Cellular Security
- What can we expect for 5G? -

Yongdae Kim

KAIST
SysSec Lab

SysSec Lab.

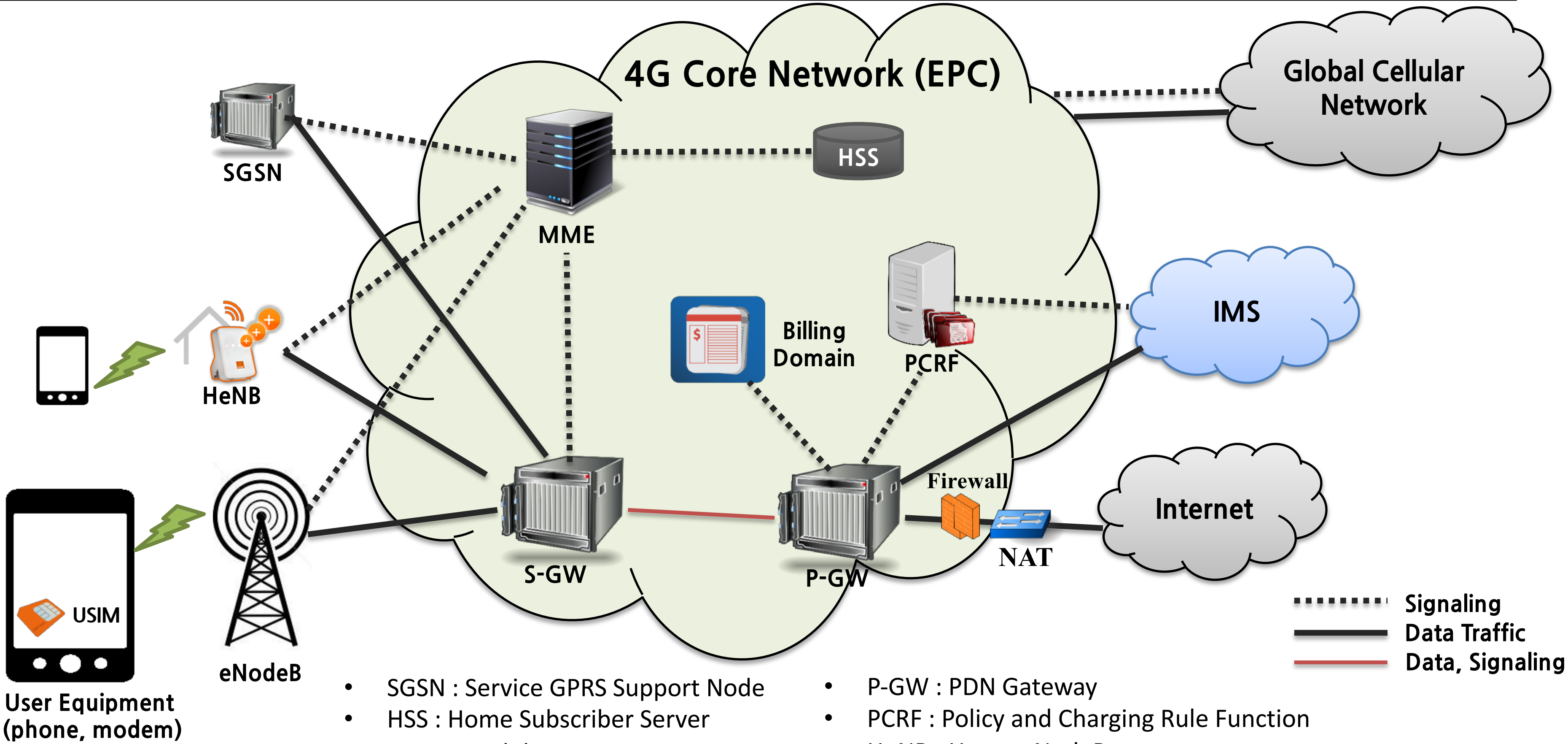
- System Security Lab. @ KAIST, Korea
  - Yongdae Kim
  - Prof @ Electrical Engineering & Information Security
  - Director @ Cyber Security Research Center

- Research areas: Hacking Emerging Technologies such as IoT, Drone, Blockchain, Medical device, Automobiles, Critical Infra, Cellular, …
  - Software vulnerability (hacking)
  - Physical cyber system security (sensor, hardware Trojan, …)
  - Wireless communication security (Bluetooth, Zigbee, …)
  - Mobile network security (privacy, abuse, …)

Cellular Security Publications (Selected)

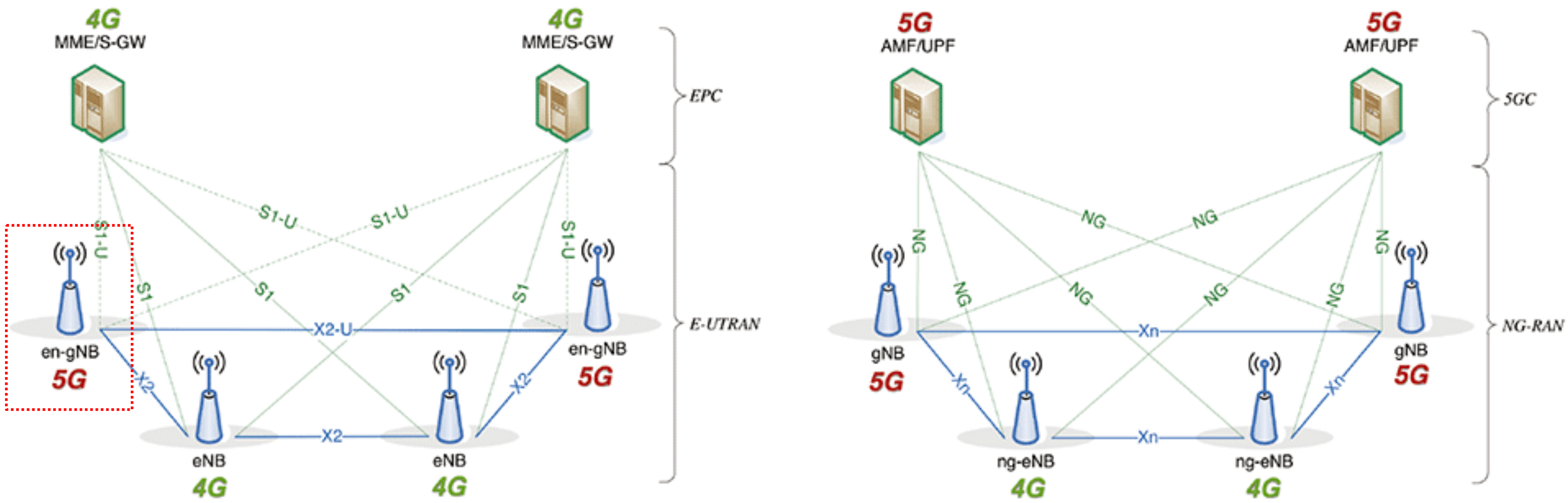
- Location leaks on the GSM Air Interface, ISOC NDSS'12
- Gaining Control of Cellular Traffic Accounting by Spurious TCP Retransmission, NDSS' 14
- Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations, ACM CCS'15
- When Cellular Networks Met IPv6: Security Problems of Middleboxes 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 Transactions on Mobile Computing, Vol. 17, No. 10, 2018
- Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane, IEEE S&P 2019
- Hidden Figures: Comparative Latency Analysis of Cellular Networks with Fine-grained State Machine Models, HotMobile 2019
- Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE, Usenix Security 2019

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



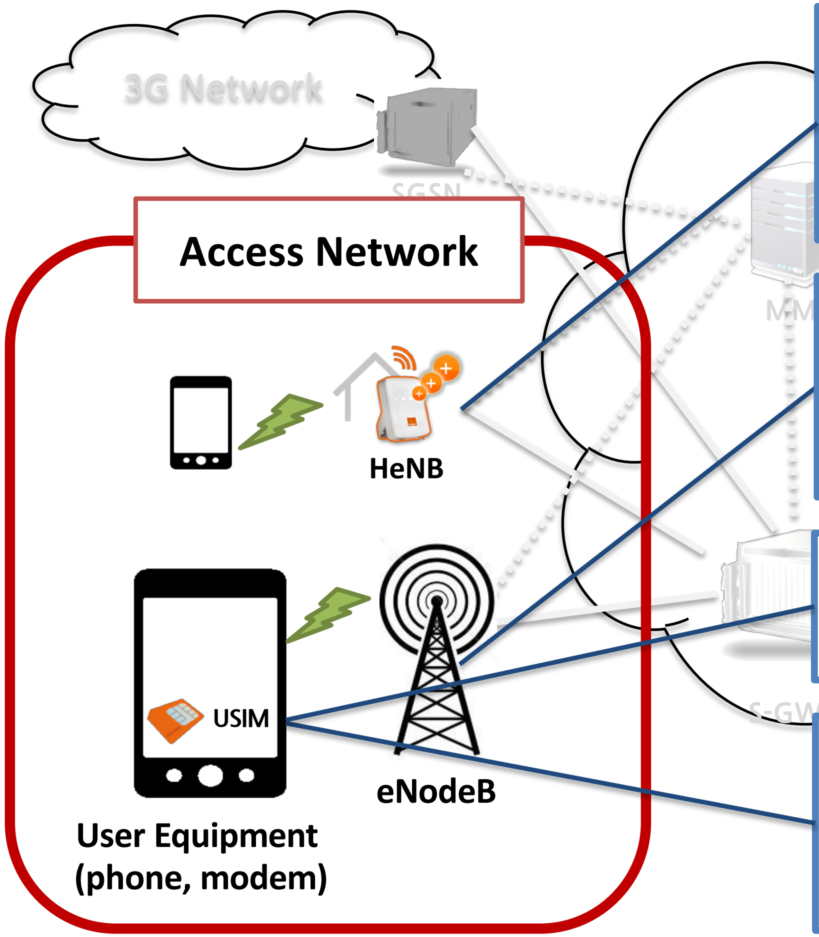
gNB (Next generation NodeB), eNB (Evolved Node B), MME (Mobility Management Entity), SPGW (Serving/Packet data network Gateway), HSS (Home Subscriber Server), IMS (IP Multimedia Subsystem)

5G Security?

- From control plane security point of view, 5G NSA = 4G LTE!
- Still long time left before 5G SA.
- So let's review 4G LTE security for now.

- 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

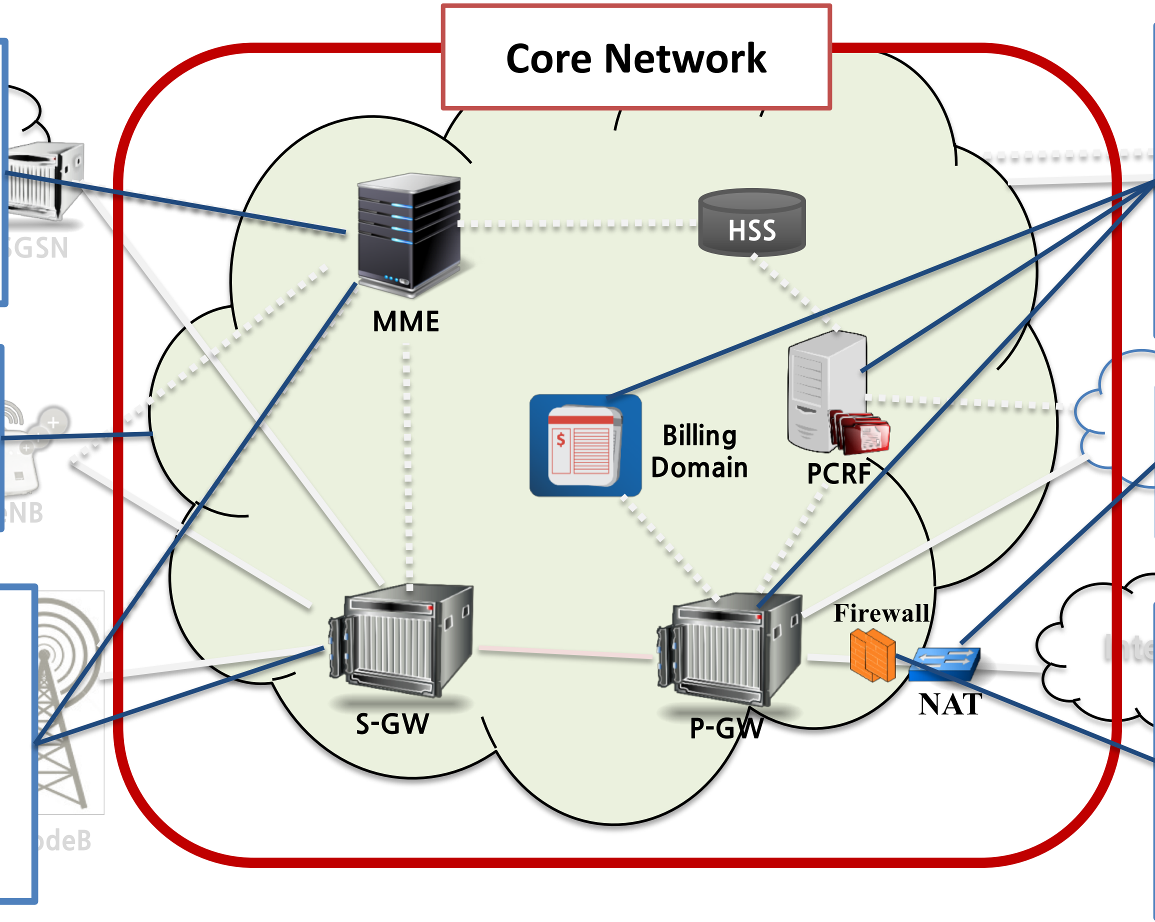
- Reading privacy info. (SMS, Phonebook, cell location)
- Get an authentication vector
- Exploit other applets

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

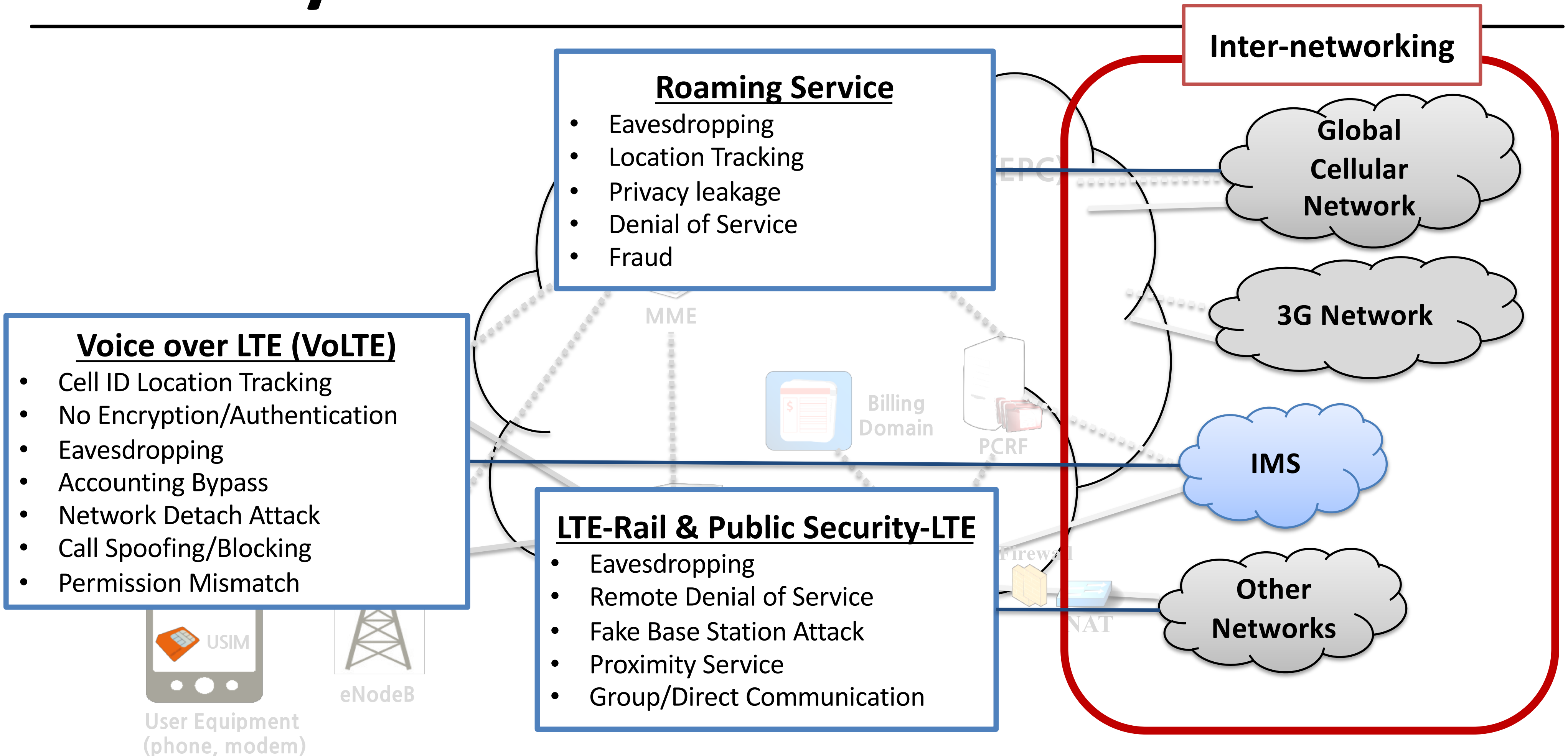


Charging policy
- Overbilling
- Free riding
  - ✓ Zero rating protocol
  - ✓ TCP Retransmission

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?

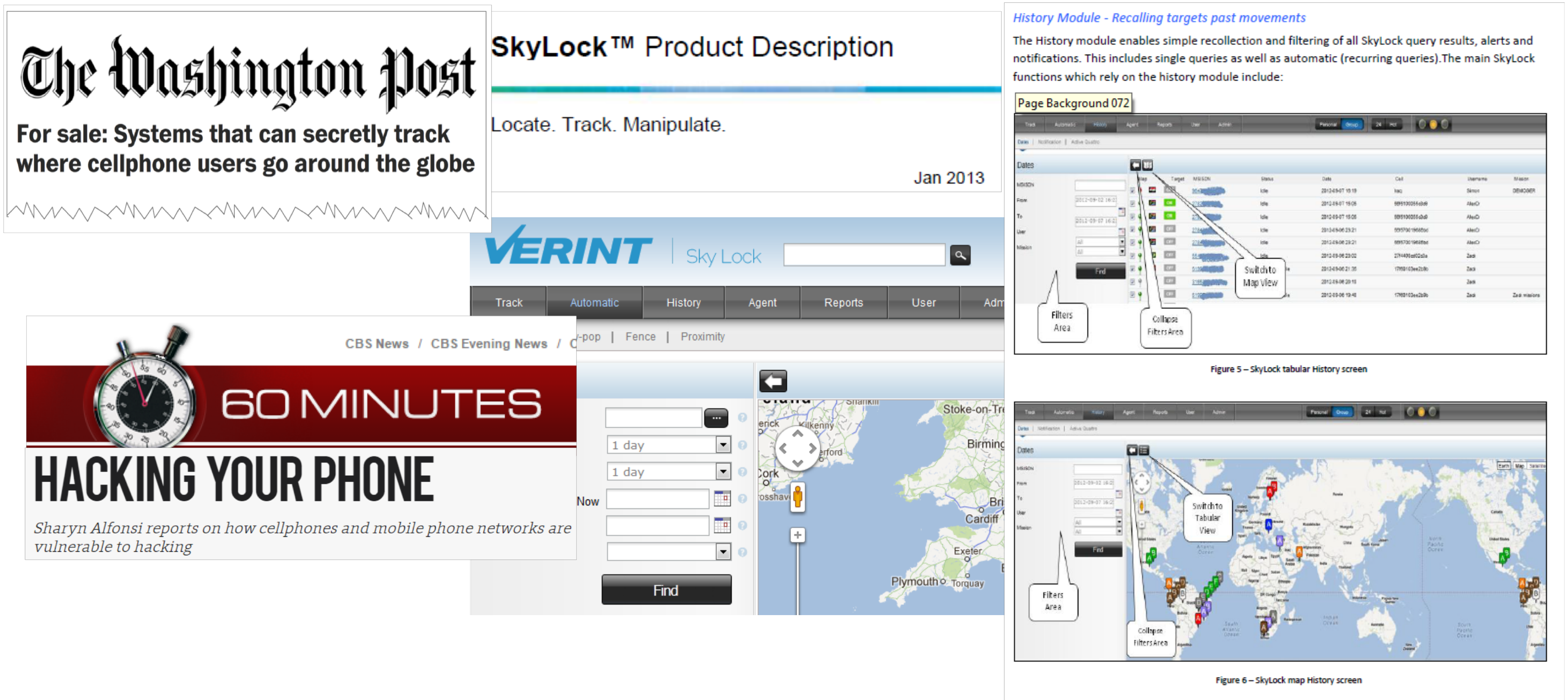
- New Generation (Technology) every 10 year
  - New Standards, Implementation, and Deployment ➔ New vulnerabilities
- Many standard vulnerabilities have not been patched.
  - Backward compatibility
- Generation Overlap, e.g. LTE CSFB, 5G NSA
  - CSFB: 3G, LTE and CSFB vulnerabilities
- Cellular networks are different from each carrier and manufacturer in terms of implementations and configurations
  - Therefore, vulnerabilities are different ➔ Need for global analysis
- Device manufacturers tend to follow carrier's requirement.
- Walled Garden
  - Carriers (smartphone vendors) don't talk to each other about their problem.
  - One vulnerability from a carrier will appear in other carriers.

Cellular Security: Special Circumstances

- 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
- Multiple protocols co-work, but written in separate docs ➔ Analysis complexity
- Most of the cellular security analyses have been manual.
- New HW/SW tools are needed for each generation.
  - Slow/imperfect open-source development
- Serious silo effect in carriers, and device vendors

Security Problems in Standard

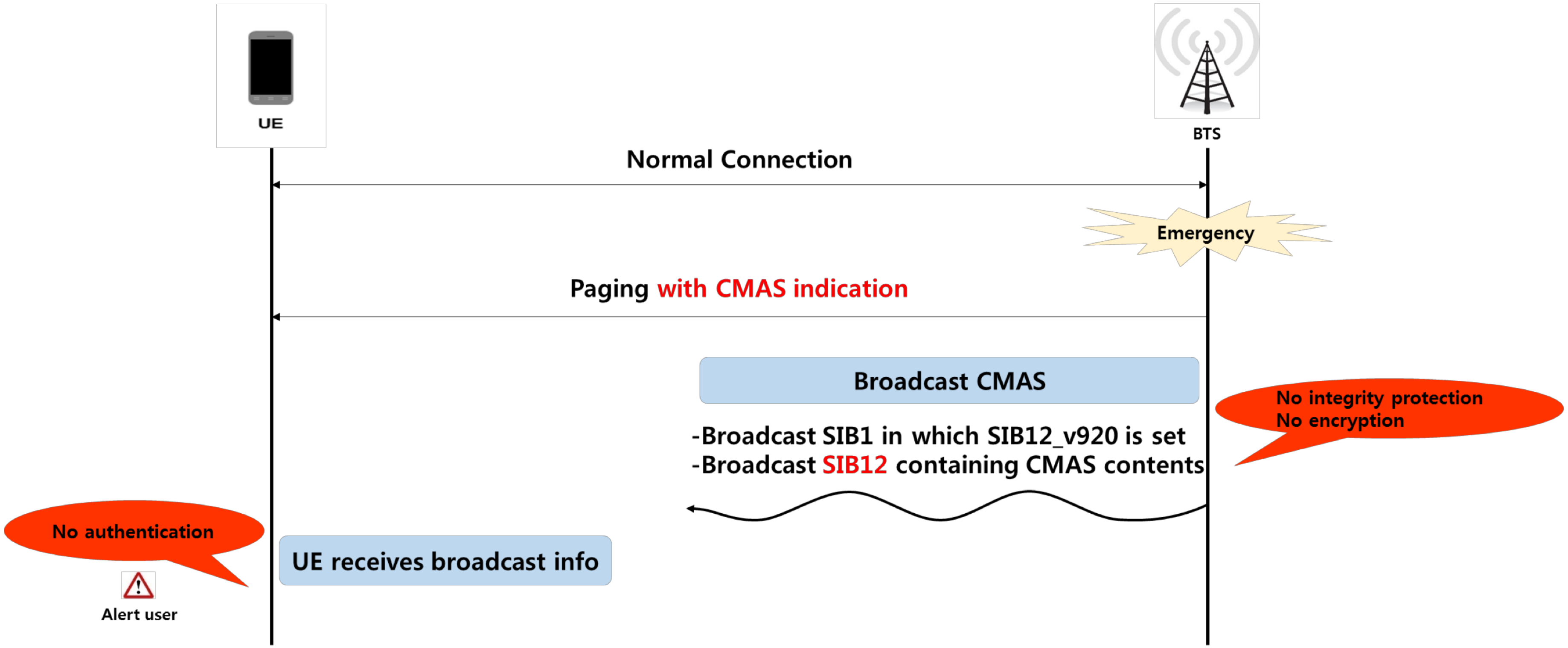
Roaming network is insecure.



Results of Security Measurement

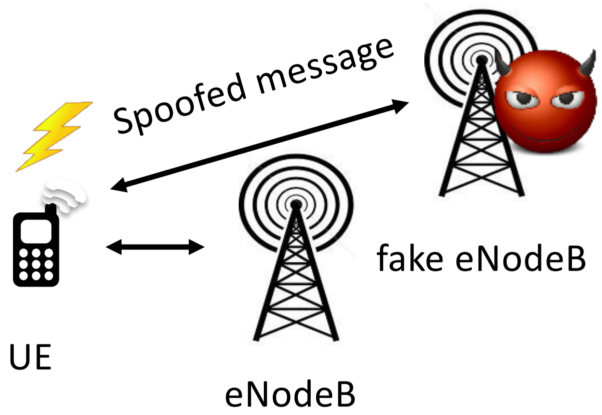
MAP message	*Threat Category*	*Target*	*Prerequisites*
updateLocation	***DoS, Interception***	***All the subscriber***	***IMSI***
cancelLocation	*DoS*	*Roaming subscriber*	*IMSI*
purgeMS	*DoS*	*Roaming subscriber*	*IMSI*
insertSubscriberData deleteSubscriberData	*DoS*	*Roaming subscriber*	*IMSI and MSISDN*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

Broadcast messages (CMAS)



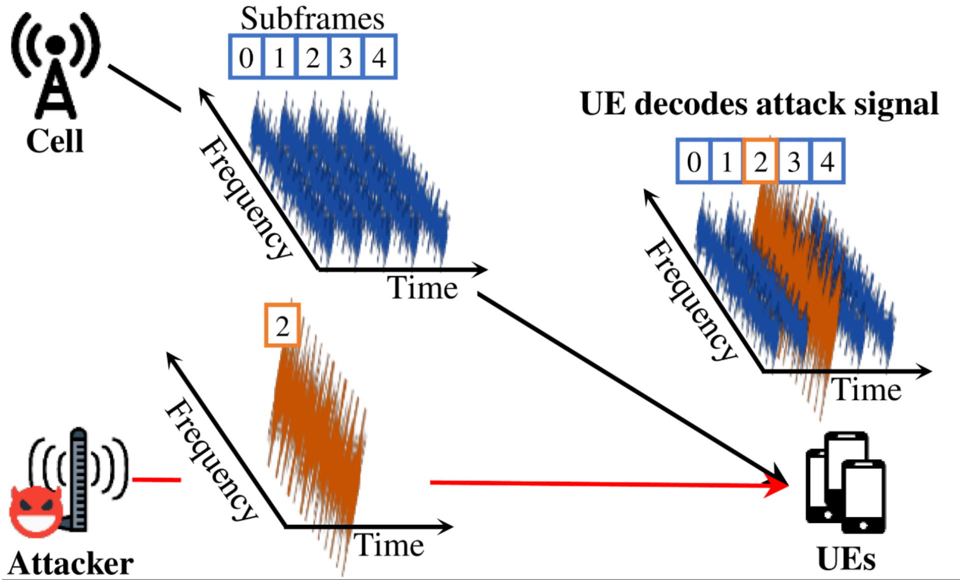
Attacks using SDR based "Fake BTS"

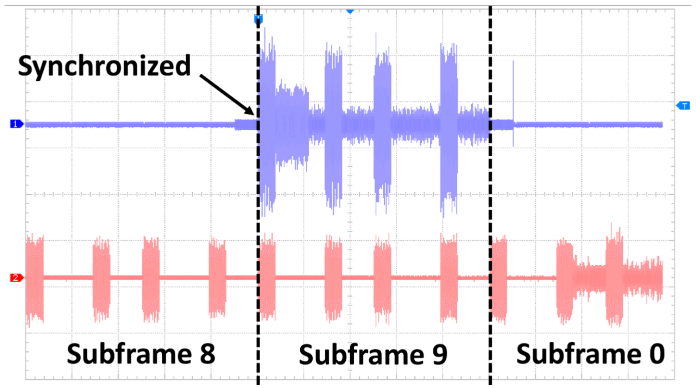
- Exploit physical layer procedure
  - Fake BTS synchronizes with a benign eNodeb, and send spoofed signal to UEs or receive uplink signal from UEs
    - Selective Jamming
    - Malicious data injection
      - e.g. warning message (Emergency SMS), detach message



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





Attack Efficiency (Power)

Relative Power (dB)	1	3	5	7	9
SigOver	38%	98%	100%	100%	98%

Relative Power (dB)	25	30	35	40	45
FBS attack	0%	0%	80%	100%	100%

FBS consumes x5000 more power
to achieve a comparable attack success rate

Demonstration of Signal Injection attack

DATA RESTRICTIONS

Cellular Insecurity in Standard

- Broadcast Channel
- Roaming Network such as SS7 and Diameter
- No voice encryption
- Lawful Interception

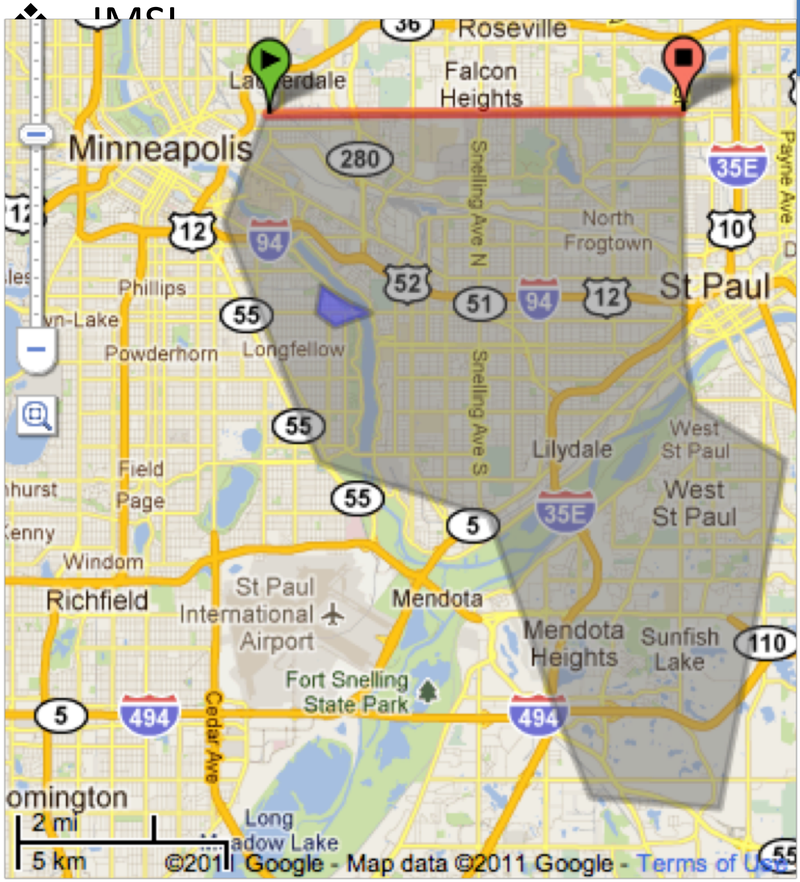
- Suppose you implement cellular network (e.g. 6G) from scratch, would you design with these insecurities?

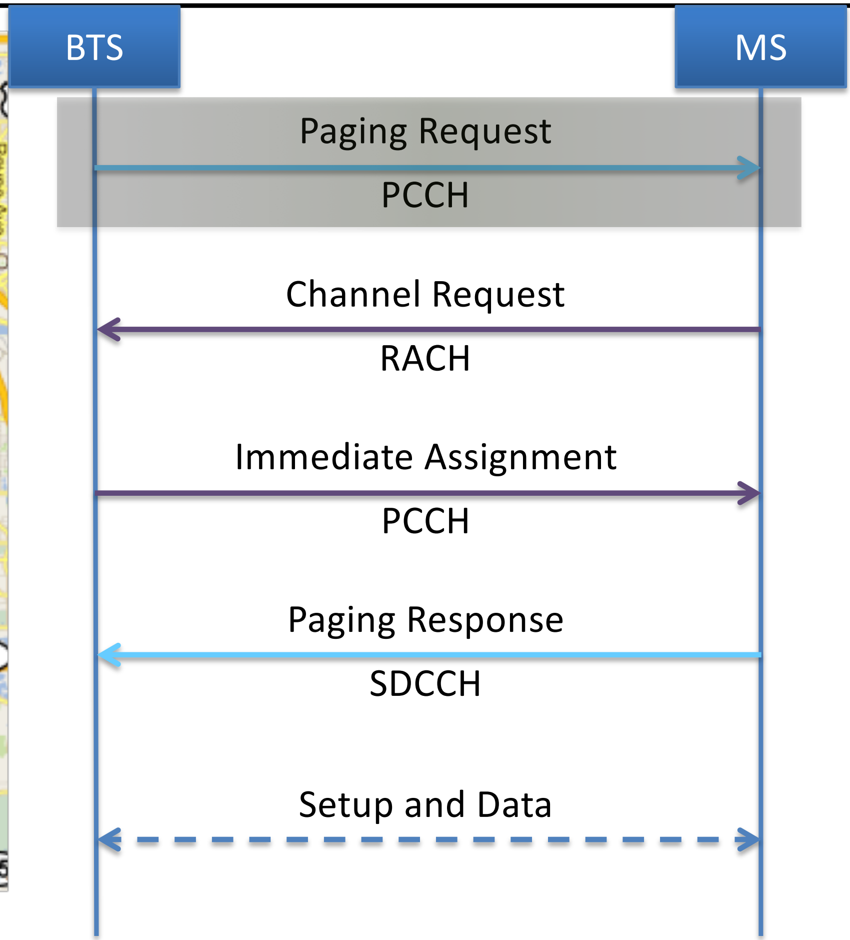
Security Problems in ISPs

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

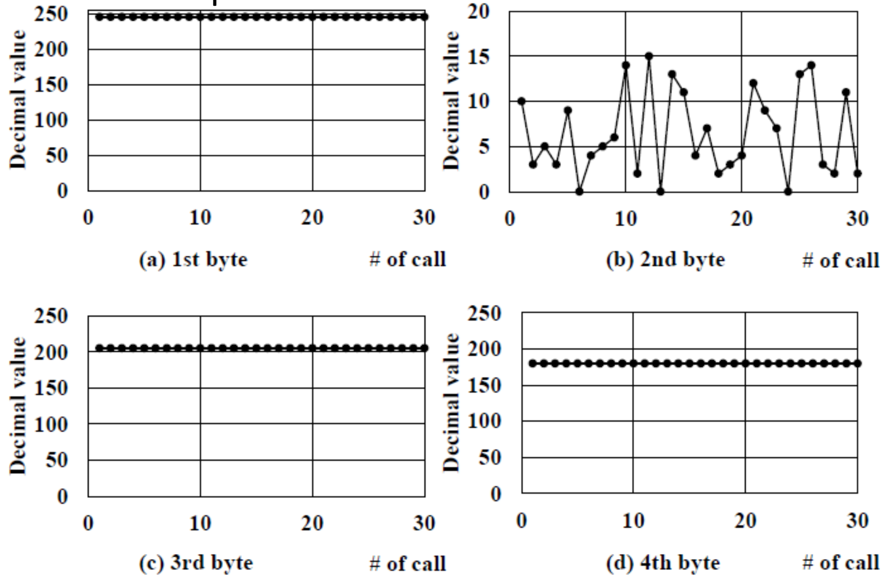




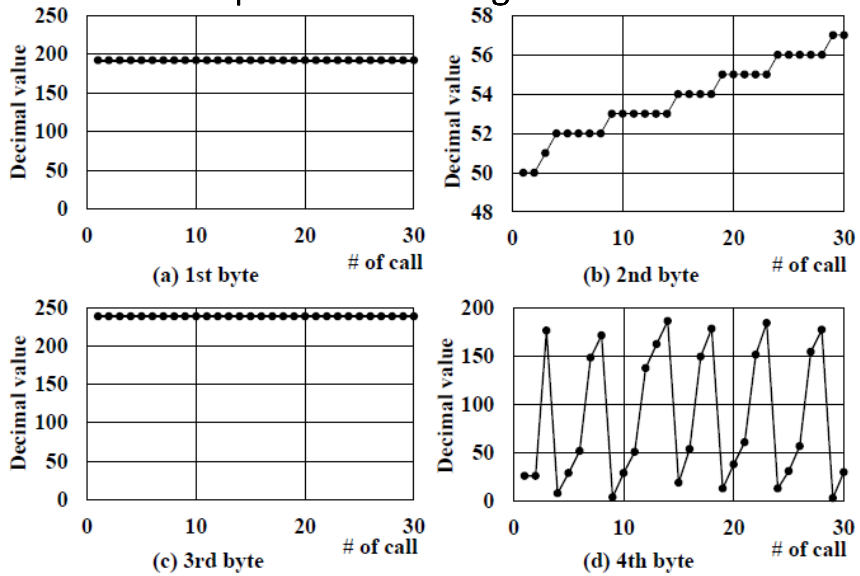
Vulnerabilities in Deployed ID Management

- 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

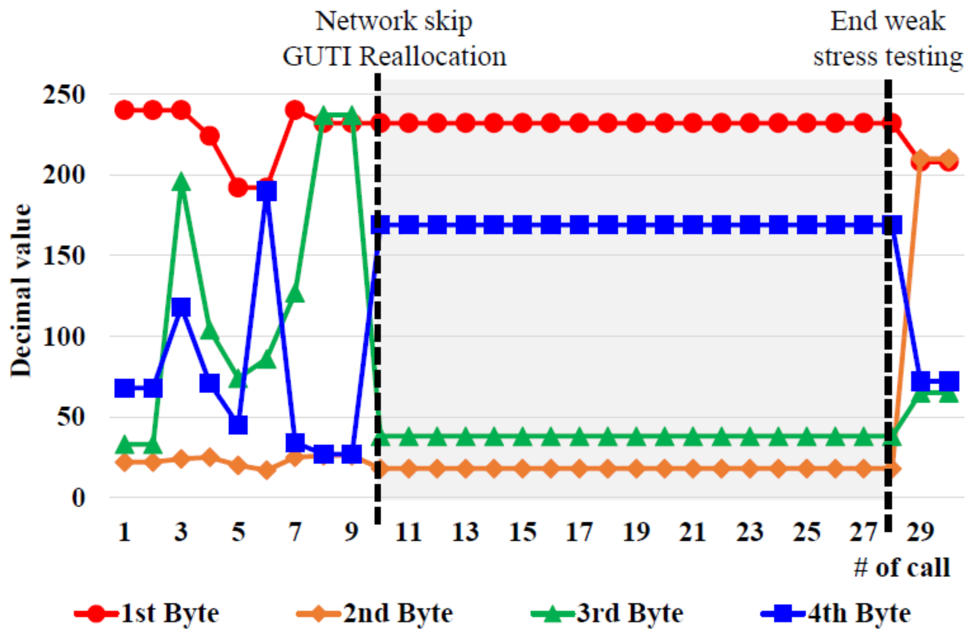
AT: Austria, BE: Belgium, CH: Switzerland, DE: Germany, ES: Spain, FR: France, JP: Japan, NL: Netherlands

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

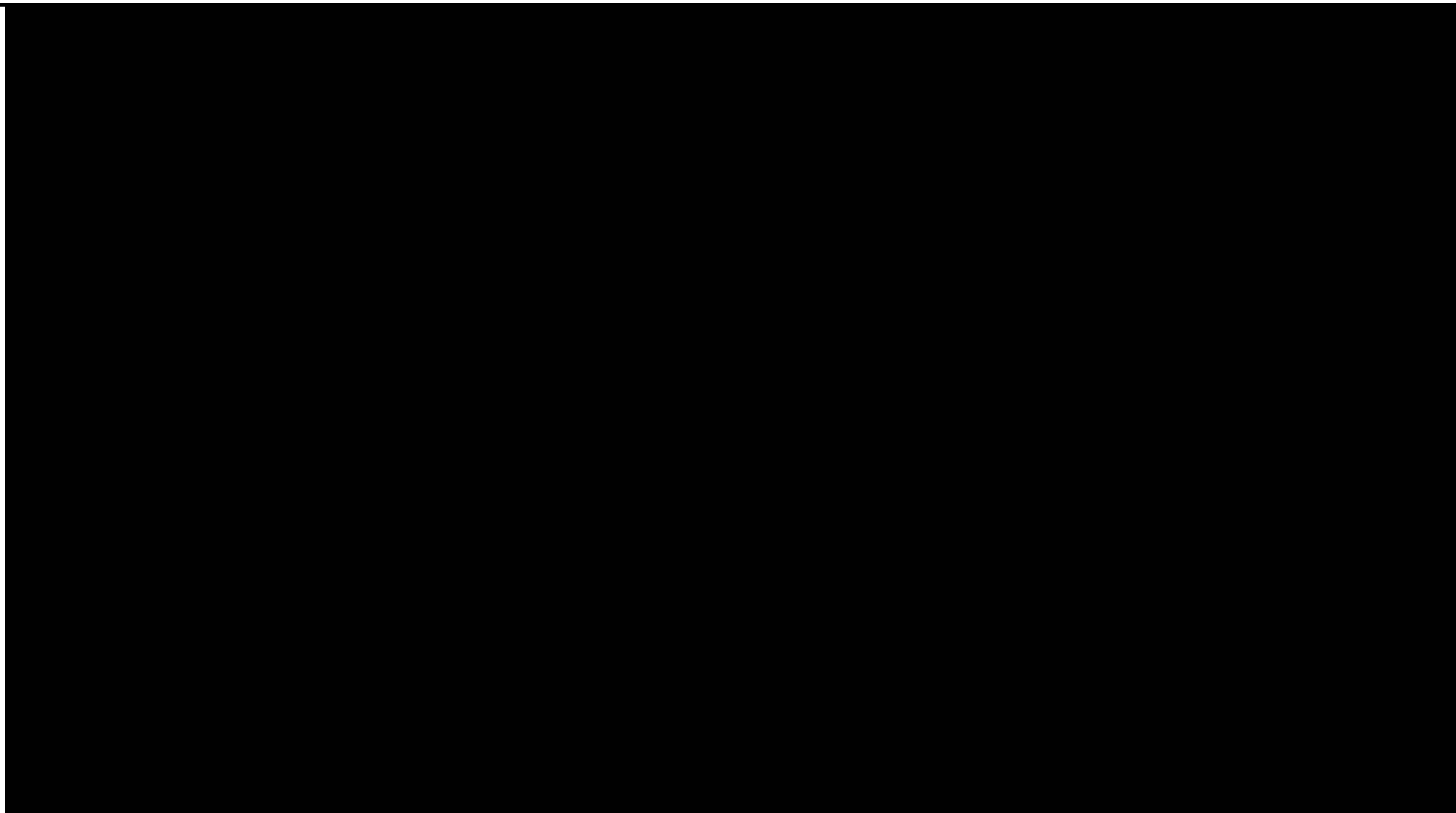
O: Network skips the *GUTI Reallocation*
X: No noticeable change



Charging Policy Summary

Tunneling Method	SKT	KT	LG U+	AT&T	Verizon	T-mobile	Direction
ICMP Echo request (phone to Internet)	**Not Charged**	**Not Charged**	**Not Charged**	Charged	Charged	Charged	Up /down
ICMP Echo request (phone to phone)	Blocked	Blocked	**Not Charged**	Blocked	Blocked	Charged	Up /down
ICMP Unreachable (Internet to phone, TCP)	**Not charged but limited**	**Not Charged**	**Not Charged**	Charged	Blocked	Charged	down
ICMP Unreachable (Internet to phone, UDP)	**Not charged but limited**	**Not Charged**	**Not Charged**	Charged	Blocked	Charged	down
IGMP (phone to Internet)	**Not Charged**	Blocked	Blocked	-	-	-	up
Syn with payload (phone to Internet)	**Not Charged**	**Not Charged**	**Not Charged**	Charged	Charged	**Not Charged**	Up /down

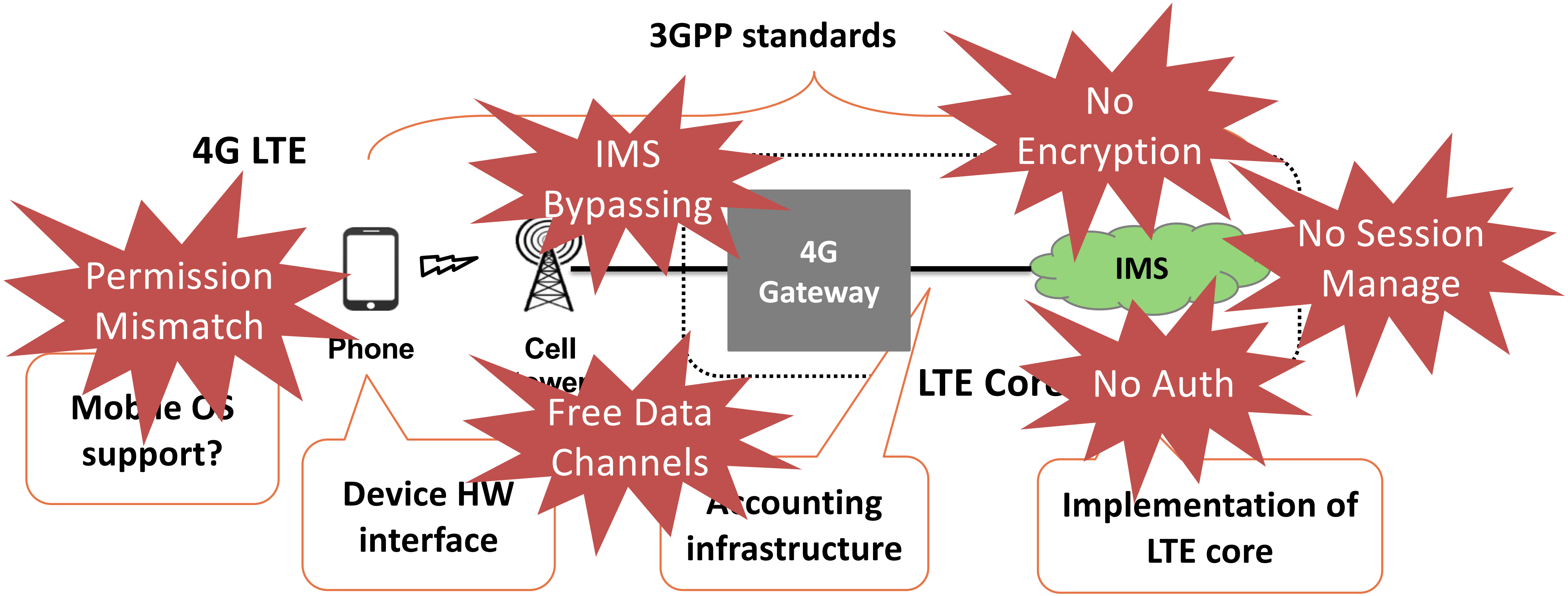
Using 3G and 4G for Free (NDSS'13)



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

ISPs don’t talk to each other!

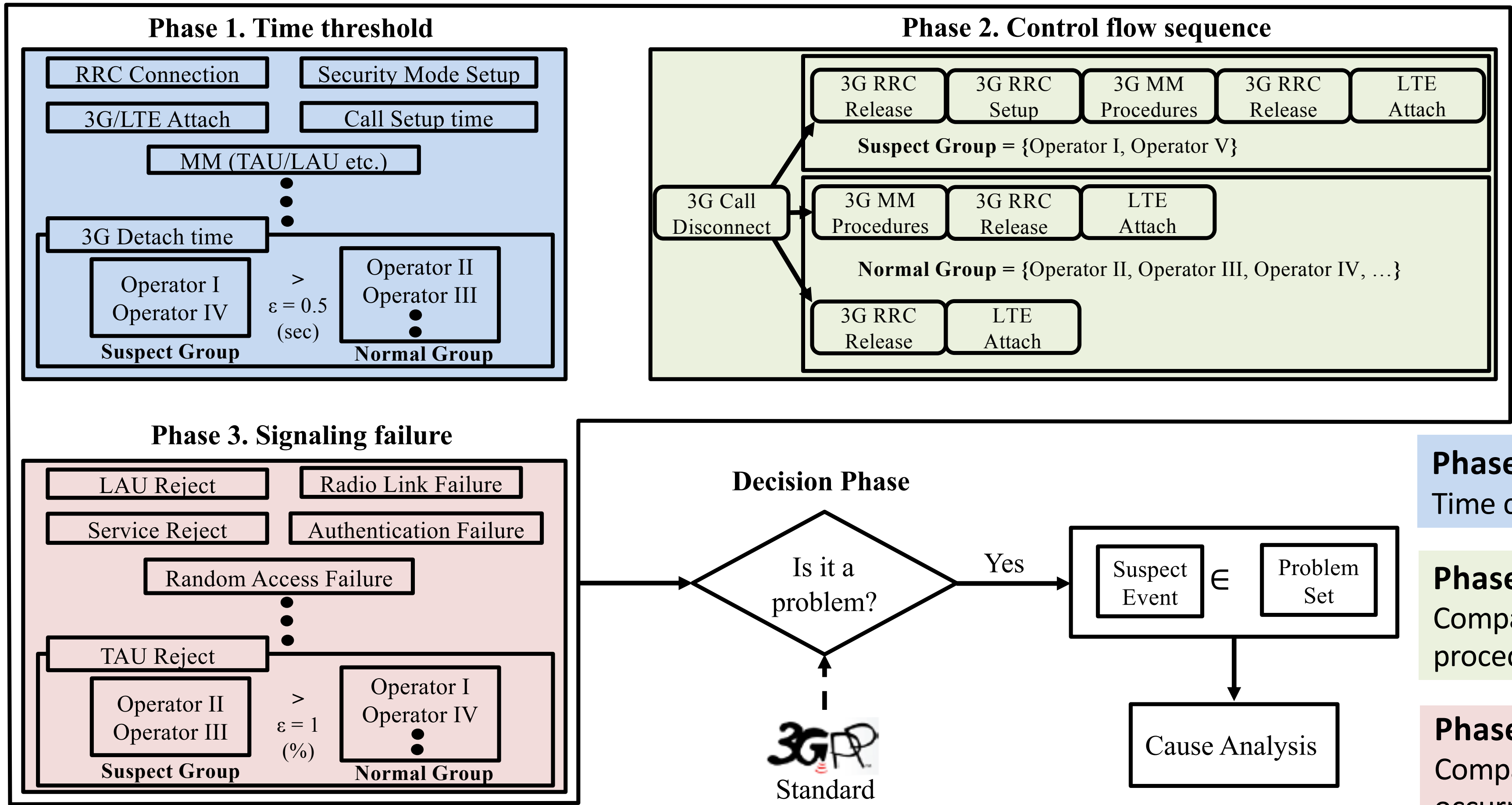
Worldwide Data Collection

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

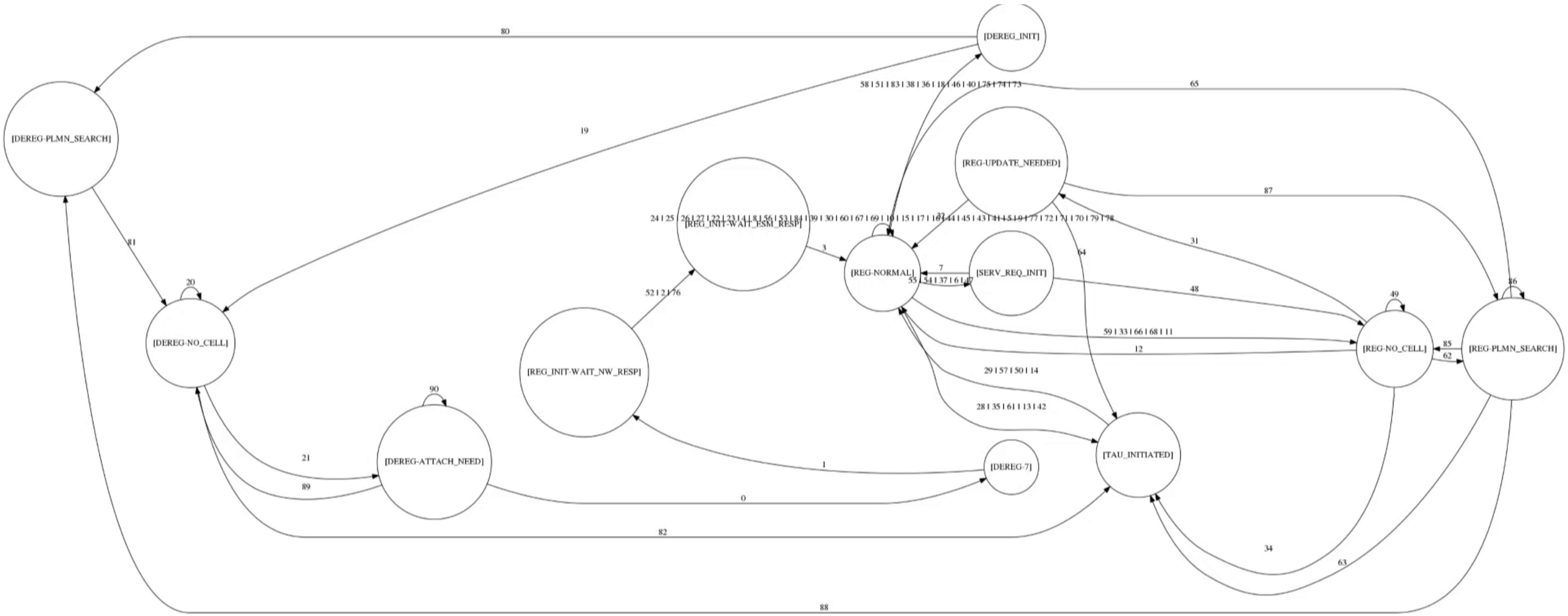
Phase 3
Comparison of signaling failure occurrence probability

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
[DEREG-PLMN_SEARCH]
19
58 | 51 | 83 | 38 | 36 | 18 | 46 | 40 | 75 | 74 | 73
65
[REG-UPDATE_NEEDED]
87
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
[REG_INIT-WAIT_ESM_RESP]
32
81
3
64
31
[REG-NORMAL]
7
[SERV_REQ_INIT]
55 | 54 | 37 | 6 | 47
20
86
48
49
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
[TAU_INITIATED]
21
[DEREG-ATTACH_NEED]
1
[DEREG-7]
89
0
82
34
63
88

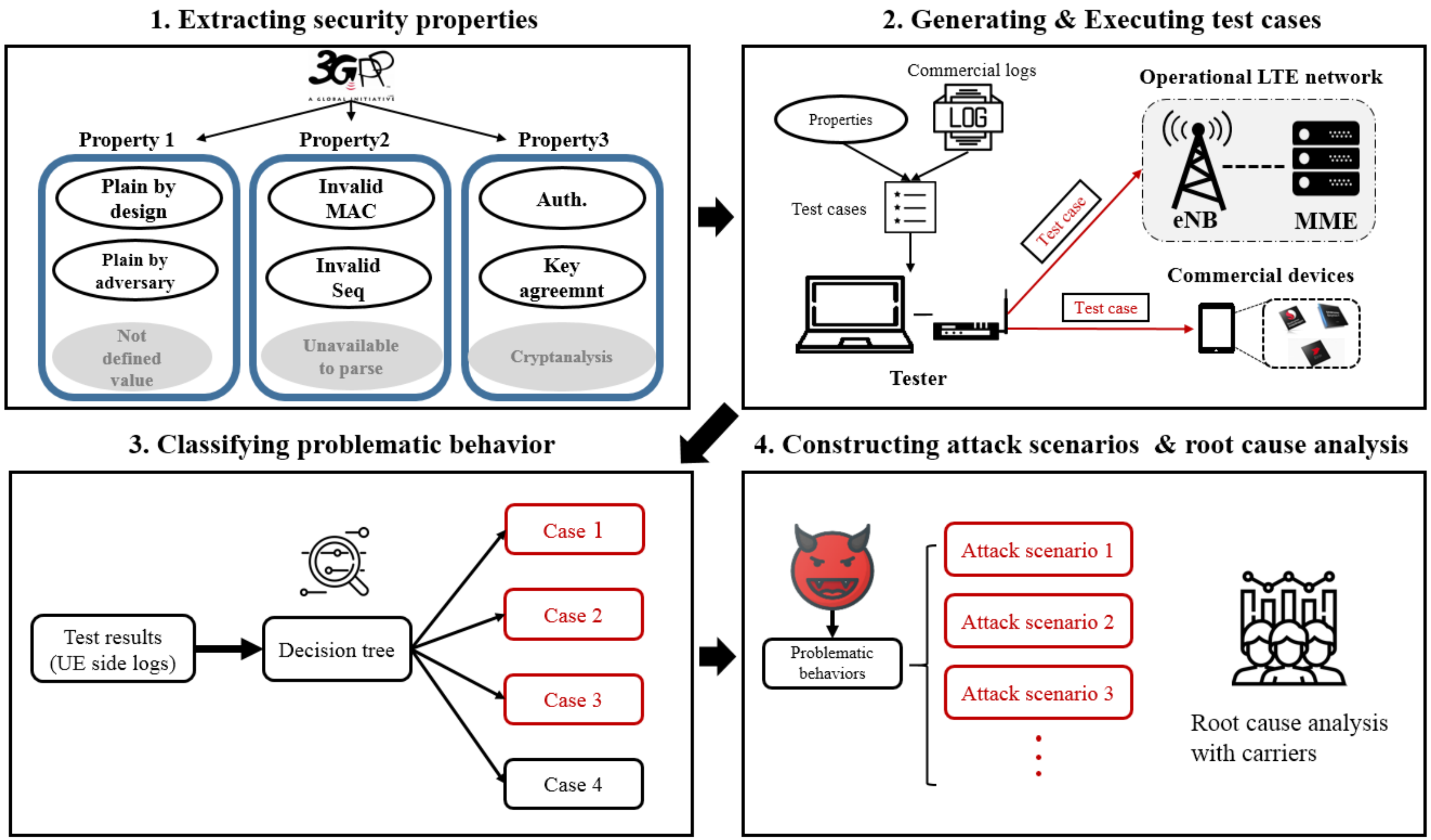
Fuzzing LTE Core and Baseband

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

LTEFuzz


1. Extracting security properties
3GPP
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

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		
	$\mathbf{MME_1}$	$\mathbf{MME_2}$	$\mathbf{MME_3}$
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

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

Lessons Learned from 4G LTE Security

- Long patch cycle
  - Carrier
    - Carrier A: First reported at Aug. 2018 -> Validated the vulnerabilities in their testbed at Oct. 2018 -> Patched and re-validated in the testbed at Jul. 2019
    - Carrier B: First reported at Aug. 2018 -> Validated the vulnerabilities in their testbed at Sep., 2018 -> Patched and re-validated in the testbed at Apr. 2019
  - Baseband vendor
    - First reported at Dec. 2018 -> Qualcomm confirmed the bug at Jan. 2019 -> Vendor release in progress -> Public release in Oct. 2019.
  - Qualcomm's response against AKA Bypass attack

In 2012 Qualcomm turned on the integrity protection by default and released a note to OEMs informing about that. OEMs were still left an option to disable integrity protection with a special flag as a backward-compatibility measure.

Lessons Learned from 4G LTE Security

- A lot of systematic problems from cellular industry

- Standard has a lot of unpatched 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
- ISPs don’t talk to each other. They don’t respond to public scrutiny.
  - Vendors don’t talk to each other.

(In 3 years) 5G Security

- A lot of systematic problems from cellular industry

- Standard has a lot of unpatched 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
- 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"