

DoLTest: In-depth Downlink Negative Testing Framework for LTE Devices

**CheolJun Park, Sangwook Bae, BeomSeok Oh, Jiho Lee, Eunkyu Lee,
Insu Yun, and Yongdae Kim**



LTE is Everywhere

❖ > 22,000 LTE user devices from 990 manufacturers



Railway communication (LTE-R)



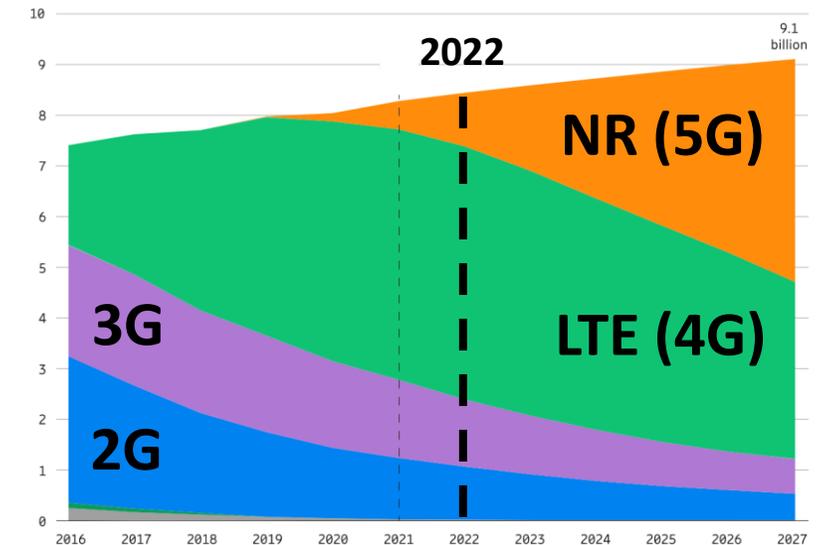
Industrial devices (LTE-M, NB-IoT)



Public safety services (PS-LTE)



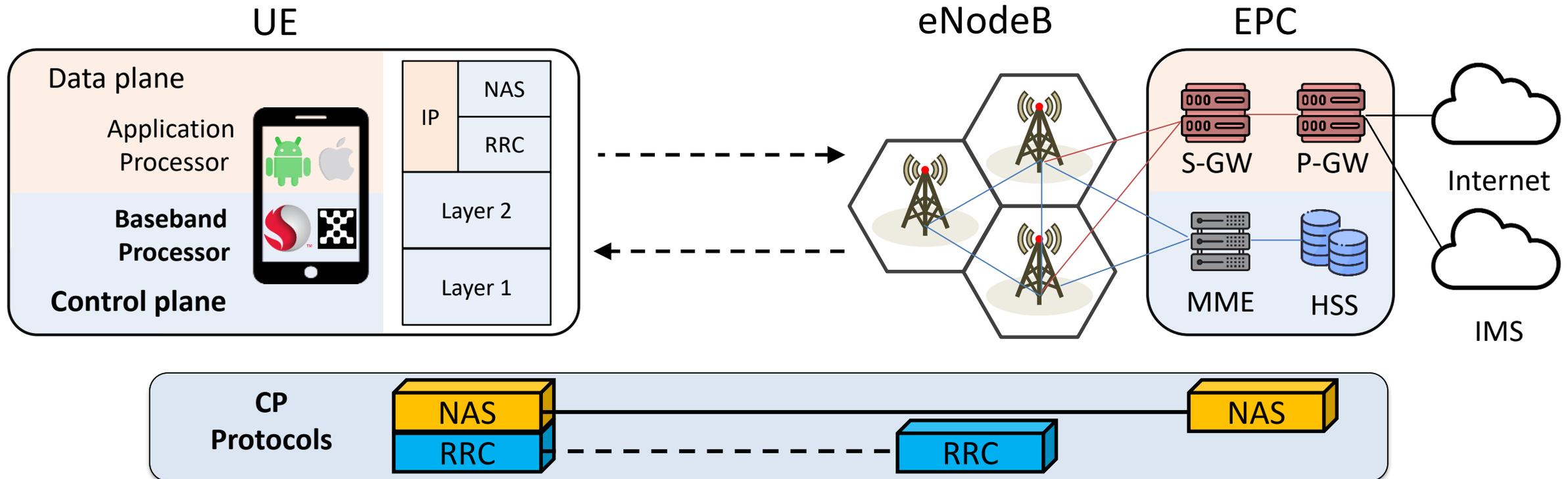
Vehicle communication (C-V2X)



> 60% LTE subscription

LTE Network Architecture

- ❖ LTE service procedures are separated into **control plane** and user plane
 - Two main control plane protocols: **RRC, NAS**



Negative Testing

- ❖ Positive 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. ^[1]
(3 RRC and 11 NAS)
 - Challenges
 - How do we enumerate all violating cases?
 - UE/Network state dependence
 - Spec is difficult to understand → Oracle?

[1] 36.523, v15.5.0

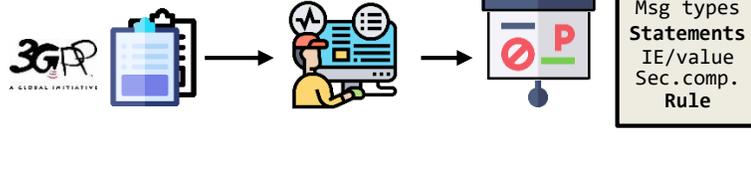
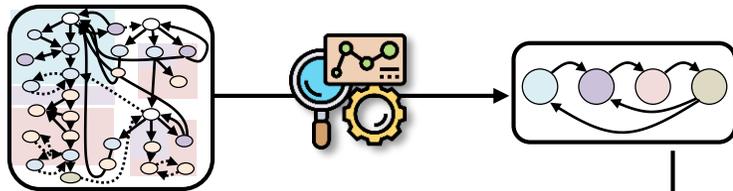
Overview of Our Approach (DoLTest)

1. Manual spec. analysis

2. Test case generation & OTA testing

3. Manual post-analysis

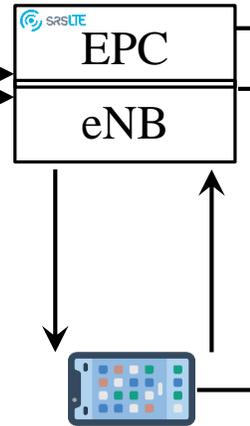
① Define new security-abstracted states



② Construct *guidelines*

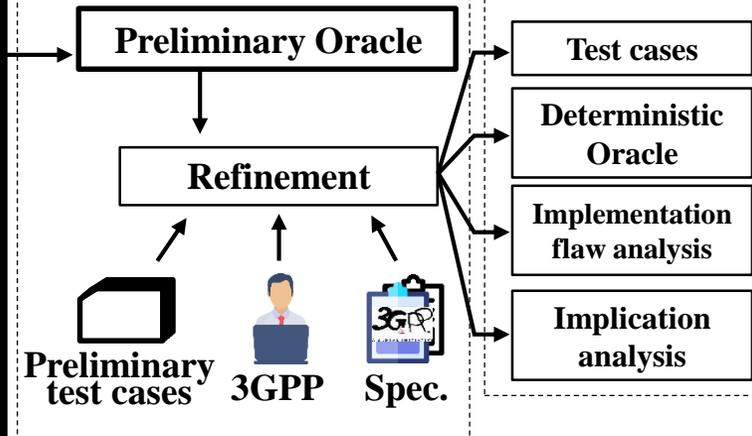
③ Generate test cases

State: No-SC
Sec.hdr: 0 (no integrity)
Msg Type: Identity Req
IE : Identity Type 2
Value : 0 (reserved)
MAC : plain



④ Open-source LTE stack based over-the-air device testing

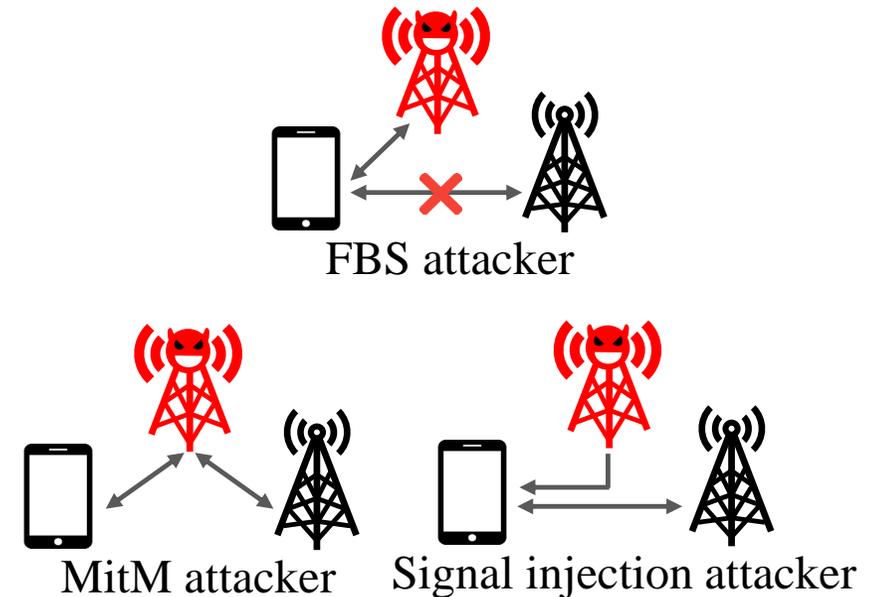
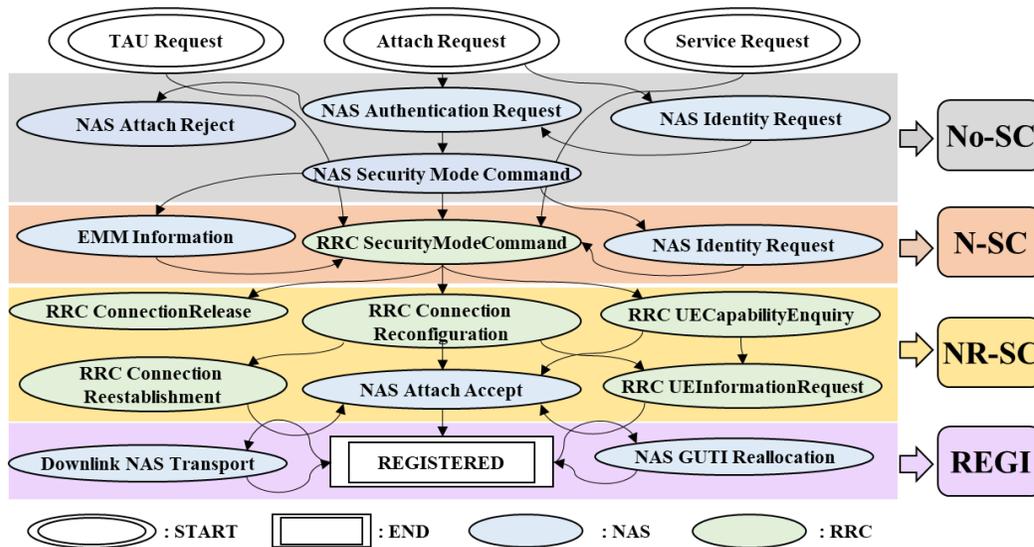
⑤ Deviant behavior analysis



⑥ Flaw & implication analysis, oracle refinement

Security Abstracted States

- ❖ Re-define the existing implicit UE states as **new security abstracted states**
- ❖ Advantages
 - Reflecting **advanced LTE attacks**
 - **Reduce** total number of test cases



Test Case Generation

- ❖ Goal: Generating test messages that are **invalid or prohibited by specification**
 - We found every **statement** related with message authentication^[1,2]
 - Addressing ambiguities in the spec: over-approximation

Protocol	Guideline						MAC	Reference	# of test cases for each state	Page #
	No.	State	Security Header Type	Message Type	IE					
RRC	1	*	N/A	RRCCONNECTIONRECONFIGURATION	drb-ToAddModList: {...}	*	A.6, 5.3.1.1 in [7]	2	68p	
	2	*	N/A	RRCCONNECTIONRECONFIGURATION	srb-ToAddModList: {SRB2}	*	A.6, 5.3.1.1 in [7]	2	39p	
	3	*	N/A	RRCCONNECTIONRECONFIGURATION	measConfig: {...}	*	A.6, 5.5.5.1 in [7]	2	68p	
	4	*	N/A	RRCCONNECTIONRECONFIGURATION	mobilityControlInfo: {...} securityConfigHO: {...}	*	A.6, 5.6.5.1 in [7]	2	918p, 72p	
	5	*	N/A	RRCCONNECTIONRELEASE	...	*	A.6 in [7]	2	918p	
	6	*	N/A	SECURITYMODECOMMAND	integrityProtection: {EIA1, EIA2, EIA3} ^c	*	A.6, 5.3.1.2 in [7]	10	70p	
	7	*	N/A	UECAPABILITYENQUIRY	...	*	A.6, 5.6.3.2 in [7]	2	230p	
	8	*	N/A	COUNTERCHECK	...	*	A.6 in [7]	2	918p	
	9	*	N/A	UEINFORMATIONREQUEST	...	*	A.6, 5.6.5.2 in [7]	2	919p	
	10	*	N/A	DLINFORMATIONTRANSFER	...	*	A.6 in [7]	2	918p	
NAS	11	*	*	IDENTITY REQUEST	Identity Type2: {IMSI} ^c	*	4.4.4.2 in [4]	124	50p, 51p	
	12	*	*	SECURITY MODE COMMAND	integrityProtAlgorithm: {EIA1, EIA2, EIA3} ^c	*	4.4.4.1, 4.4.4.2 in [4]	155	50p	
	13	*	*	GUTI REALLOCATION COMMAND	...	*	4.4.4.2 in [4]	31	50p, 51p	
	14	*	*	EMM INFORMATION	...	*	4.4.4.2 in [4]	31	50p, 51p	
	15	*	*	DOWNLINK NAS TRANSPORT	...	*	4.4.4.2 in [4]	31	50p, 51p	
	16	*	*	ATTACH REJECT	EMM cause: {#25}	*	4.4.4.2, 5.5.1.2.5 in [4]	31	50p, 51p, 129p	
	17	*	*	ATTACH ACCEPT	...	*	4.4.4.2 in [4]	31	50p, 51p	

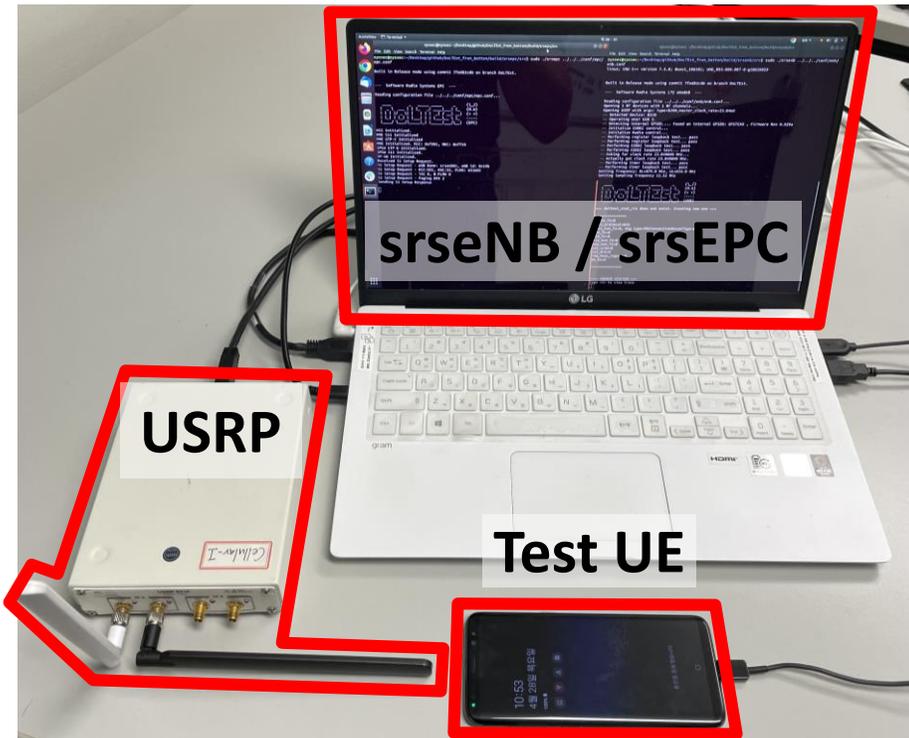
[1]: TS. 24.301, [2]: TS. 36.331

Example

Specification	<p>Except the messages ... below, no NAS signalling messages shall be processed by the UE... unless the network has established secure exchange of NAS messages...</p> <p>...</p> <p>- Identity Request ((if requested identification parameter is IMSI))</p>					
Guideline	State	Security Header Type	Message Type	IE	Value	MAC
	* ✘	* ✘	✘ Identity Request ✘	Identity Type 2 ✘	✘ not IMSI ✘	* ✘
Over-approximation	No-SC ... No-SC ... No-SC N-SC	0 (no integrity protected) ... 1 (no integrity protected) ... 3 (integrity protected with...) 3 (integrity protected with...)	Identity Request ... Identity Request ... Identity Request Identity Request	Identity Type 2 ... Identity Type 2 ... Identity Type 2 Identity Type 2	0 (reserved) ... 2 (IMEI) ... 3 (IMEISV) 3 (IMEISV)	plain ... random ... random plain

Implementation

- ❖ We edited srsLTE (9,234 LoC) to send total 1,848 test messages
 - State control + Test message generation
- ❖ Available on: <https://github.com/SysSec-KAIST/DoLTEst>



```
syssec@syssec:~/Desktop/github/DoLTEst_from_bottom/build/srsepc/src$ sudo ./srsepc ../conf/epc/epc.conf
Built in Release mode using commit 7fed81cd6 on branch DoLTEst.

--- Software Radio Systems EPC ---

Reading configuration file ../conf/epc/epc.conf...

          ( \ / )
          ( 0.0 )
          ( > < )
          -----
          (EPC)

HSS Initialized.
MME S11 Initialized
MME GTP-C Initialized
MME Initialized. MCC: 0xf901, MNC: 0xff55
SPGW GTP-U Initialized.
SPGW S11 Initialized.
SP-GW Initialized.
Received S1 Setup Request.
S1 Setup Request - eNB Name: srseNB01, eNB id: 0x19b
S1 Setup Request - MCC: 901, MNC: 55, PLMN: 651605
S1 Setup Request - TAC 0, B-PLMN 0
S1 Setup Request - Paging DRX 2
Sending S1 Setup Response

syssec@syssec:~/Desktop/github/DoLTEst_from_bottom/build/srsenb/src$ sudo ./srsenb ../conf/enb/enb.conf
Built in Release mode using commit 7fed81cd6 on branch DoLTEst.

--- Software Radio Systems LTE eNodeB ---

Reading configuration file ../conf/enb/enb.conf...
Opening 1 RF devices with 1 RF channels...
Opening USRP with args: type=b200, master_clock_rate=23.04e6
-- Detected Device: B210
-- Operating over USB 3.
-- Detecting internal GPSDO.... Found an internal GPSDO: GPSTCX0 , Firmware Rev 0.929a
-- Initialize CODEC control...
-- Initialize Radio control...
-- Performing register loopback test... pass
-- Performing register loopback test... pass
-- Performing CODEC loopback test... pass
-- Performing CODEC loopback test... pass
-- Asking for clock rate 23.040000 MHz...
-- Actually got clock rate 23.040000 MHz.
-- Performing timer loopback test... pass
-- Performing timer loopback test... pass
Setting Frequency: DL=879.0 Mhz, UL=834.0 Mhz
Setting Sampling frequency 11.52 Mhz

          ( \ / )
          ( 0.0 )
          ( > < )
          -----
          (eNB)

==== doltest_stat_rrc does not exist. Creating new one ====

*****
state_fz=0
test_protocol=NAS
test_num_fz=0, Asg type=RRCConnectionReconfiguration
EIA_fz=0
EEA_fz=0
eia_num_fz=0
eea_num_fz=0
set_srbz=0
set_drbs=0
req_meas_report=0
do_ho=0

*****

==== eNodeB started ====
Type <t> to view trace
```

Results

- ❖ Tested **43** cellular devices from **five** major baseband manufacturers
 - Qualcomm, Exynos, MediaTek, HiSilicon, and Intel
- ❖ Discovered **26** implementation flaws, of which **22** were new

Type of flaw for handling: S*- Security header type, M*- Message type, I*- IE/value

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)	S3	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	-		-	-		-	-

Studied?: Attacks using the message type was previously studied, †: Previously reported

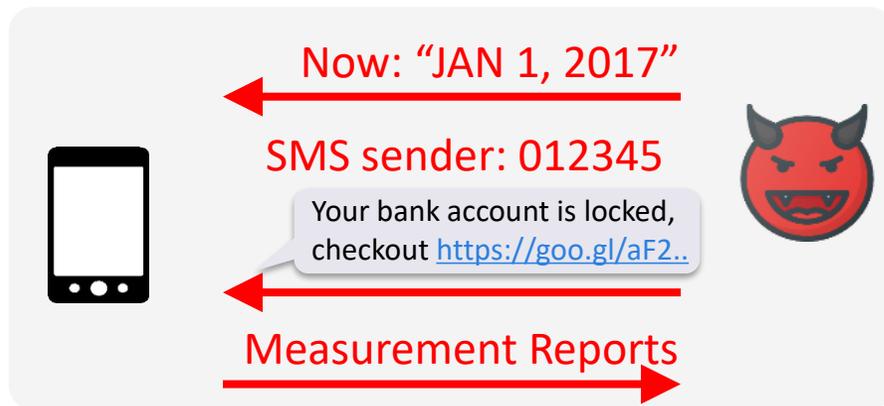
Findings

- ❖ Manufacturer-dependent flaws
 - 5 NAS integrity bypass @ every **Qualcomm BP**
 - 2 RRC integrity bypass @ every **Exynos BP**
- ❖ Device-specific flaws
 - Null integrity algorithm (EIA0) and measurement report b/f security activation @ Galaxy S10 (**Exynos**)
 - AKA bypass @ iPhone 6s (**Qualcomm**)
- ❖ Others
 - Integrity bypass for NAS Identity Request message @ every **MediaTek/Exynos BP** and some **Qualcomm BP**

CVE-2019-2289, CVE-2021-30826, SVE-2021-20291 (CVE-2021-25516)

Attacks

- ❖ Network identity and time zone spoofing
- ❖ SMS injection
- ❖ Eavesdropping and manipulating data traffic
- ❖ Location leakage
- ❖ Also, device fingerprinting



Baseband	Device	Message				
		#1	#2	#3	#4	#5
Intel	Apple iPhone XS	.	.	.	A ₅	.
Qualcomm	Xiaomi Mi Mix 2	.	A ₂	A ₄	A ₅	A ₃
Exynos	Samsung Galaxy S10	A ₁	.	A ₄	A ₅	.
MediaTek	LG K50	.	.	A ₄	A ₆	.
HiSilicon	Huawei Mate 20 Pro	.	A ₃	.	A ₅	.

What else?

❖ Old bug reappearing

- Null integrity check is an old (early-LTE) bug
- However, it suddenly re-appeared on brand-new device, Galaxy S10 (Exynos)

❖ New bug after firmware patch

- After patching to the latest firmware, new bug appeared
- Galaxy S8 (Qualcomm), iPhone 6s (Qualcomm)

❖ MediaTek PSRT --- Did not replied to my bug reports for years.

- Contacted multiple times for multiple bugs over multiple papers. (12/20, 05/21, 01/22, ...)
- Just received one response for another paper. None for this.
- Also, they decided to not to give a CVE for no reason.

Conclusion

- ❖ **Only a few negative test cases** in the conformance specification
- ❖ **DoLTest**: a negative testing framework for finding non-standard-compliant bugs in UE
 - Tested 43 devices and found 26 implementation flaws
 - Brand-new device, firmware patch can bring a new logical bugs
 - **Open-sourced**: <https://github.com/SysSec-KAIST/DoLTest>
- ❖ We recommend 3GPP to **include much more negative test cases on the conformance test specification**

Thank You!

- ❖ Questions?
- ❖ You can reach us:
 - CheolJun Park : fermioncj@kaist.ac.kr ( @cheoljun_p)
 - Sangwook Bae: baesangwook89@gmail.com ( @baesangwook89)
- ❖ KAIST SysSec Lab (Prof. Yongdae Kim)

