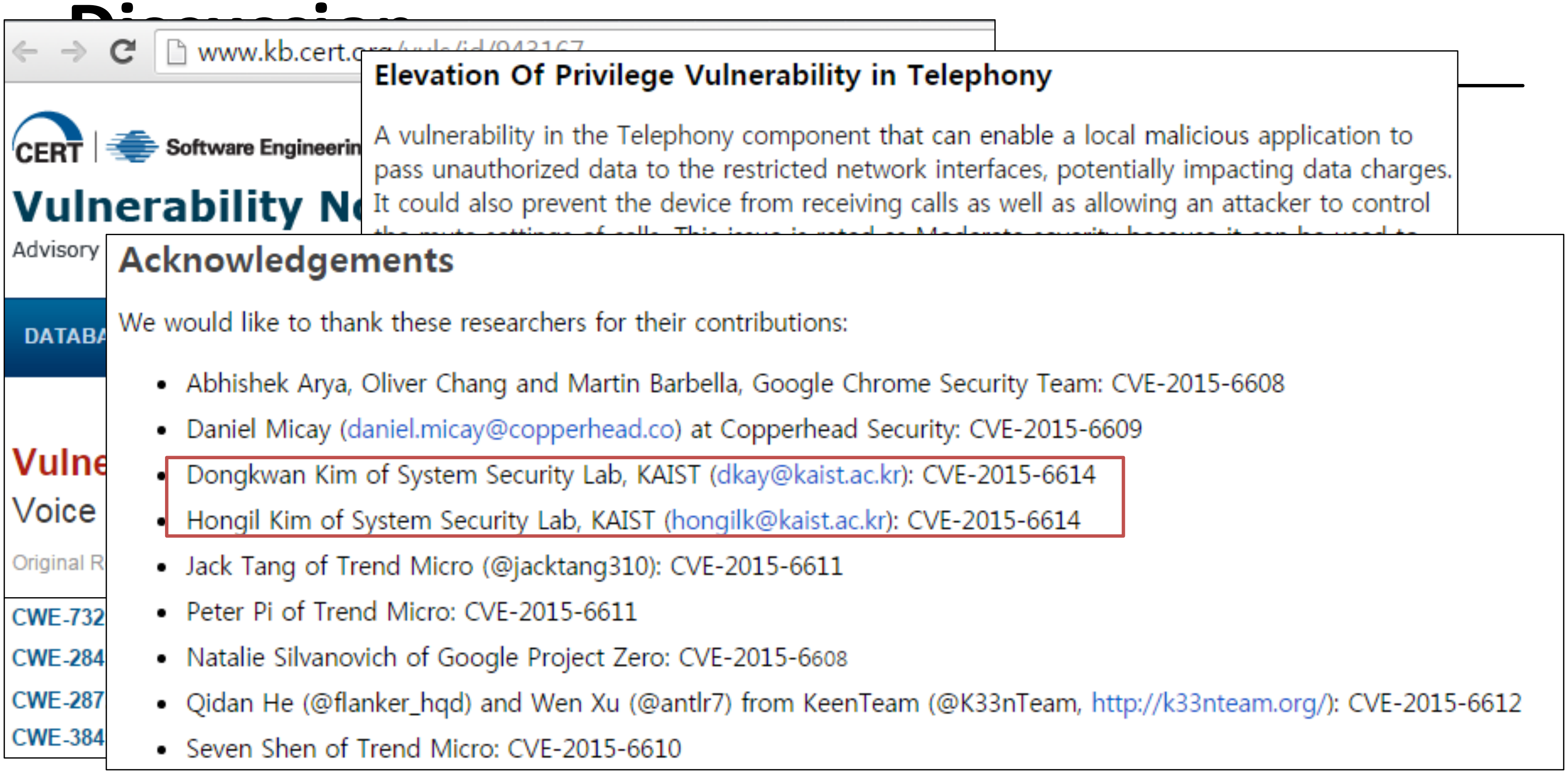


Free Data Channels	Free Channel	US-1	US-2	KR-1	KR-2	KR-3
Using VoLTE Protocol	SIP Tunneling	✓	✓	✓	✓	✓
	Media Tunneling	✓	✓	✓	✓	✓
Direct Communication	Phone to Phone	✓	✗	✓	✗	✗
	Phone to Internet	✗	✓	✓	✗	✗

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 the mute settings of calls. This issue is rated as Moderate severity because it can be used to

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

Cellular Security Testing

Cellular Security Testing (Analysis)

- Target
  - Cellular modem/devices, cellular carrier networks, standards
- Why?
  - New Generation (Technology) every 10 years
  - Complicated and huge standards
  - Ambiguous standards
  - Leave many implementation details for vendors
  - Cellular networks/devices could be different from each carrier and vendor
  - Conformance testing standard, but (almost) no security testing standard

Approaches

- Keywords
  - Static, dynamic, comparative, negative testing, formal analysis, state machine, specification, traffic, binary, source code, modem, devices, specification, …
- Summary

Venue	Topic	Test Keywords
CCS’15	VoLTE	Static, dynamic, negative testing, binary, modem, device, carrier
TMC’18	NAS/RRC	Dynamic, comparative, device, carrier
S&P’19	NAS/RRC	Dynamic, negative testing, modem, device, carrier
NDSS’21	NAS/RRC	Static, comparative, modem, binary, specification
Usenix’22	NAS/RRC	Dynamic, negative testing, modem

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**

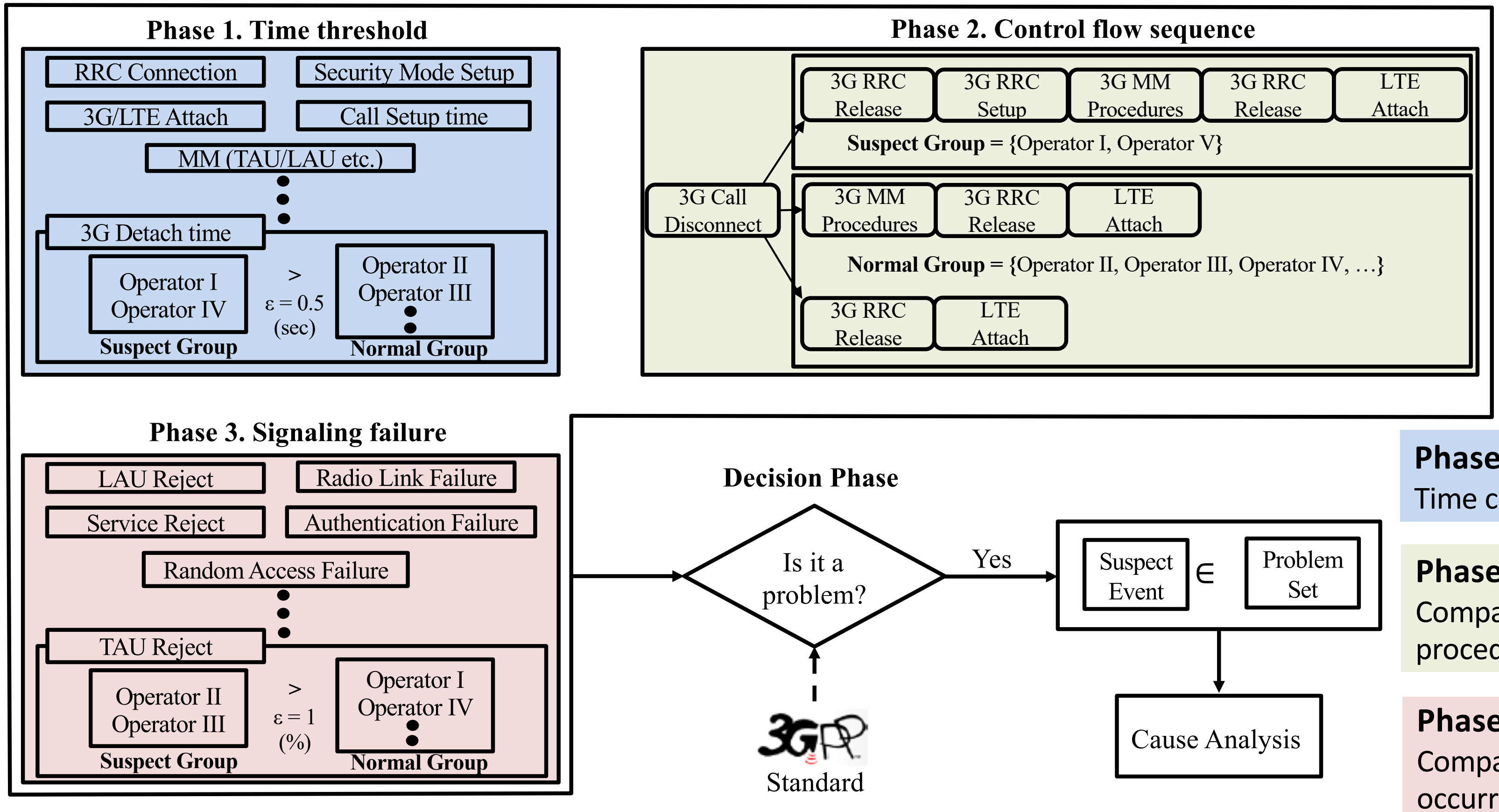
# of operators: **28**

# 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

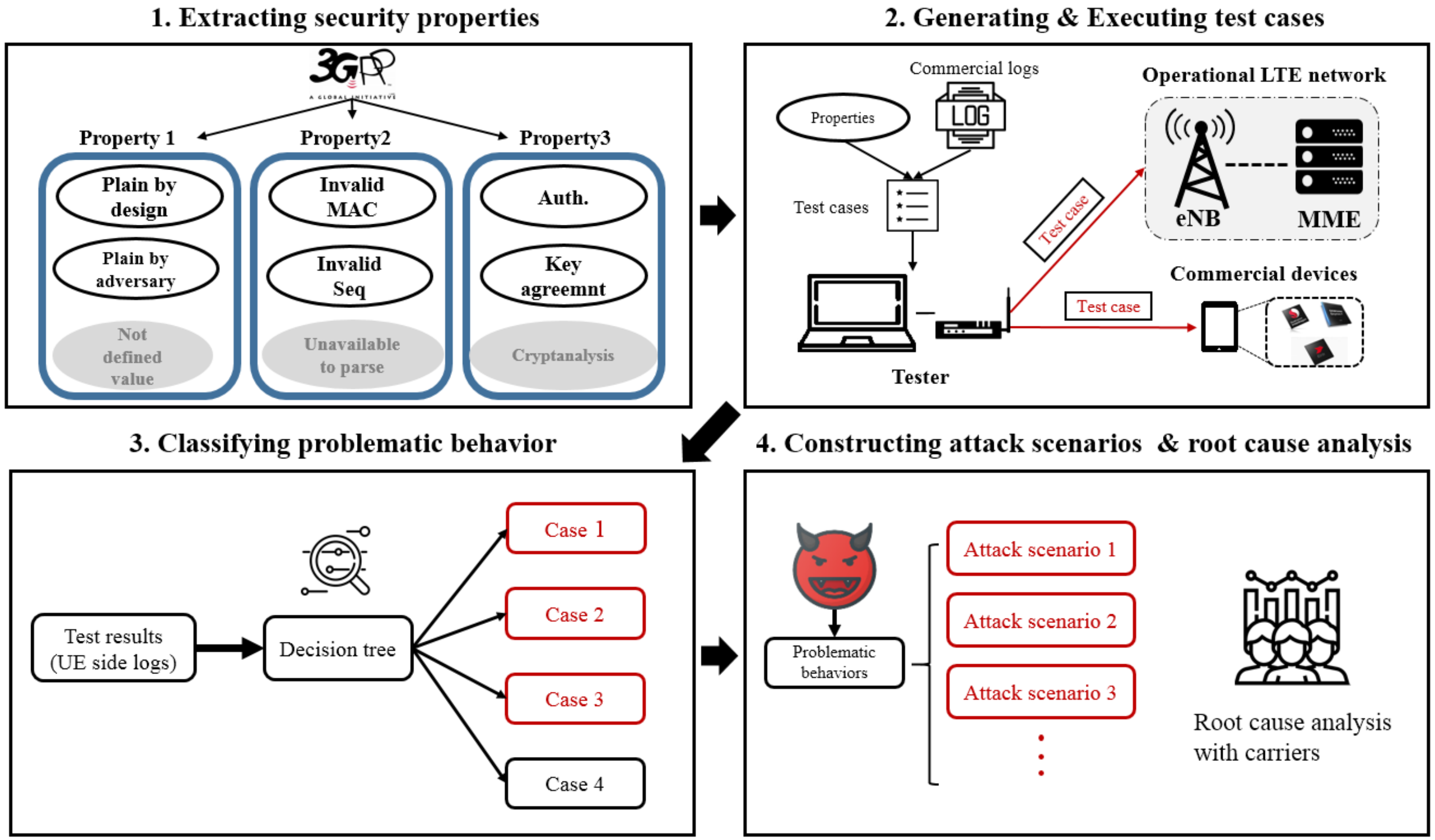
Phase 3
Comparison of signaling failure occurrence probability

Identified Problems

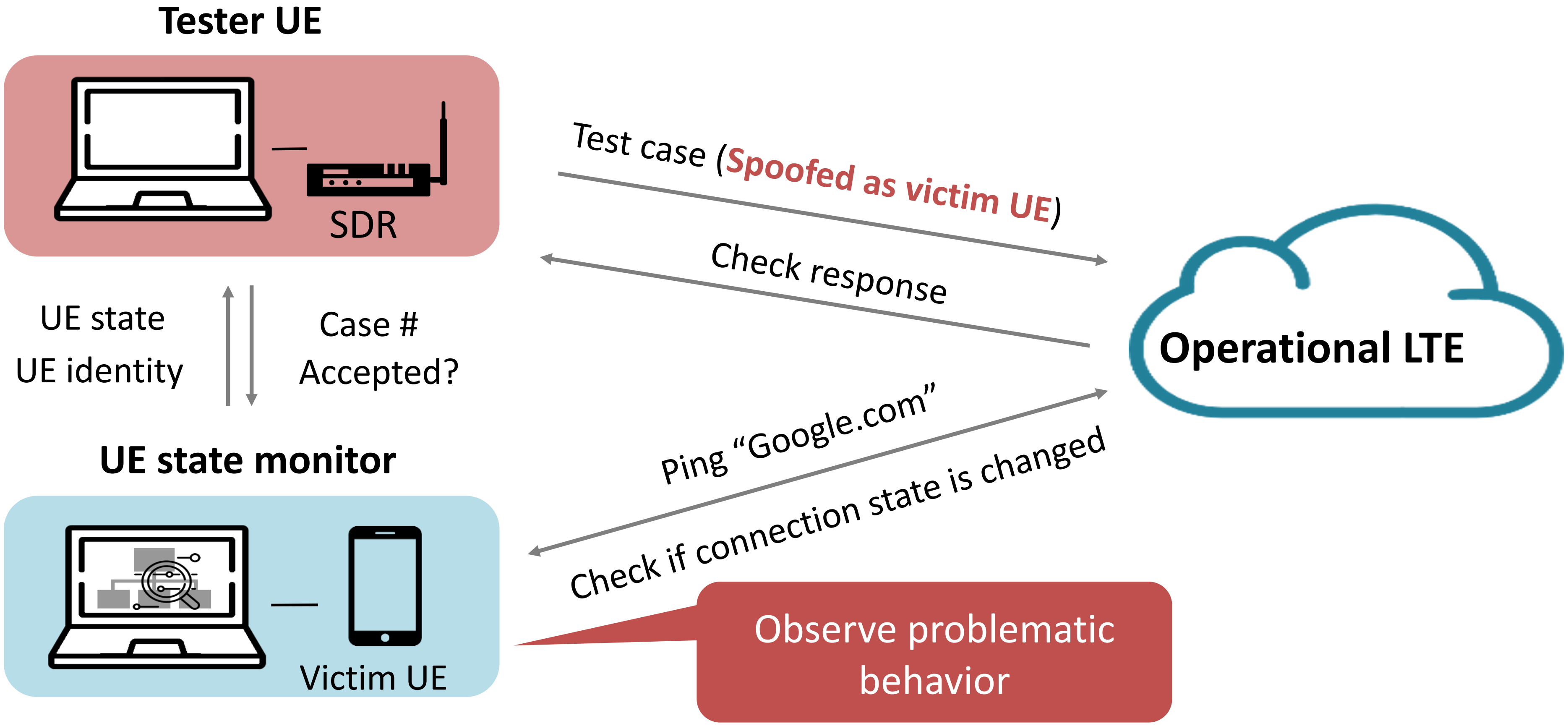
Problem	Observation	Operator
LTE location update collision	**Out-of-service** about **11 s**	US-II
Mismatch procedures	Delay of 3G detach. Worst case: **10.5 s**	US-I, DE-I. DE-II, FR-I, FR-II
Allocation of incorrect frequency	**Out-of-service 30 sec**. and **stuck in 3G for 100 s**	DE-I
Redundant location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

Fuzzing LTE Core and Baseband

LTEFuzz


1. Extracting security properties
3GPP
A GLOBAL INITIATIVE
Property 1
Property2
Property3
Plain by design
Plain by adversary
Not defined value
Invalid MAC
Invalid Seq
Unavailable to parse
Auth.
Key agreemnt
Cryptanalysis
2. Generating & Executing test cases
Commercial logs
LOG
Properties
Test cases
Tester
Test case
Test case
Operational LTE network
eNB
MME
Commercial devices
3. Classifying problematic behavior
Test results (UE side logs)
Decision tree
Case 1
Case 2
Case 3
Case 4
4. Constructing attack scenarios & root cause analysis
Problematic behaviors
Attack scenario 1
Attack scenario 2
Attack scenario 3
Root cause analysis with carriers

Executing Test Cases



Tester UE

SDR

UE state

UE identity

Case #

Accepted?

UE state monitor

Victim UE

Test case (**Spoofed as victim UE**)

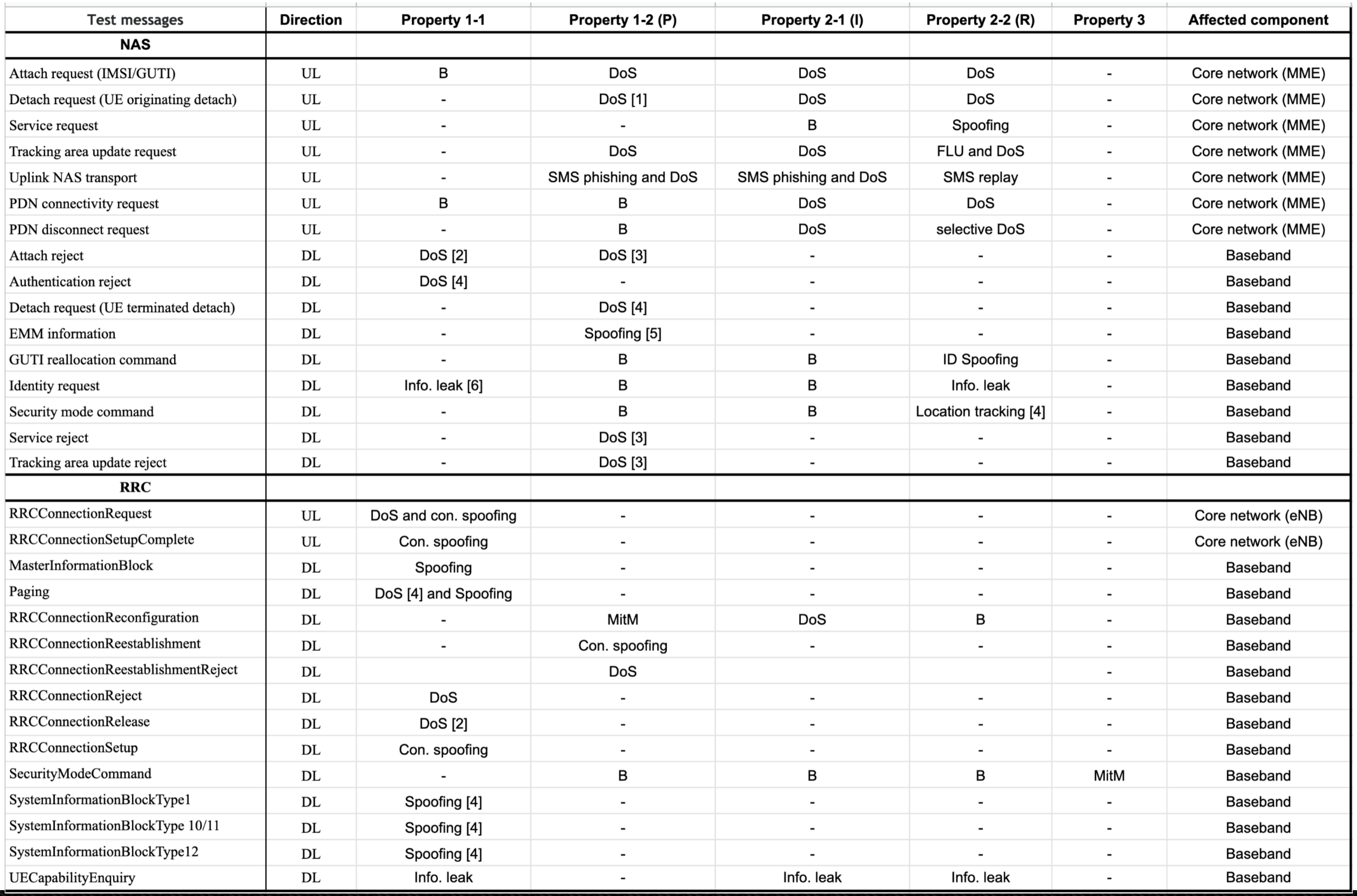
Check response

Operational LTE

Ping "Google.com"

Check if connection state is changed

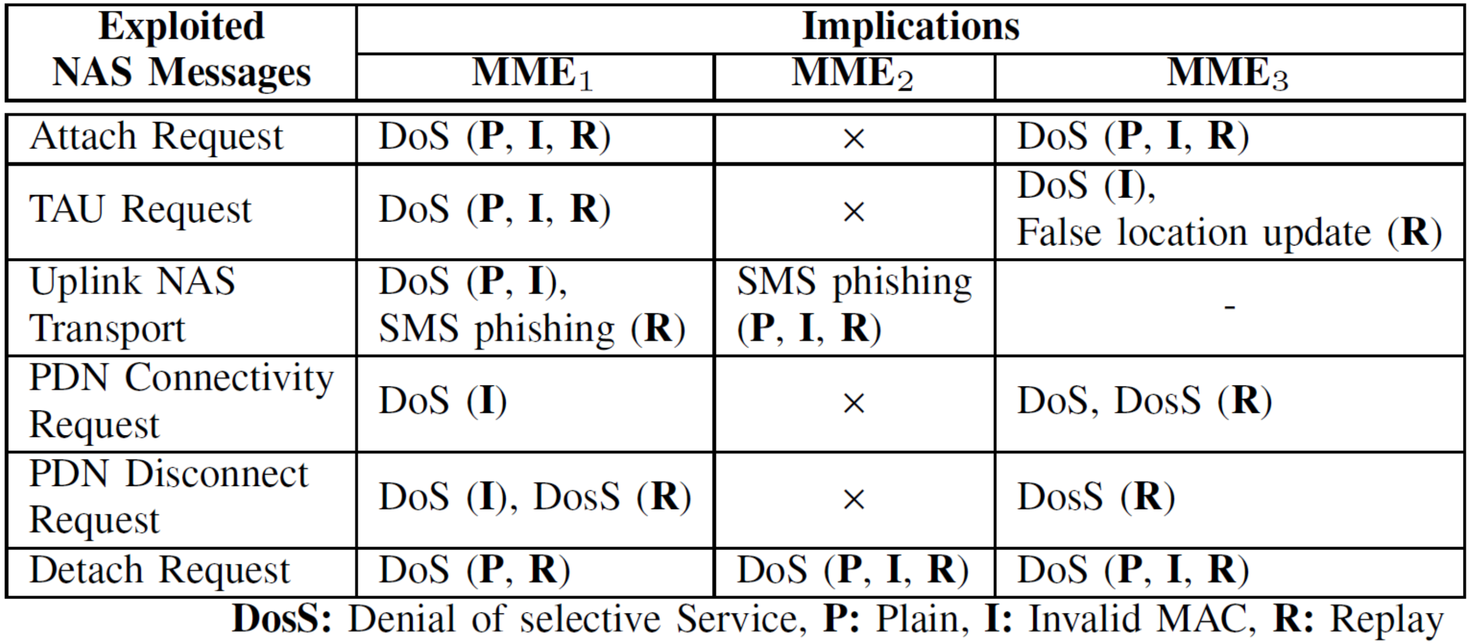
Observe problematic behavior



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

Attacks exploiting MME

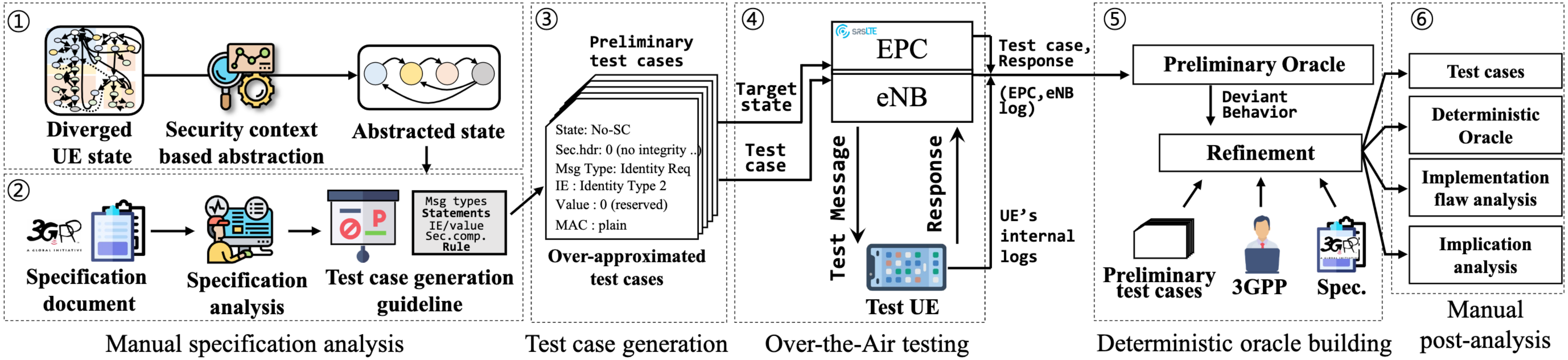
- Result of dynamic testing against different MME types
  - Carrier 1: MME1, MME2, Carrier2: MME3 (MME1 & MME3: the same vendor)



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


①
Diverged UE state
Security context based abstraction
Abstracted state
②
3GPP
Specification document
Specification analysis
Test case generation guideline
Msg types
Statements
IE/value
Sec.comp.
Rule
Manual specification analysis
③
Preliminary test cases
State: No-SC
Sec.hdr: 0 (no integrity ..)
Msg Type: Identity Req
IE : Identity Type 2
Value : 0 (reserved)
MAC : plain
Over-approximated test cases
Test case generation
④
srsLTE
EPC
eNB
Target state
Test case
Test Message
Response
Test UE
Over-the-Air testing
Test case, Response
(EPC,eNB log)
UE's internal logs
⑤
Preliminary Oracle
Deviant Behavior
Refinement
Preliminary test cases
3GPP
Spec.
Deterministic oracle building
⑥
Test cases
Deterministic Oracle
Implementation flaw analysis
Implication analysis
Manual post-analysis

Conclusion

- ❖ Design vulnerabilities
  - – Technical problems + Political problems
  - – Clear slate design for 6G
- ❖ Spec could be written better.
  - – Formally verifiable?
  - – Sample implementation needs to be provided
  - – Negative testing (security testing) should be standardized!
- ❖ Use of NLP to understand 3GPP Spec
  - – Seems impossible… Inconsistencies, ambiguities, and domain knowledge
- ❖ Binary vs. Source code vs. Spec comparison
  - – Long long way to go ☹

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”