Cellular Security
- Why is it difficult? -

Yongdae Kim

KAIST
SysSec Lab

* A revised presentation from QPSS'19 presentation

SysSec Lab.

- System Security Lab. @ KAIST, Korea
  - Yongdae Kim
  - Prof @ Electrical Engineering & Information Security

- Research areas: Finding new problems in Emerging Technologies such as Drone, Blockchain, Medical device, Automobiles, Cellular, …
  - Software vulnerability (hacking)
  - Physical system security (sensor, hardware Trojan, …)
  - Wireless communication security (Bluetooth, Zigbee, …)
  - Mobile network security (privacy, abuse, …)
- My students report vulns to vendors e.g. Qualcomm, Samsung, Apple, Huawei, LG, Carriers, Velodyne, etc.

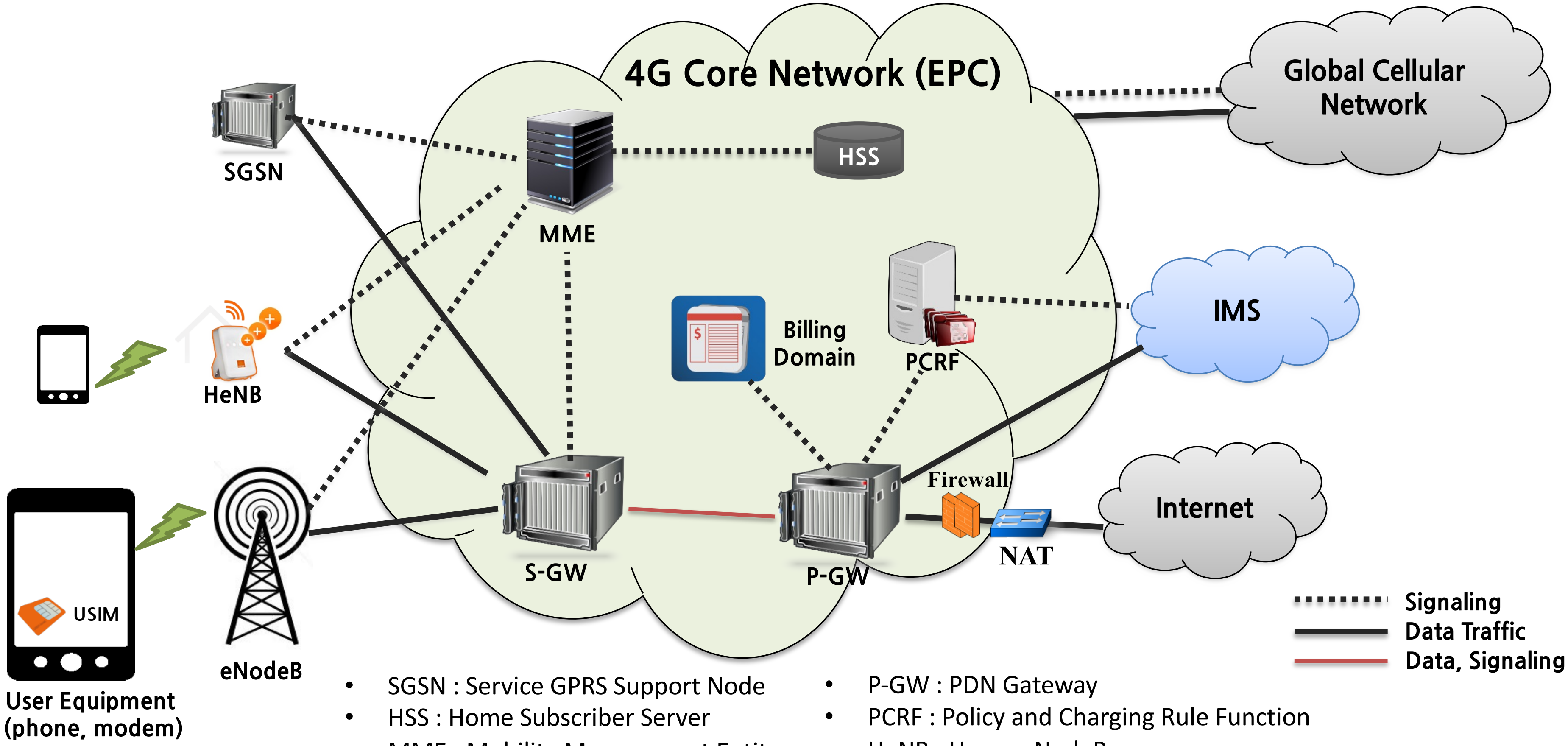
Cellular Security Publications (Selected)

- 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
- Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE, Usenix Sec’19
- Hidden Figures: Comparative Latency Analysis of Cellular Networks with Fine-grained State Machine Models, Hotmobile’19
- BASESPEC: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols, NDSS’21
- DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices, Usenix Sec’22
- Watching the Watchers: Practical Video Identification Attack in LTE Networks, Usenix Sec’22

IMO, many mores to come…

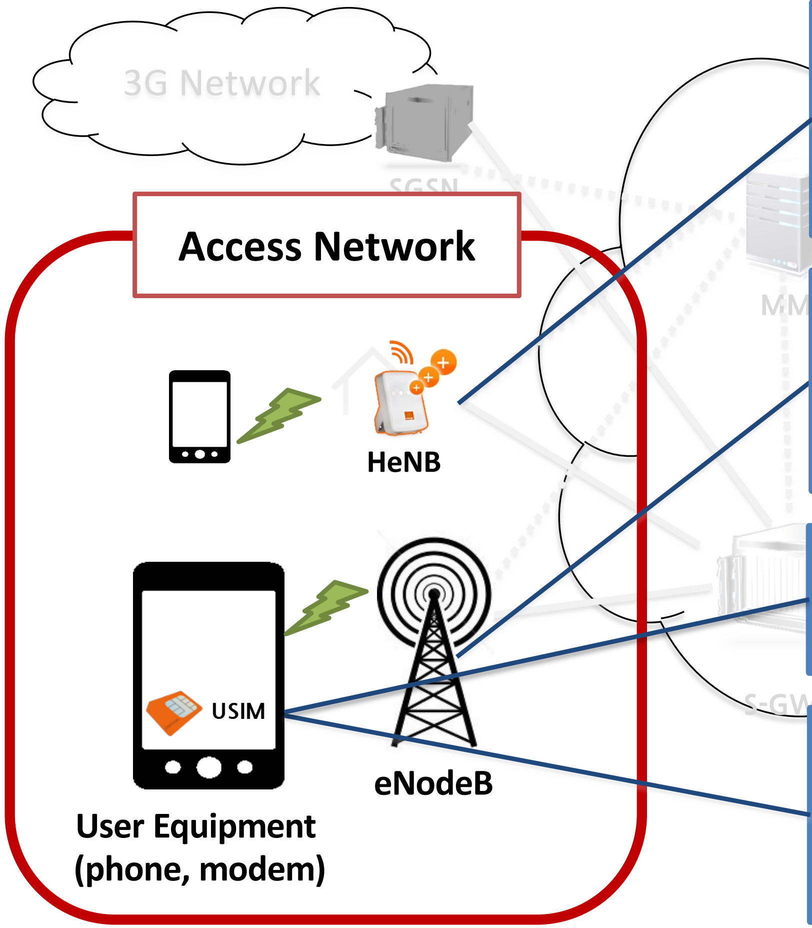
Why
cellular networks/devices/protocols
have so many security problems?

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 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, privacy leak, Emergency SMS
- “Signal Overshadowing”: DoS, privacy leak, …
- “Fake UE”: LTE interception attack, Core network fuzzing

3G/LTE modem security

- Remote access/command injection
- Firmware repackaging

USIM security

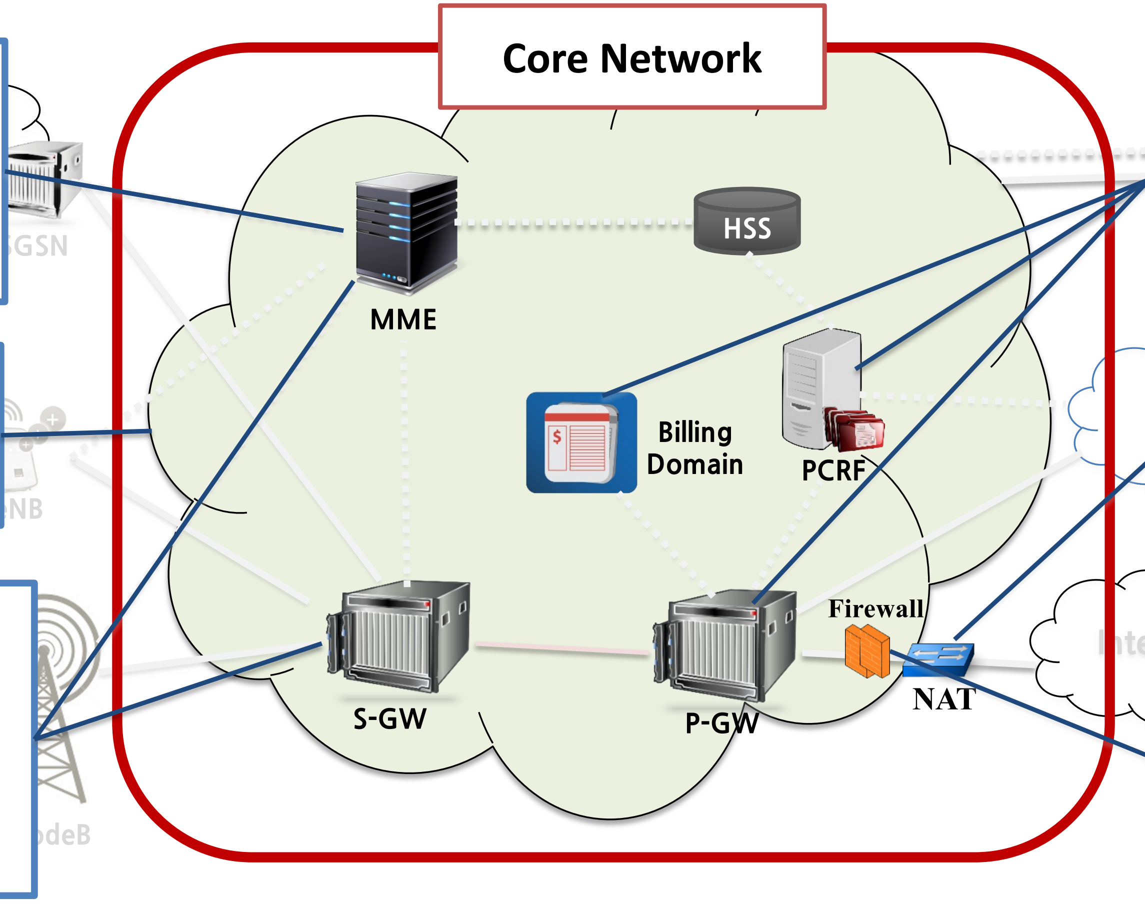
- Reading privacy info. (SMS, Phonebook, cell location)
- Get an authentication vector
- SIM Cloning/Spoofing

Security Issues in Core Network

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

Distributed Denial of Service
- 1Tbps DDoS

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

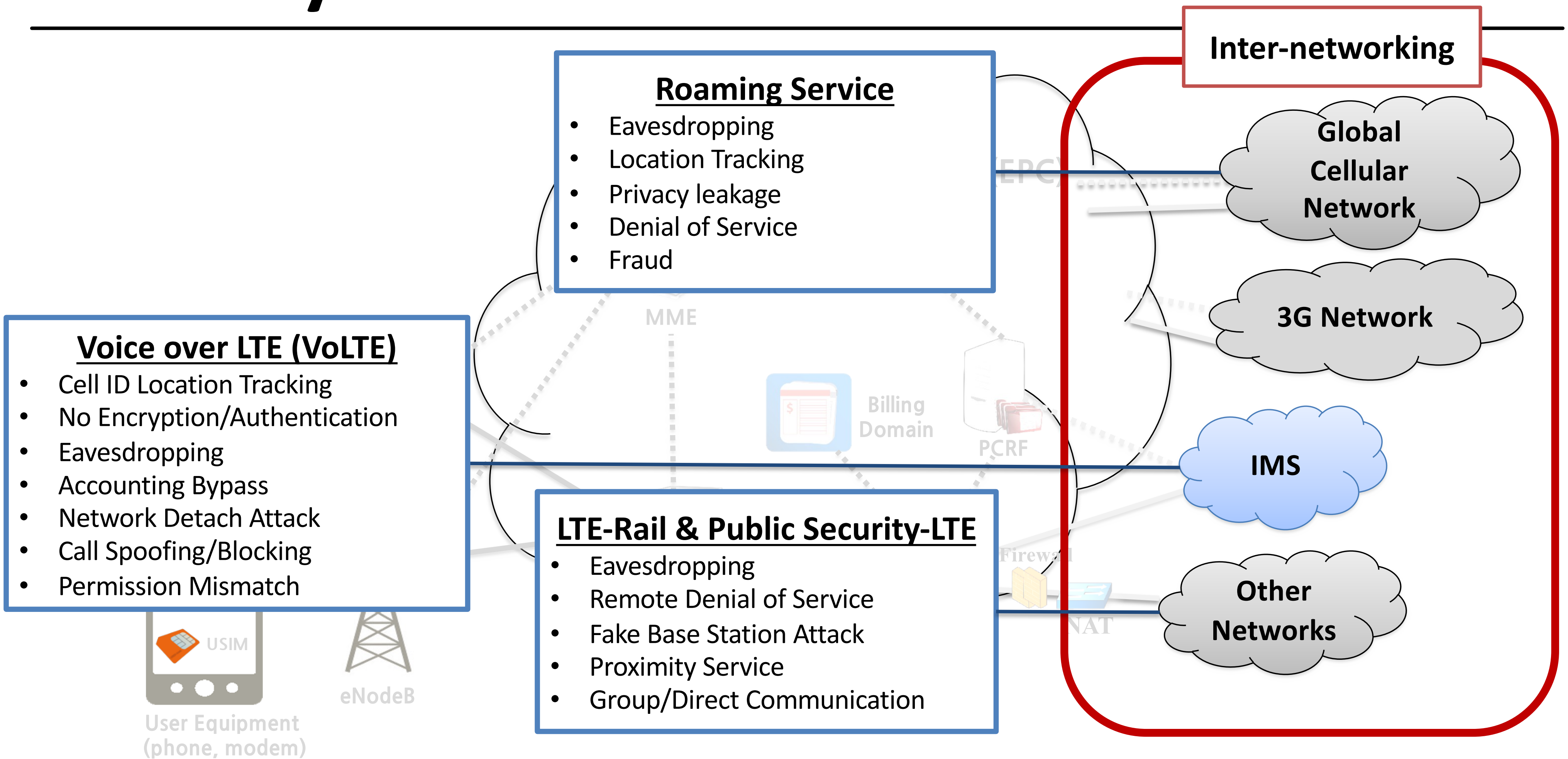


Charging policy
- Overbilling
- Free riding
  - ✓ Zero rating protocol
  - ✓ TCP Retransmission

NAT
- NAT Public IP Disabling
- NAT Resource Exhaustion

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

Security Issues in Services



Cellular Security: Why Difficult? Meta

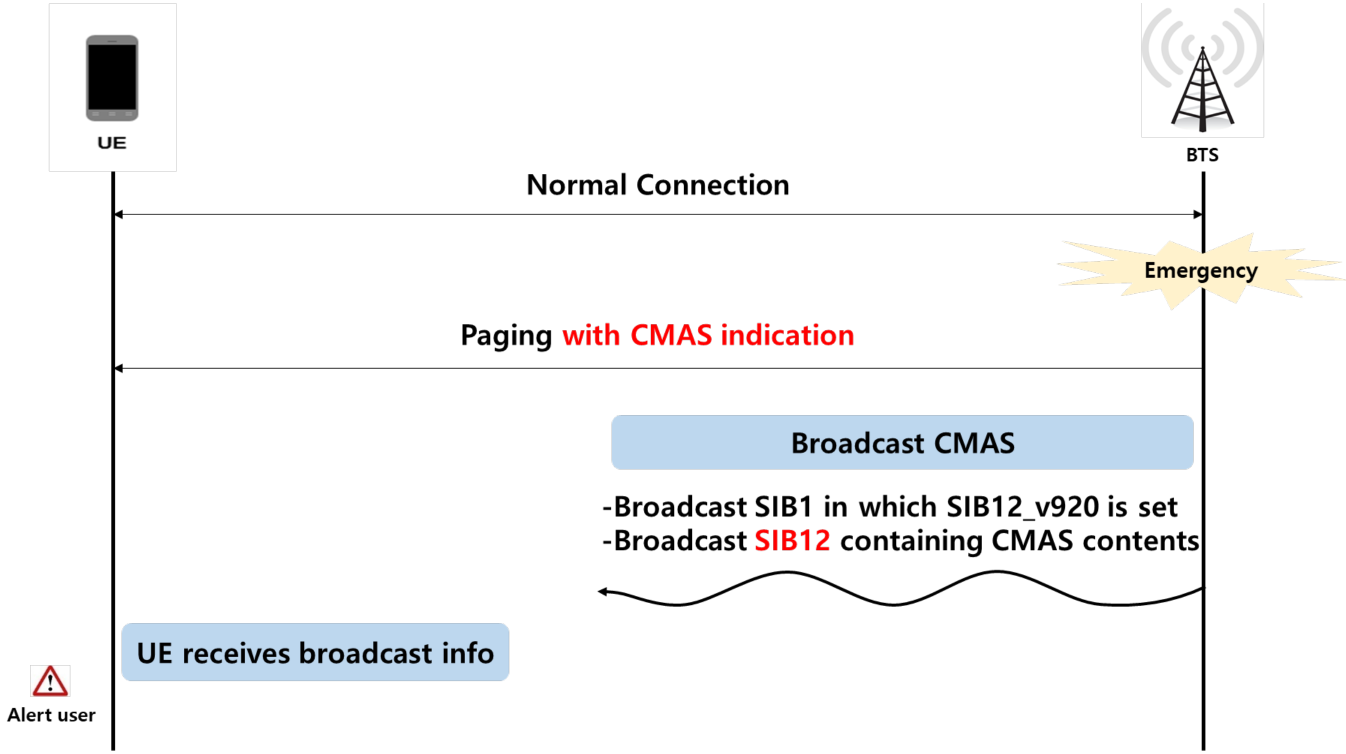
- New Generation (Technology) every 10 years
  - New Standards, Implementation, and Deployment → New vulnerabilities
- Generation overlap: e.g. 3G, LTE and CSFB vulnerabilities in CSFB
- Backward compatibility: e.g. supporting 2G
- Government > Carrier > Device vendors > Customers ☺
- Walled Garden
  - 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 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

Unpatched Design Vulnerabilities

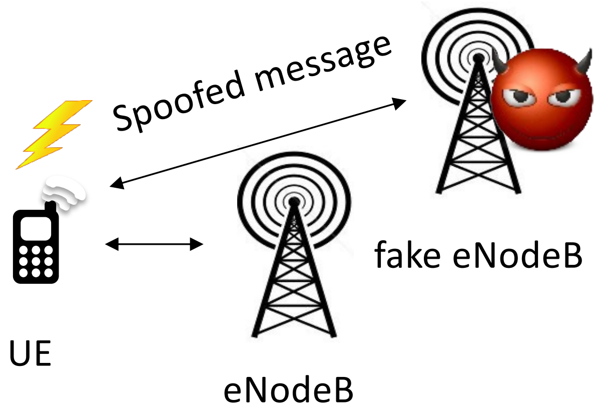
CMAS Protocol



Fake CMAS broadcast attack

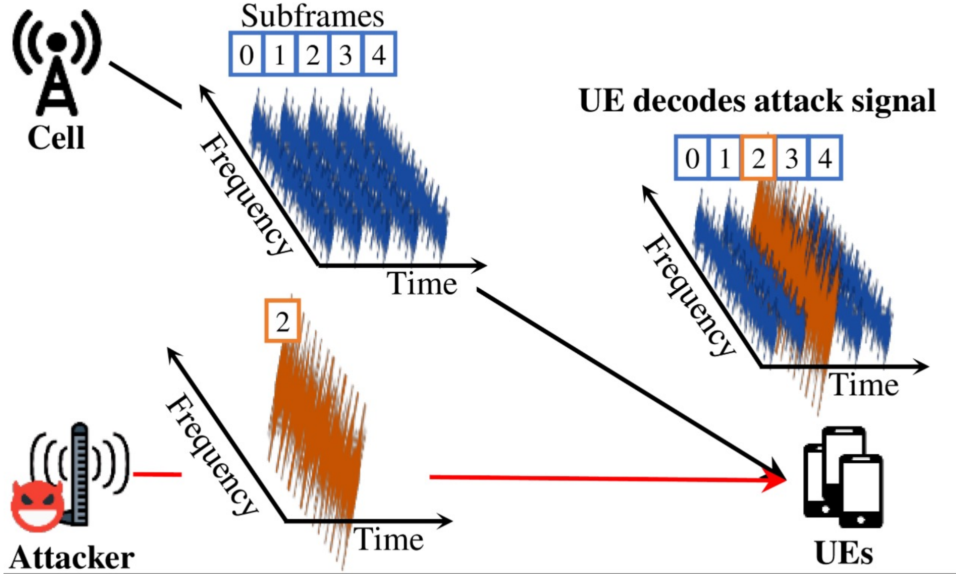
Attacks using SDR based "Fake BTS"

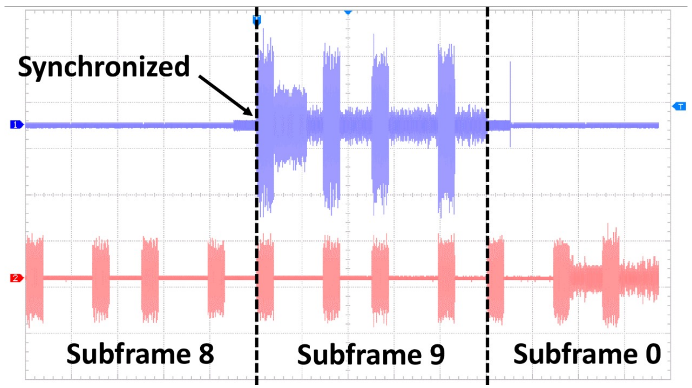
- Exploit physical layer procedure
  - Fake BTS synchronizes with a benign eNodeb, and send spoofed signal to UEs or receive uplink signal from UEs
    - Selective Jamming
    - Malicious data injection
      - e.g. warning message (Emergency SMS), detach message
- Exploit unprotected RRC, NAS Procedure
  - 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





SysSec
System Security Lab

Demonstration of Signal Injection attack

DATA RESTRICTIONS

Cellular Insecurity in Standard

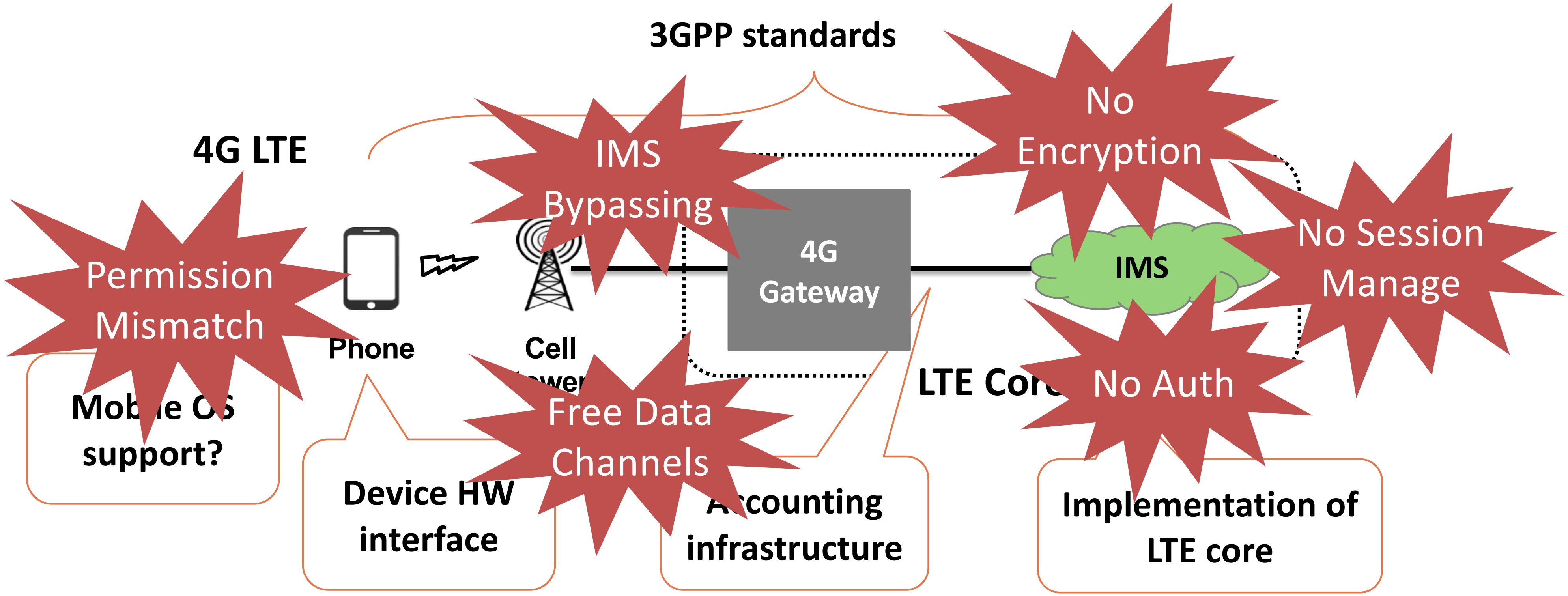
- Unauthenticated broadcast channel
- Roaming networks such as SS7 and Diameter
- Unauthenticated initial messages
- No voice encryption
- Lawful Interception
- Still symmetric key-based key management

- 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

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

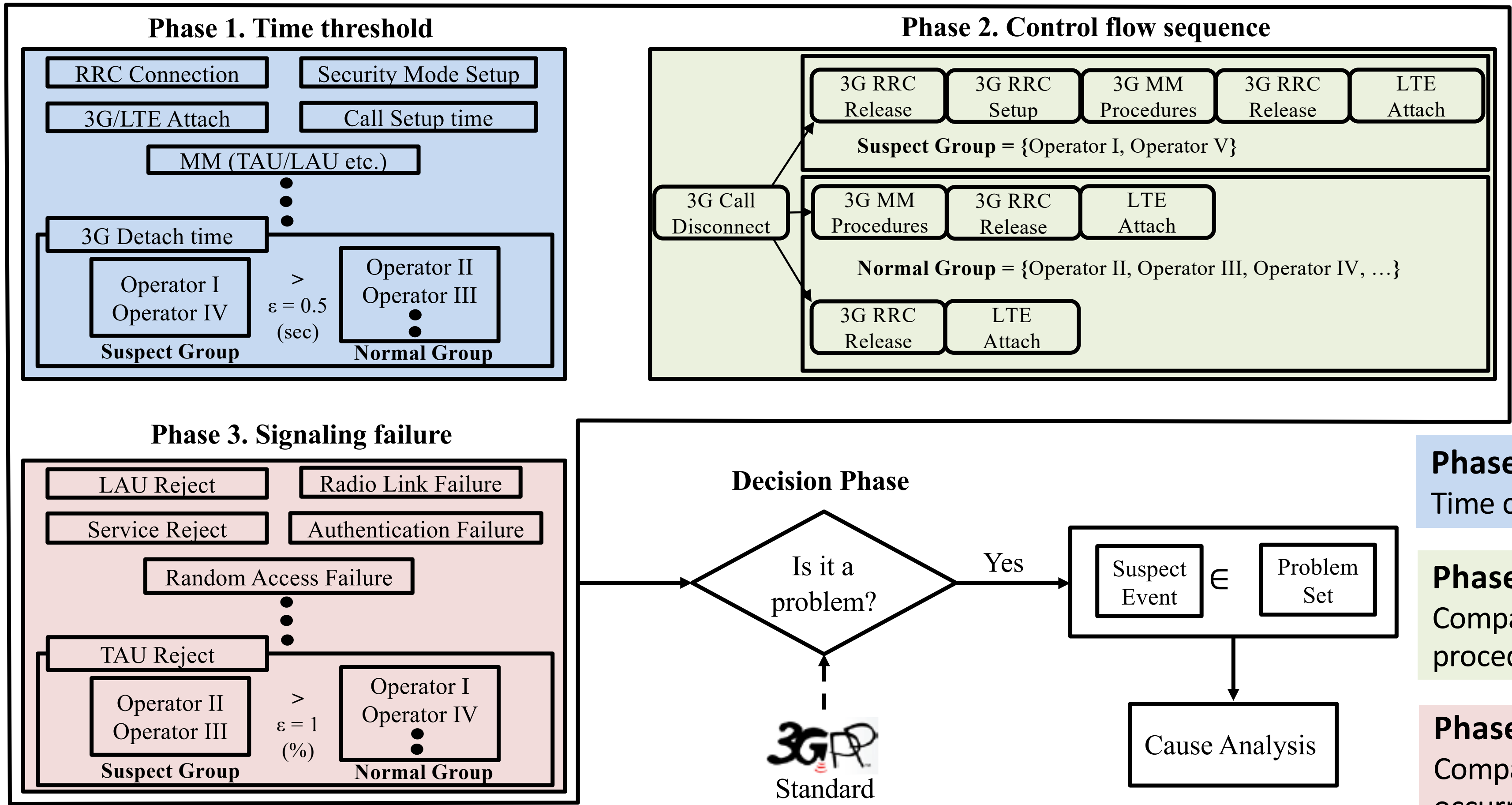
Worldwide Data Collection

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



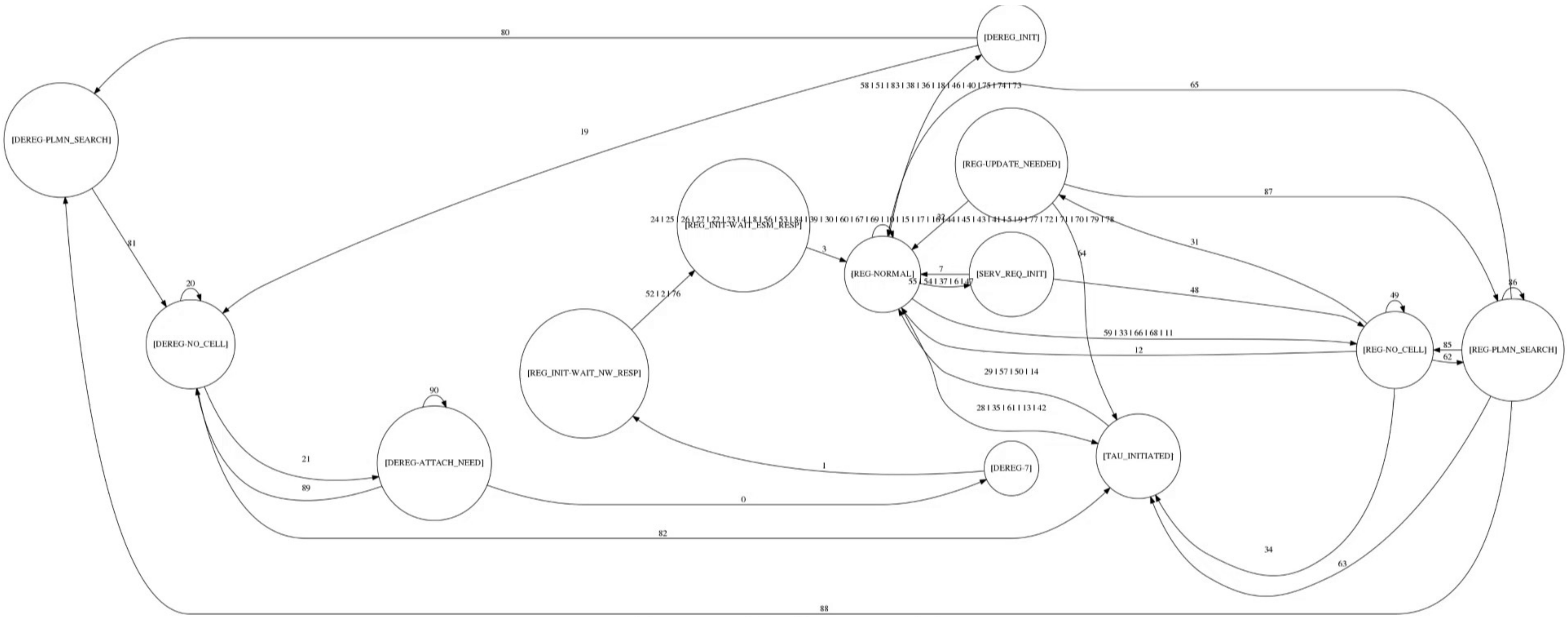
Phase 1
Time comparison by procedure

Phase 2
Comparison of signaling procedure sequence

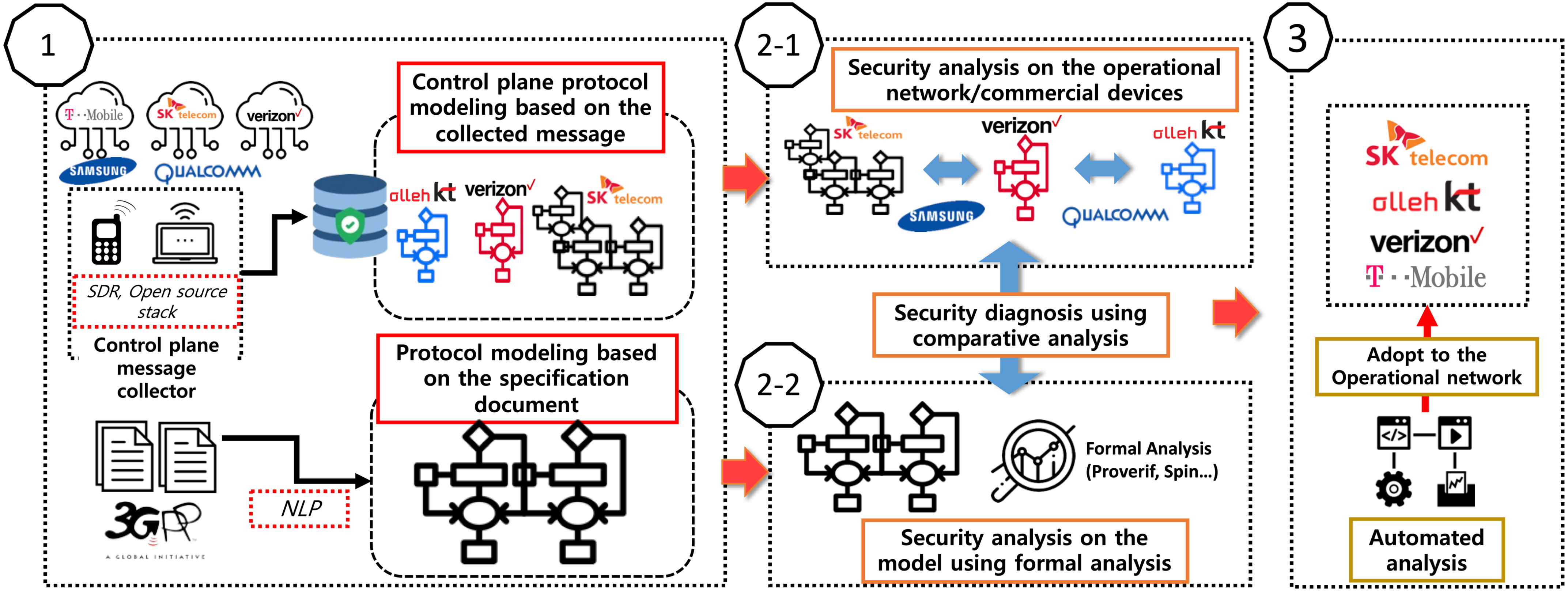
Phase 3
Comparison of signaling failure occurrence probability

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



[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
48
49
86
52 | 2 | 76
[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
90
28 | 35 | 61 | 13 | 42
21
[DEREG-ATTACH_NEED]
[TAU_INITIATED]
1
[DEREG-7]
89
0
82
34
63
88



Phase 1: Protocol modeling

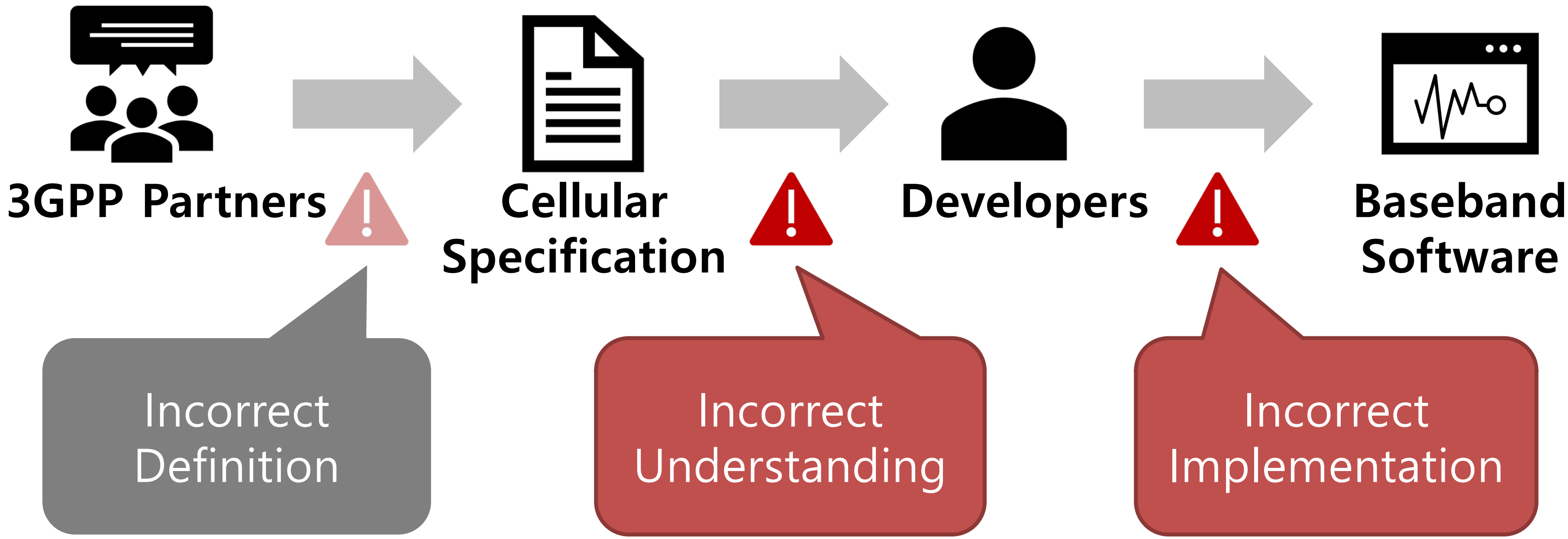
Phase 2: Security analysis

Phase 3: Verification

BaseSpec: Comparative Analysis of Baseband Software and Cellular Specifications

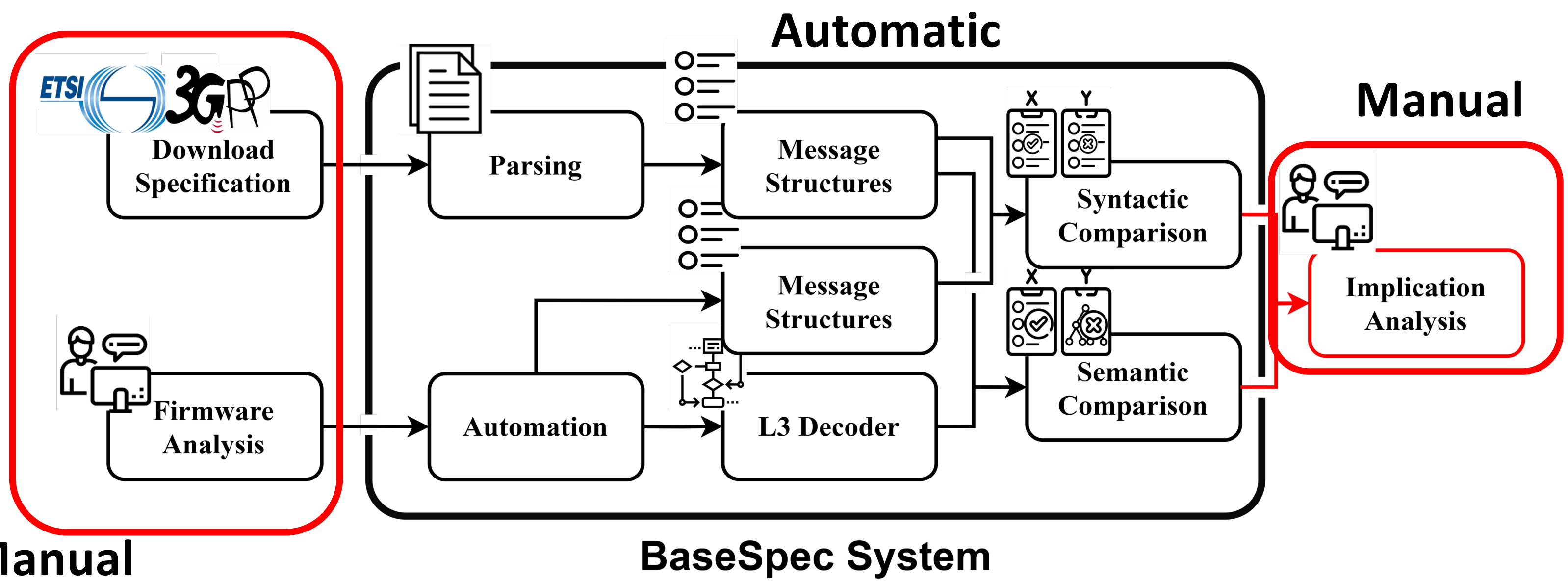
Errors in Protocol Implementation

❖ Many points of **human errors** in development process



BaseSpec Overview

1. Extract message structures from the specification documents
2. Extract message structures and decoder information from the firmware
3. Syntactically, 4. Semantically compare them
5. Report the mismatch results



Mismatch Results (vendor x)

- Missing Mismatches of mandatory IE & Unknown Mismatches
  - Directly indicate **functional errors** (drop of benign IE / undefined behavior)
- Invalid Mismatches
  - Numerous incorrect length limit / ad-hoc length checkers
  - Can lead to **memory-related bugs**
- Missing optional IEs
  - May not be buggy

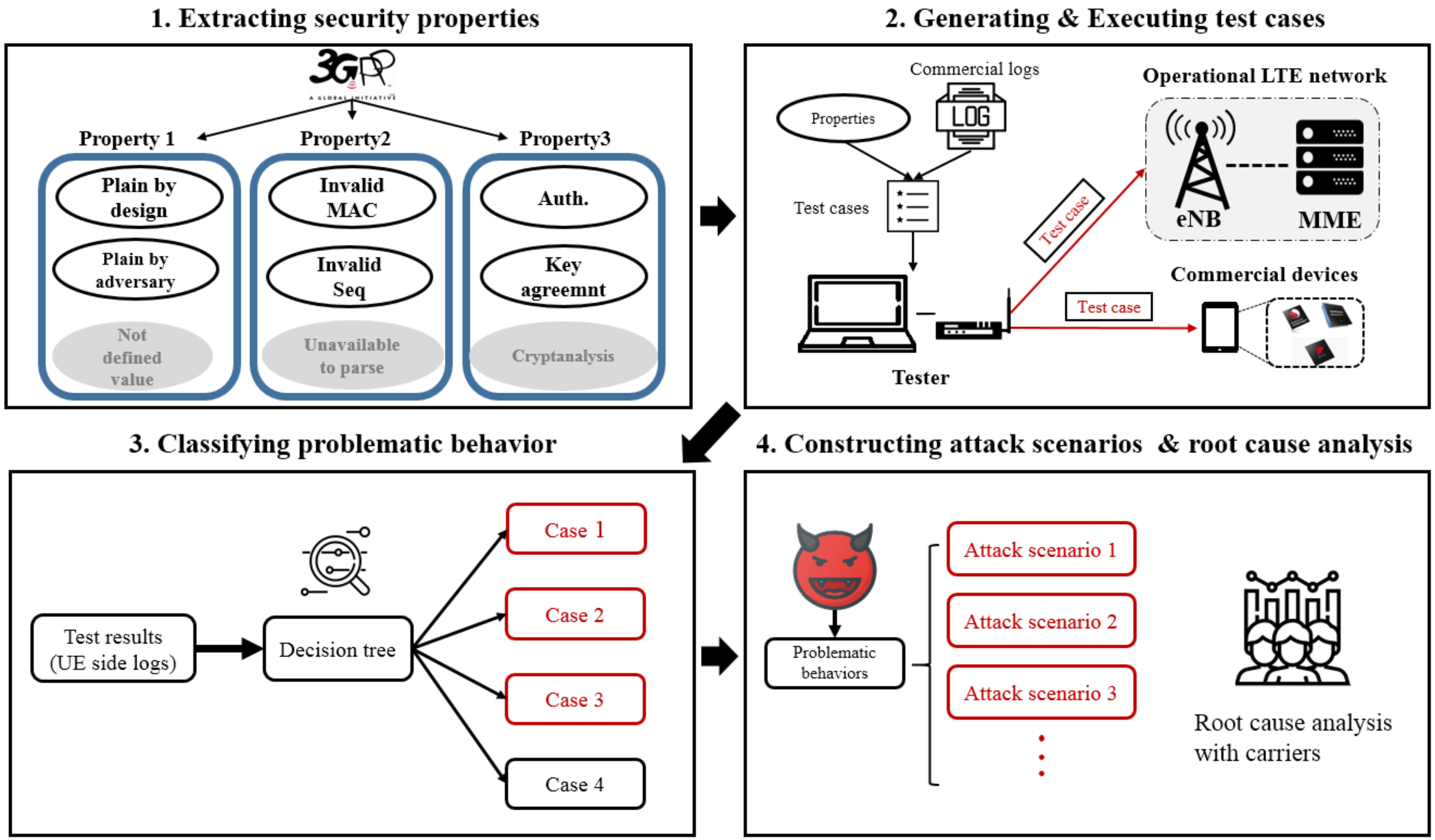
9 Error cases
(4 Memory-related including 2 RCEs)

		Missing Mismatch		Unknown Mismatch		Invalid Mismatch	
Models	Total IEs	Mandatory IE	Optional IE	Mandatory IE	Optional IE	Mandatory IE	Optional IE
Model A	1475	5	189	6	58	94	364
Model B	1475	5	192	6	58	94	361
Model C	1475	5	192	6	58	94	361
Model D	1475	5	203	6	58	94	349
Model E	1475	5	203	6	58	94	349

*IE: Information Element (= message field)

Fuzzing LTE Core and Baseband

LTEFuzz


1. Extracting security properties
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
Properties
LOG
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

Specification issues

Vendor issues

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

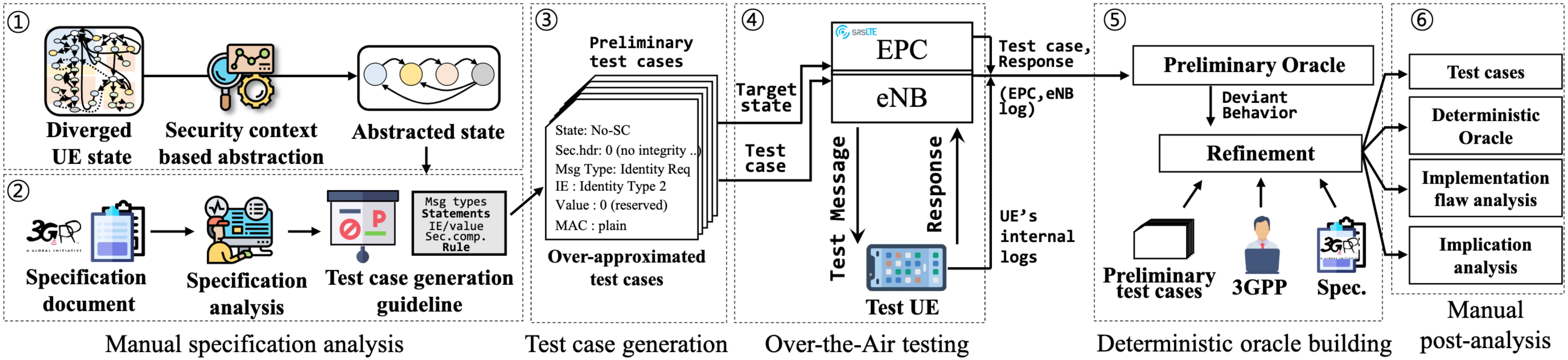
Negative Testing

- ❖ Conformance testing → check if valid messages are correctly handled

- ❖ Negative testing?
  - check if invalid or prohibited messages are appropriately handled
  - Among 993 test scenarios in conformance spec, only 14 cases are negative.

  - Challenges
    - How do we enumerate violating cases?
    - UE/Network state dependence
    - Spec is difficult to understand → Oracle?
    - Baseband/UE implementation diversity

DoLTEst



①
Diverged UE state
Security context based abstraction
Abstracted state
②
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
Target state
Test case
EPC
eNB
Test Message
Response
Test UE
Test case, Response
(EPC, eNB log)
UE's internal logs
Over-the-Air testing
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

1	iPhone 6	Apple	Qualcomm	MDM9625	7.21.00 / 7.80.04	1810/2101	S1,S3,I1 / S2,S3,I1
2	iPhone 8	Apple	Intel	XMM 7480	4.02.01	2103	I3
3	iPhone XS	Apple	Intel	XMM 7560	1.03.08	1902	I3
4	iPhone 12 Pro	Apple	Qualcomm	Snapdragon X55	1.62.11	2104	-
5	Y9	Huawei	HiSilicon	Kirin 659	21C60B269S003C000	1806	S3,I3
6	P10 Lite	Huawei	HiSilicon	Kirin 658	21C60B268S000C000	1711	I3
7	P10	Huawei	HiSilicon	Kirin 960	21C30B323S003C000	1805	I3
8	Mate 10 Pro	Huawei	HiSilicon	Kirin 970	21C10B551S000C000	1801	I3
9	P20 pro	Huawei	HiSilicon	Kirin 970	21C20B369S007C000	1904	I3
10	Mate 20 pro	Huawei	HiSilicon	Kirin 980	21C10B687S000C000	1812	I3
11	X401	LG	Mediatek	MT6750	MOLY.LR11.W1552.MD.TC01.LVSF.SP.V1.P22	1802	S2,M1
12	X6	LG	Mediatek	Helio P22 MT6762	MOLY.LR12A.R3.TC01.PIE.SP.V1.P10.T12	1907	S2
13	K50	LG	Mediatek	Helio P22 MT6762	MOLY.LR12A.R3.TC01.PIE.SP.V1.P26	2012	S2
14	G6	LG	Qualcomm	MSM8996 Snapdragon 821	MPSS.TH.2.0.1.c3.1-00024-M8996FAAAANAZM-1.142344.1.143233.1	1804	S1,S2,S3
15	V35 ThinQ	LG	Qualcomm	SDM845 Snapdragon 845	MPSS.AT.4.0.c2.9-00057-SDM845_GEN_PACK-1	1901	S1,S2
16	G7 ThinQ	LG	Qualcomm	SDM845 Snapdragon 845	MPSS.AT.4.0.c2.9-00088-SDM845_GEN_PACK-1.299473	2008	S2
17	G8 ThinQ	LG	Qualcomm	SM8150 Snapdragon 855	MPSS.HE.1.0.c4-00104-SM8150_GEN_PACK-1	2101	S2
18	V50	LG	Qualcomm	SM8150 Snapdragon 855	MPSS.HE.1.5.c4-00270.1-SM8150_GENFUSION_PACK-1.215515.14	1909	S2
19	Oppo find X	OPPO	Qualcomm	SDM845 Snapgragon 845	Q_V1_P14,Q_V1_P14	1808	S1
20	Galaxy S4	Samsung	Qualcomm	MSM8974 Snapdragon 800	E330KKKUCNG5	1609	S1,S2,S3,M1,M2,I1,I2,I3
21	Galaxy S5	Samsung	Qualcomm	MSM8974AC Snapdragon 801	G900VVRU1ANI2	1411	S1,S3,M1,M2,I2
22	Galaxy S5 A	Samsung	Qualcomm	APQ8084 Snapdragon 805	G906LKLU1CPK2	1612	S1,S2,S3,M2,I1,I2,I3
23	Galaxy Note5	Samsung	Samsung	Exynos 7 (7420)	N920SKSU2DQH2	1708	S2,M1,I2
24	Galaxy S6	Samsung	Samsung	Exynos 7 (7420)	G920SKSU3EQC9	1704	S2,M1,I3
25	Galaxy Note FE	Samsung	Samsung	Exynos 8 (8890)	N935JJJU4CTJ1	2102	S2,M1
26	Galaxy Note8	Samsung	Samsung	Exynos 9 (8895)	N950NKOU4CRH2	1810	S2,M1
27	Galaxy S8	Samsung	Qualcomm	MSM8998 Snapdragon 835	G950U1UES5CSB2	1902	S1,S2,S3
28	Galaxy Note9	Samsung	Samsung	Exynos 9 (9810)	N960NKOU3DSLA	1912	S2,M1
29	Galaxy S10	Samsung	Samsung	Exynos 9 (9820)	G977NKOU2BTA2 / G977NKOU4DK1	2001/2011	S2,M1,I1,I2 / S2,M1,I1
30	Galaxy S10	Samsung	Qualcomm	SM8150 Snapdragon 855	G977UVRS3YSJK	1911	-
31	Galaxy A31	Samsung	Mediatek	Helio P65 MT6768	A315NKOU1BUA1	2102	S2
32	Galaxy S20	Samsung	Qualcomm	SM8250 Snapdragon 865	G981NKSU1CTKD	2011	-
33	Galaxy A71	Samsung	Samsung	Exynos 9 (980)	A716SKSU1ATF4 / A716SKSU3BTL2	2006/2012	S2,M1,I1,I2 / S2,M1,I1
34	Galaxy Note20	Samsung	Qualcomm	SM8250 Snapdragon 865	N986NKSU1CUC9	2103	-
35	Redmi 5	Xiaomi	Qualcomm	SDM450 Snapdragon 450	MPSS.TA.2.3.c1-00522-8953_GEN_PACK-1_V042	1712	S1,S3
36	Redmi note 4x	Xiaomi	Qualcomm	MSM8953 Snapdragon 625	953_GEN_PACK-1.122638.1.123338.1	1712	S1,S3
37	Mi Max 3	Xiaomi	Qualcomm	SDM636 Snapdragon 636	AT32-00672-0812_2359_46aa9a7	1807	S1
38	Mi 5S	Xiaomi	Qualcomm	MSM8996 Snapdragon 821	TH20c1.9-0612_1733_9fe7ce8	1805	S1,S3
39	Mi Mix 2	Xiaomi	Qualcomm	MSM8998 Snapdragon 835	AT20-0608_2116_6c4a86b	1805	S1,S3
40	Black Shark	Xiaomi	Qualcomm	SDM845 Snapdragon 845	00888-SDM845_GEN_PACK-1.163713.1	1811	S1
41	POCOphone F1	Xiaomi	Qualcomm	SDM845 Snapdragon 845	AT4.0.c2.6-144-1008_1436_e3055ba	1809	S1
42	ZTE Blade V8 Pro	ZTE	Qualcomm	MSM8953 Snapdragon 625	-8953_GEN_PACK-1.79091.1.79899.1	1612	S1,S3
43	ZTE Axon 7	ZTE	Qualcomm	MSM8996 Snapdragon 820	TH.2.0.c1.9-00104-M8996FAAAANAZM	1712	S1,S3

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"