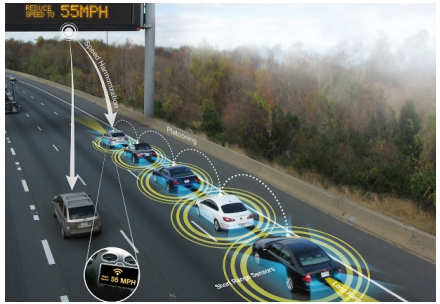
Touching the Untouchables:
Dynamic Security Analysis of the LTE Control Plane

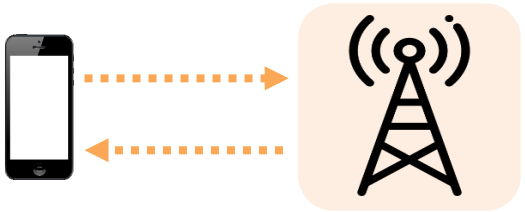
Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim

2019 IEEE Symposium on Security and Privacy

LTE communication is everywhere



Autonomous driving
(Cellular V2X)



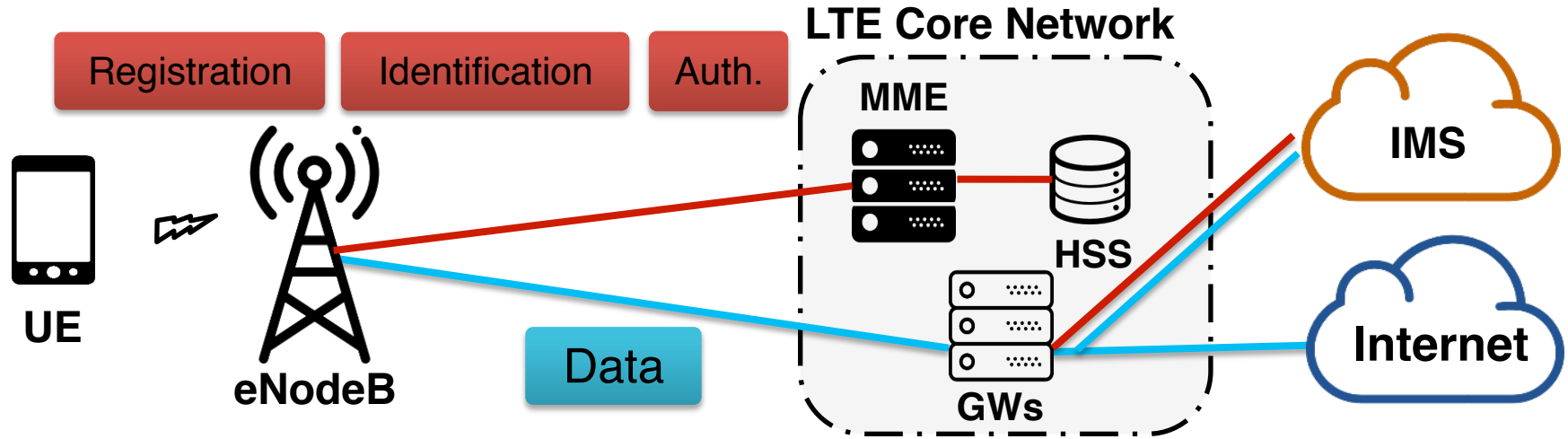
Public safety services
(PS-LTE)

Industrial IoT devices
(NB-IoT, LTE-M)

Railway communication
(LTE-R)

Maritime communication
(LTE-Maritime)

LTE network architecture



- LTE service procedures are separated into **control plane** and **user plane**
- Control plane procedures
  - (De)Registration of mobile phones, mutual authentication, mobility support, …
  - **Always preceded by the user plane procedures**
  - **Might be a good target for adversaries**

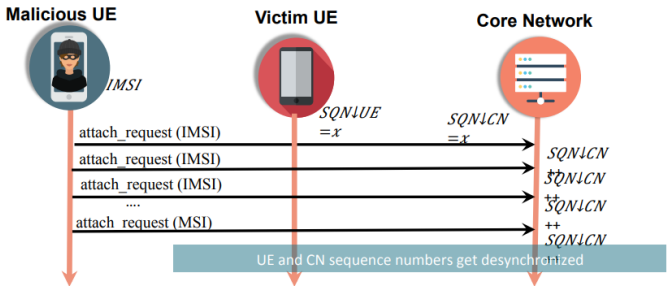
*UE: User Equipment, *MME: Mobility Management Entity

Previous studies and its limitations

- Formal analysis of **LTE specification**

LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE

Syed Rafiul Hussain, Purdue University, hussain1@purdue.edu
Omar Chowdhury, The University of Iowa, omar-chowdhury@uiowa.edu
Shagufta Mehnaz, Purdue University, smehnaz@purdue.edu
Elisa Bertino, Purdue University, bertino@purdue.edu



Ambiguities in LTE specification

- include a lot of exception cases
- leave freedom to the carriers and v endors about the implementation d etails
- have protocol conformance test sta ndard but,
  - Only for UE (LTE phone)
  - Do not consider the malicious/inco rrect procedures

Carriers may have implementation bugs even if the spec. is correct

Previous studies and its limitations

Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems

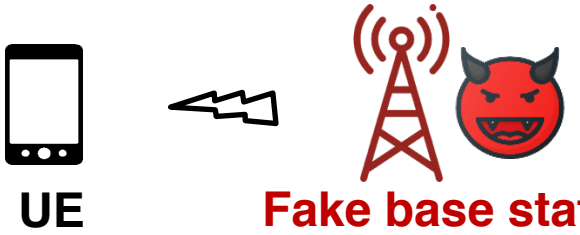
Putting LTE Security Functions to the Test: A Framework to Evaluate Implementation Correctness

nsen

LTE REDIRECTION

Forcing Targeted LTE Cellphone into Unsafe Network

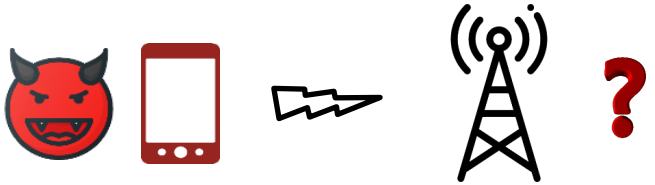
HUANG Lin



UE

Fake base station

- Steal user identity
- Location tracking
- DoS attack



Fake UE

Commercial network

What about a fake LTE phone to inspect commercial networks?

Challenges in active network testing

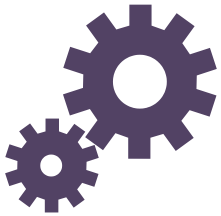
- Difficulties to actively inspect operational LTE networks
  1. Sending malicious signal to a commercial network is not allowed
     - ➔ Got Carriers' Testbed access
  2. It is hard to control baseband chipsets for simulating malicious behavior
     - ➔ Use open-source LTE software (srsLTE, openLTE, and SCAT)
  3. An LTE network is a closed system
     - ➔ Device-side debugging

Goal of our research

- Investigate potential problems of the control plane procedures in LTE
  - **Rooted from either**

Specification problem

Implementation bug

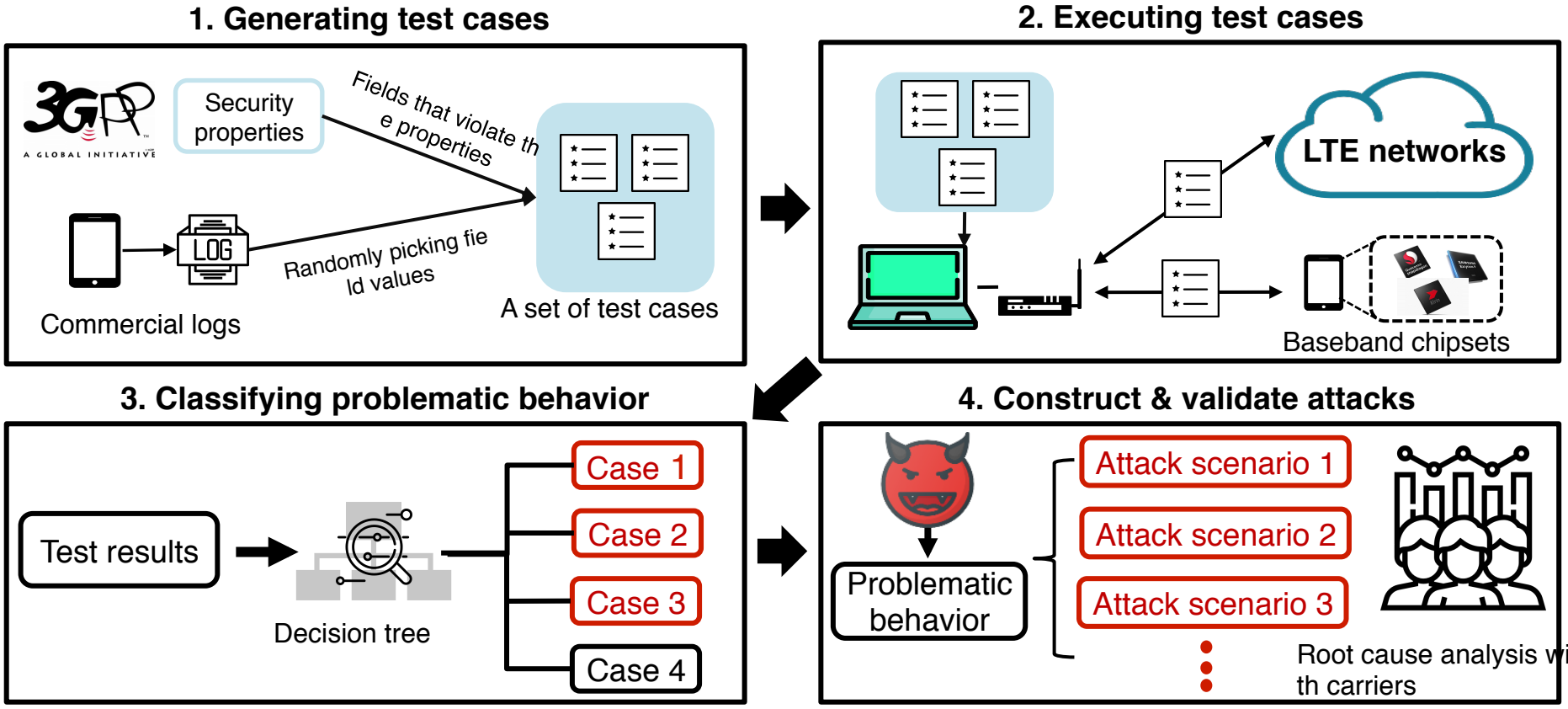


Configuration bug

  - **How?**

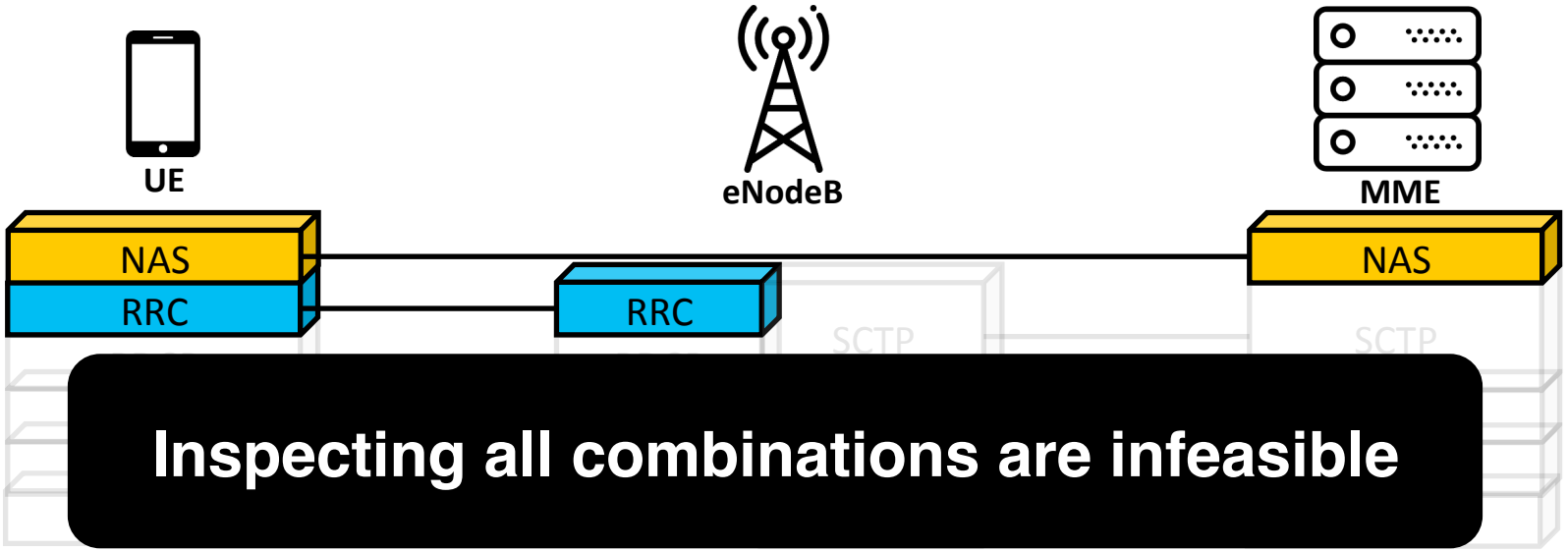
Comprehensive dynamic testing against commercial LTE networks

Overview of LTEFuzz



Generating test cases

- Target control plane protocols: RRC and NAS
- Target procedures
  - Radio connection, network attach/detach, location management, and session manag ement, …



RRC: Radio Resource Control, NAS: Non Access Stratum

Generating test cases

1. **Define basic security properties based on LTE specification**

   Property 1. Plain messages should be handled properly
   - Plain messages by design
   - Plain messages manipulated by an attacker

   Property 2. Invalid security protected messages should be handled properly
   - Invalid security header type
   - Invalid MAC (Messages Authentication Code)
   - Invalid Sequence number

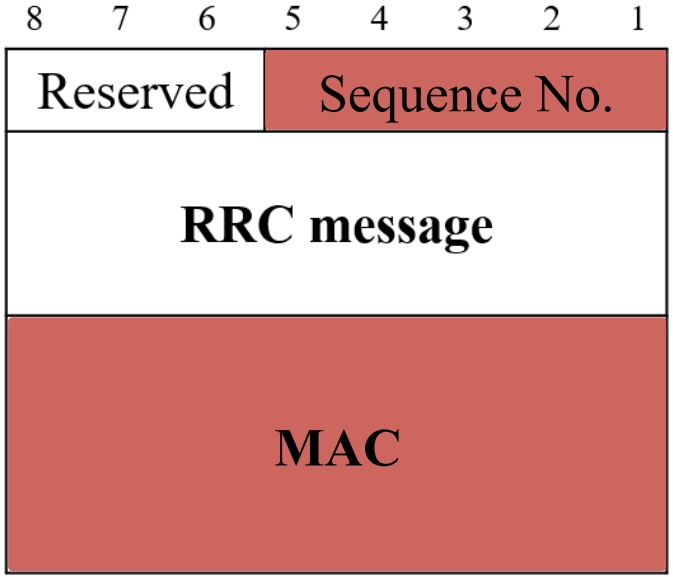
   Property 3. Mandatory security procedures should not be bypassed
   - Authentication
   - Key agreement procedure

Generate test cases that violate the properties

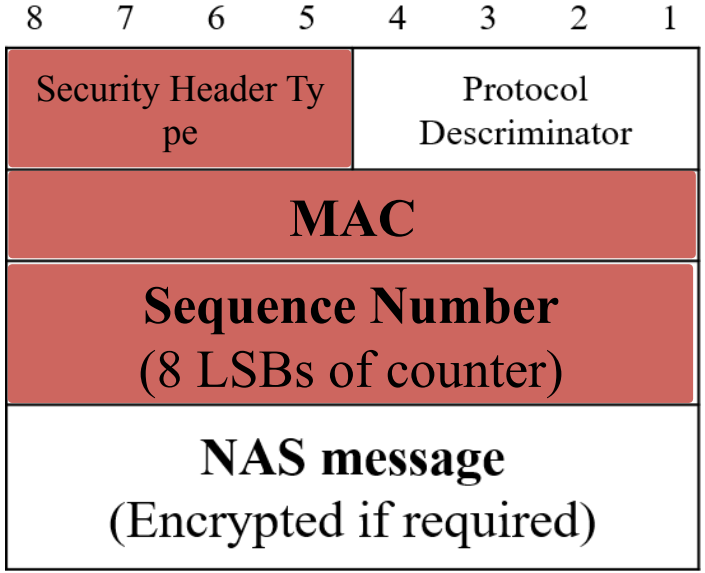
Generating test cases

1. **Define basic security properties based on LTE specification**

RRC test case



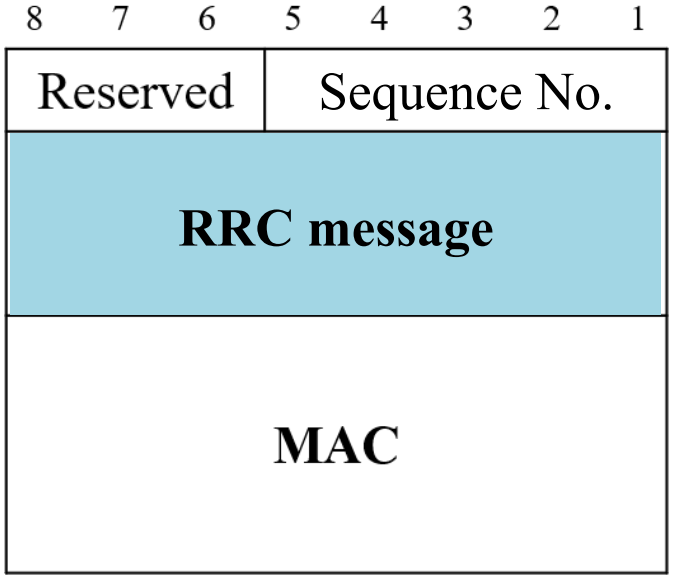
NAS test case



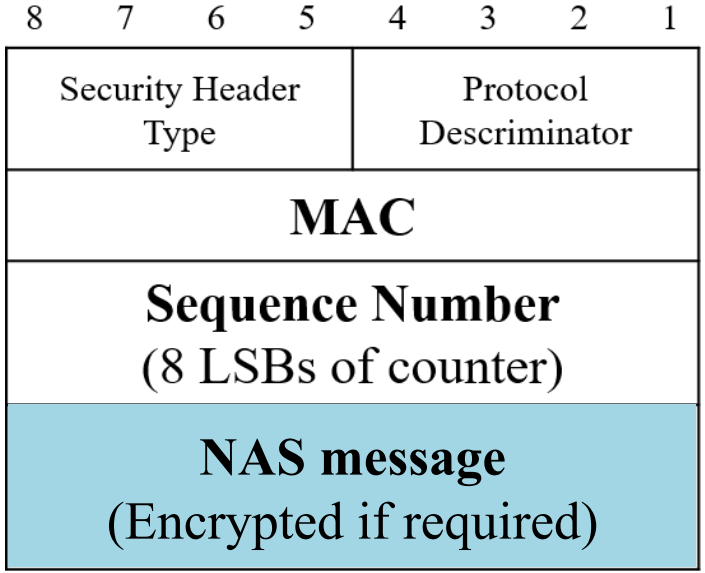
Generating test cases

1. **Define basic security properties based on LTE specification**

RRC test case



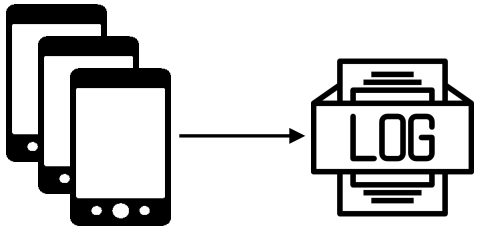
NAS test case



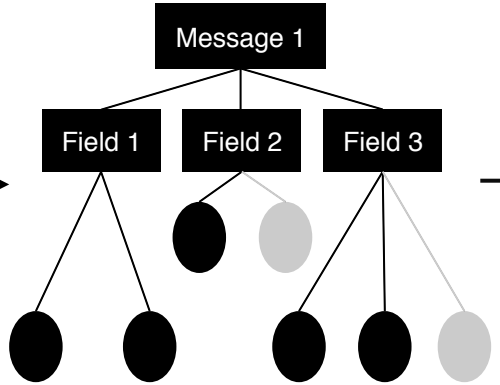
Generating test cases

2. Pick remaining field values randomly from commercial control plane logs

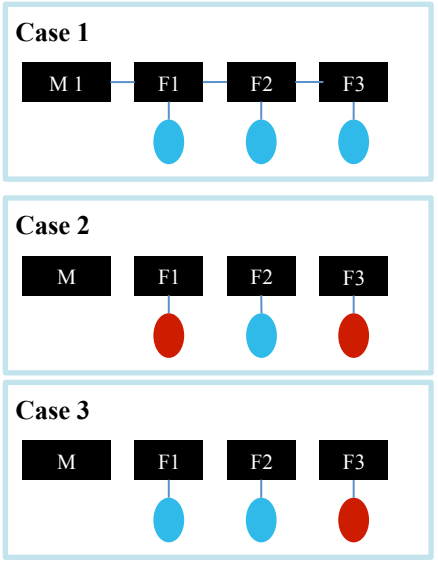
– Not to cause memory corruption errors in the operational networks



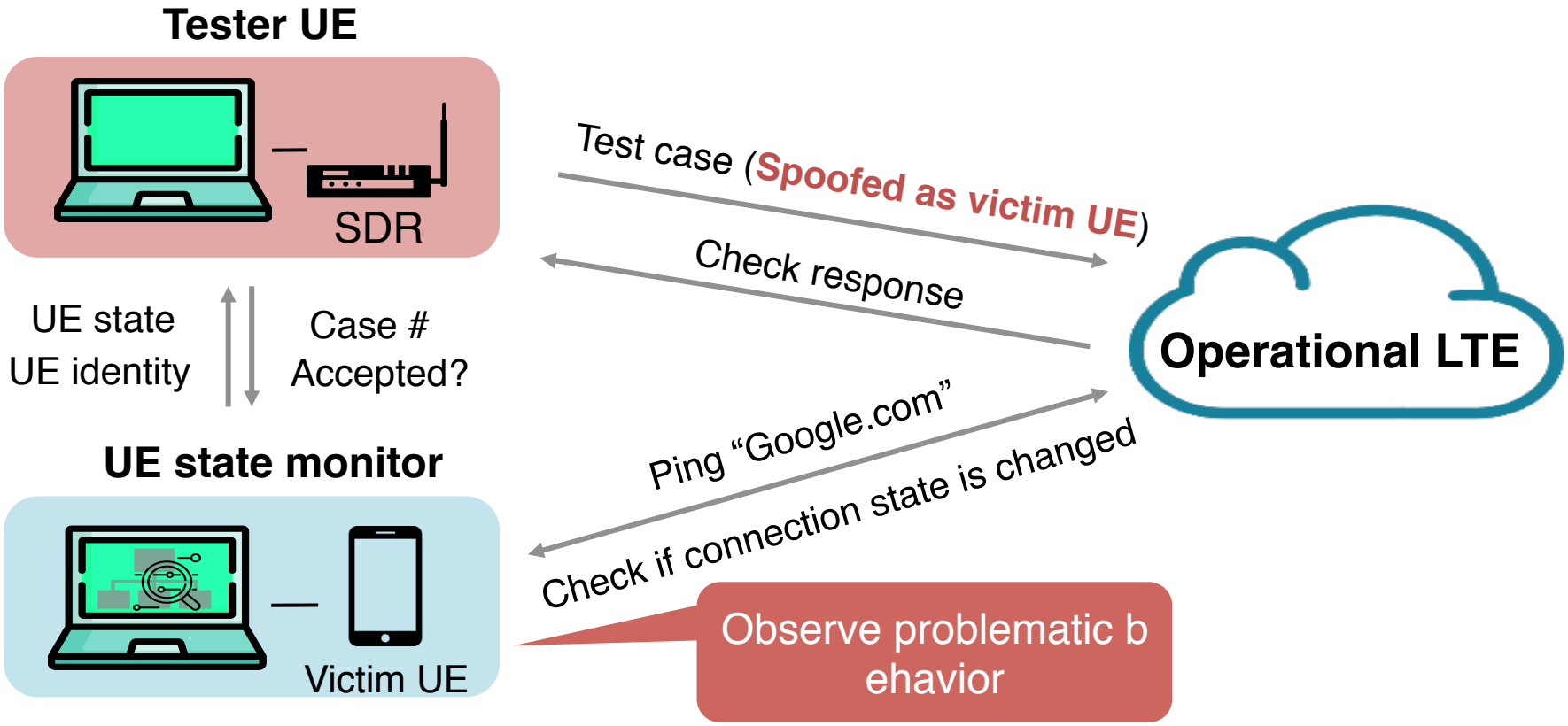
Commercial control plane logs e xtracted from the phones.



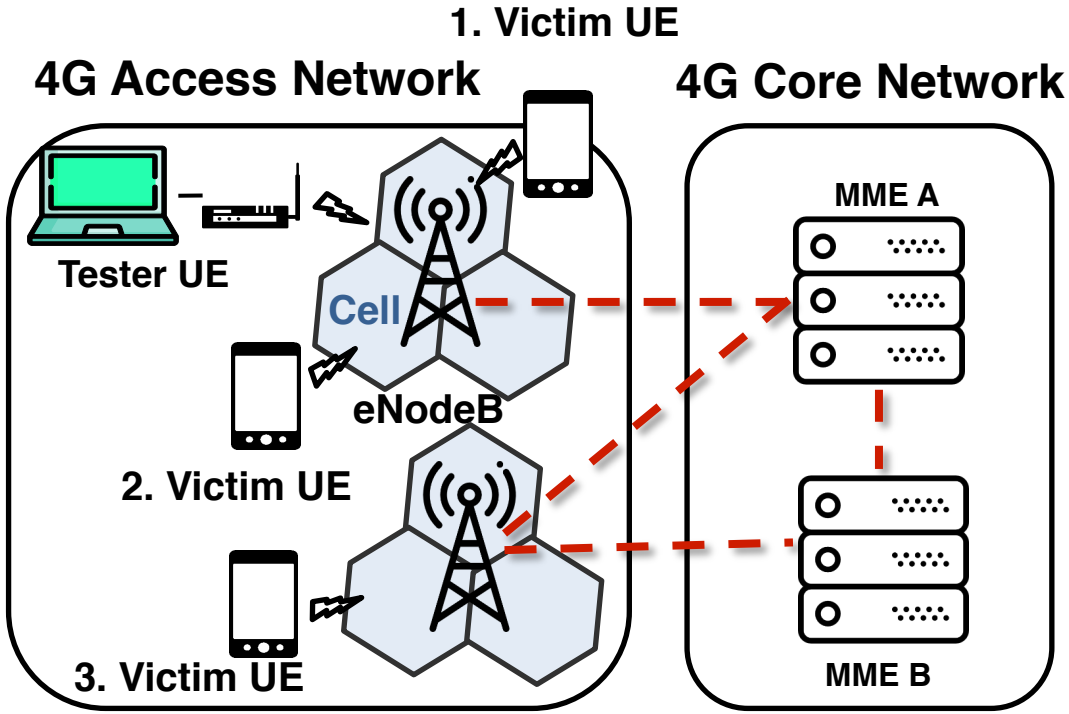
Save the field values which are u sed in the commercial networks



Executing test cases



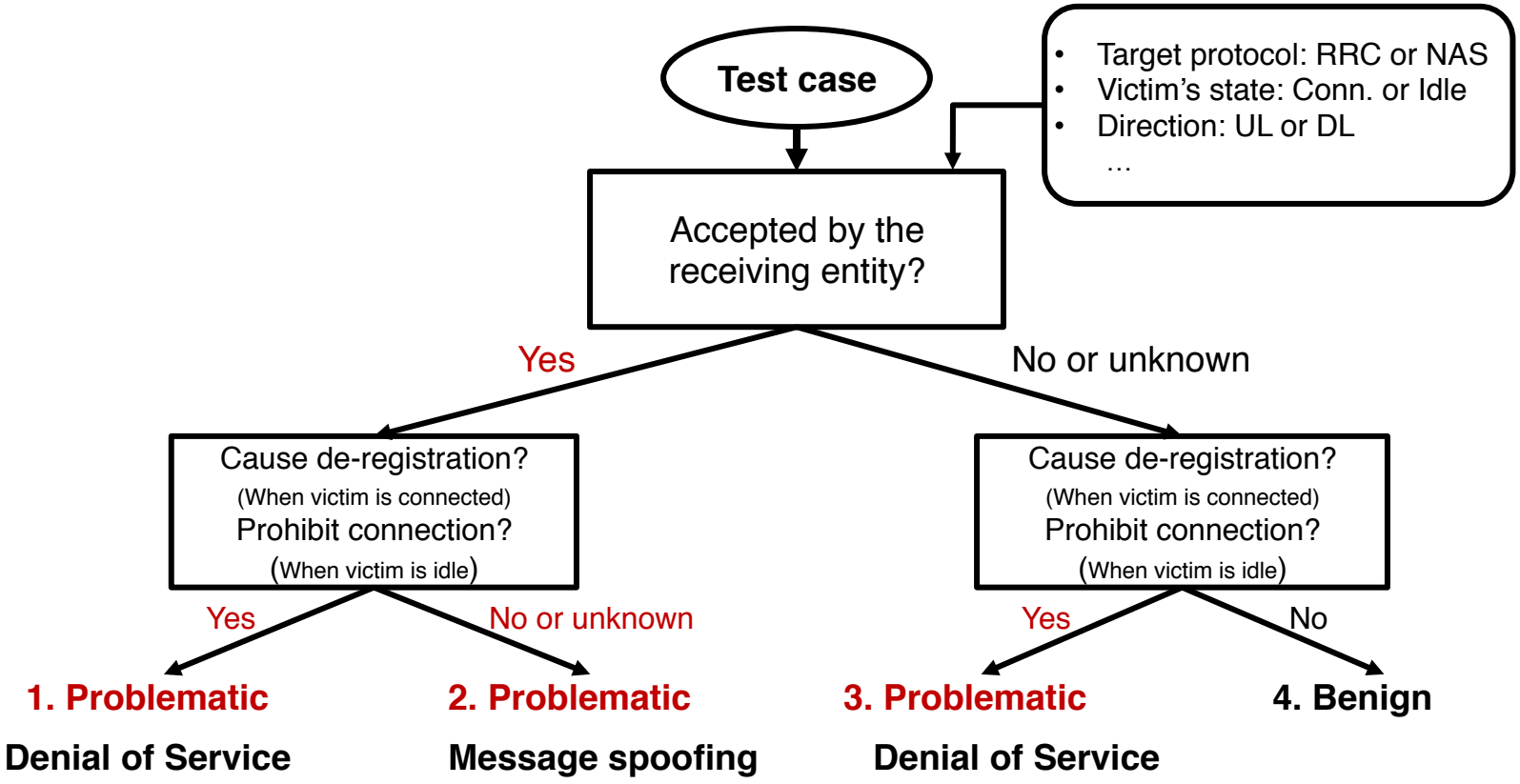
Operational networks are complicated



- Each carrier has different con figurations
- Each carrier deploys different network equipment
- In a single carrier, network eq uipment differs by the service area
- The location of the tester and the victim affects the results

Hard to manually analyze which case is problem

Classifying the problematic behavior



LTEFuzz test environment

Network testing

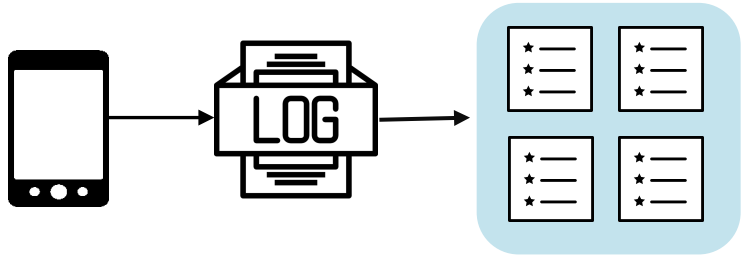
- Target network vendors
  - Carrier A: two MME vendors, one eNB vendor
  - Carrier B: one MME vendor, two eNB vendors

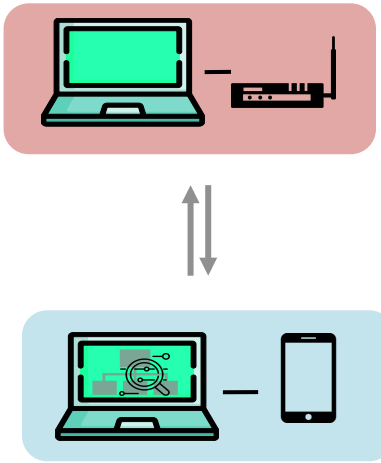
Baseband testing

- Target baseband chipsets
  - Qualcomm, Exynos, HiSilicon, MediaTek

Implementation

- **Test input collector & message generator**
  - 1937 lines of code of C++
- **Tester**
  - Network testing
    - srsUE (fully controllable LTE baseband)
    - (Additional) 550 lines of code of C++
  - Baseband testing
    - openLTE & srsLTE (fully controllable LTE network)
    - (Additional) 840 lines of code of C++
- **UE state monitor & testing automation**
  - *For classifying problematic cases* when each test case is executed
  - Based on Signaling Collection and Analysis Tool (SCAT)
  - 143 lines of code of python for testing automation
    - 80 lines for testing automation, 63 lines for monitoring victim device





Findings

- Test cases classified into problematic behavior
  - Total 51 cases: **36 new** and 15 previously known
  - Categorized into five vulnerability types
    - Unprotected initial procedure cause failure (Property 1-1)
    - Invalid plain requests are accepted (Property 1-2)
    - Messages with invalid integrity protection (Property 2-1)
    - Messages with invalid sequence number (Replay) (Property 2-2)
    - AKA procedure can be bypassed (Property 3)
- Validated with the corresponding carriers and vendors
  - No false positive, but two false negatives
    - *UplinkNAStransport* (for SMS) and *Service request* (response was encrypted)

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

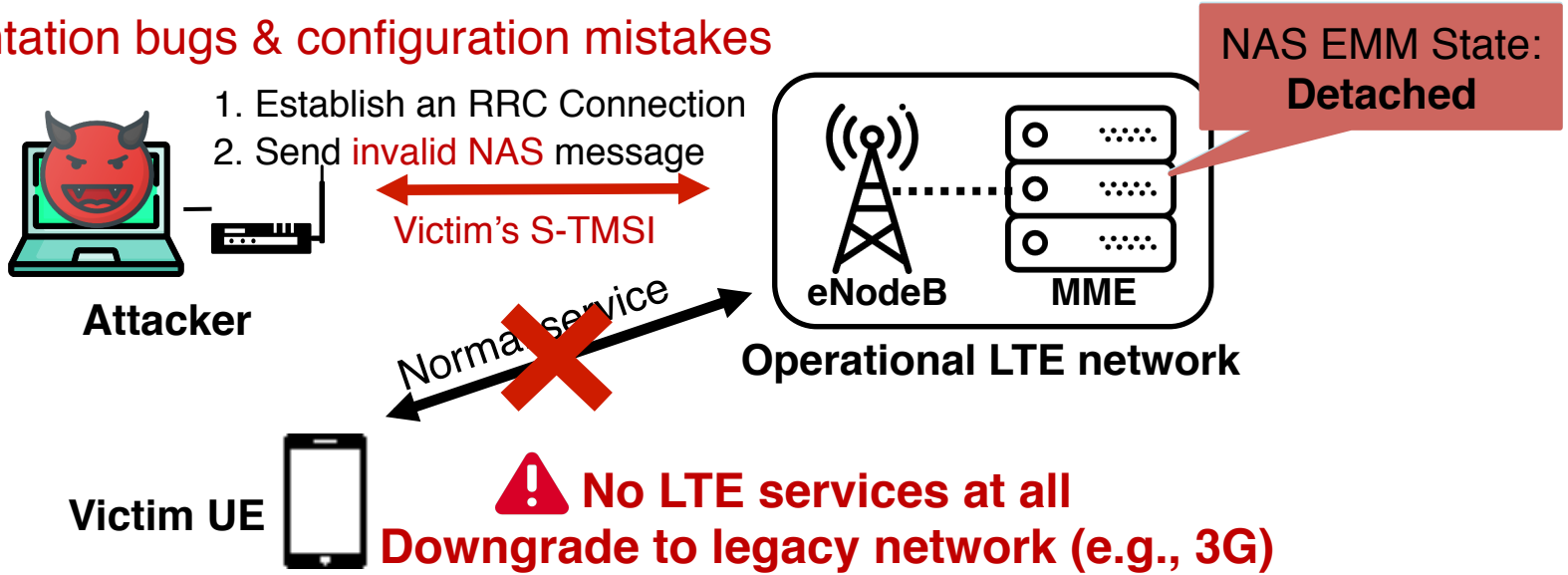
I: Invalid MAC

R: Replay

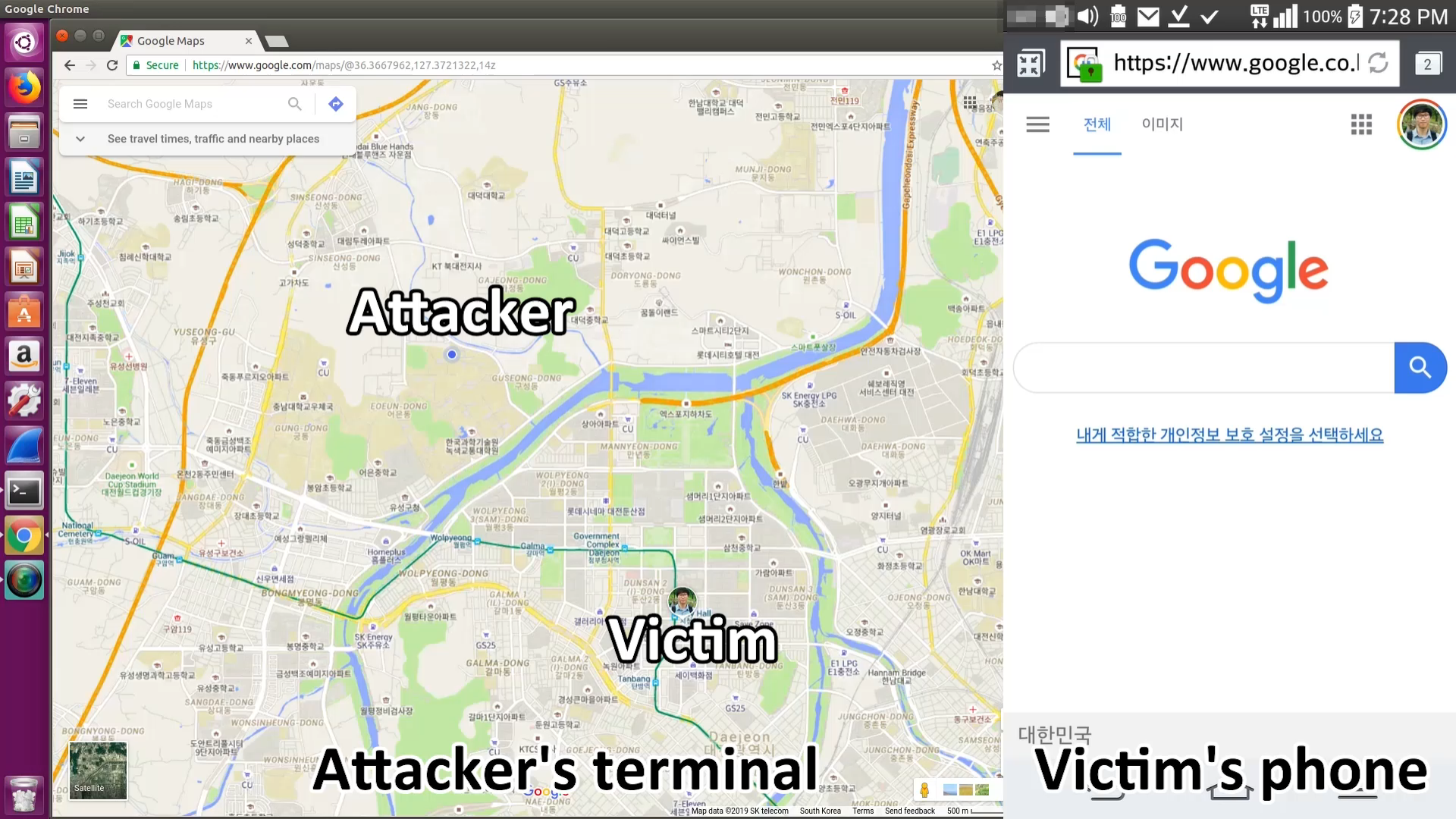
ATTACKS

Remote de-register attack

- **Exploited test case:** 15 cases in NAS (Attach, Detach, TAU, PDN con/discon…)
- An Attacker is *within the same MME pool of the victim UE*
- Implementation bugs & configuration mistakes



- *Nitpick: GUTI in NAS messages are not correctly checked in some MME vendors*


Google Chrome
Google Maps
Secure
https://www.google.com/maps/@36.3667962,127.3721322,14z
Search Google Maps
See travel times, traffic and nearby places
Attacker
Victim
Attacker's terminal
https://www.google.co.
전체
이미지
Google
내게 적합한 개인정보 보호 설정을 선택하세요
대한민국
Victim's phone

Responsible disclosure

- Standard bodies
  - 3GPP
  - GSMA
- Vendors
  - LTE network vendors
    - Validated through the contacted carriers
    - Also validated the fixes created by the vendors
  - Baseband chipset vendors
    - Reported AKA Bypass attack, and replay attack
    - Will be patched soon

Conclusion

- Operational LTE networks are not as secure as we expected!
  - **Complicated deployments (e.g., each network equipment is from different vendors) generate extremely complicated behavior (faults).**

- We have implemented LTEFuzz
  - A semi-automated dynamic testing tool for both networks and devices
  - Using open source LTE software and a simple decision tree
  - Specification problems: 16, Implementation bugs + configuration issues: 35
  - **LTEFuzz considers realistic attack assumptions in operational LTE networ k**
- Future work
  - Extend LTEFuzz to support other control protocols and 5G if allowed

Thank you

Contact: hongilk@kaist.ac.kr
Website: http://ltefuzz.syssec.kr

BACKUP SLIDES

Obtaining valid S-TMSIs

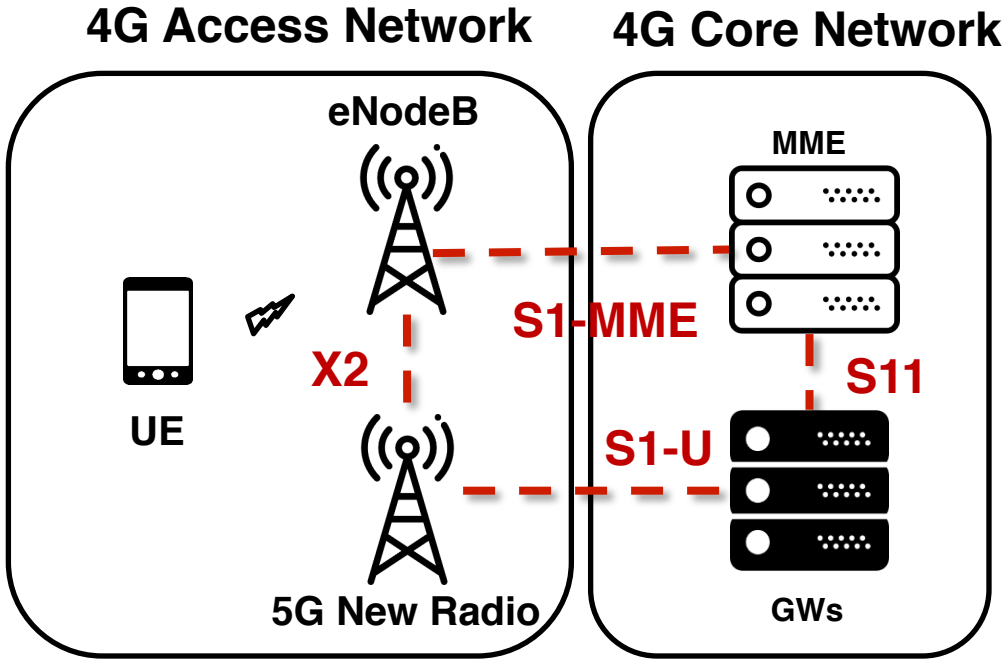
1. Install Fake LTE eNodeB
   - Obtain a UE's S-TMSI in the *TAU request* from the UE.
2. Periodically trigger *Paging* by making calls to the victim UE
   - The attacker listens pagings in a same eNodeB with the victim UE
3. Sniff downlink *RRC Connection setup*

LTE testbed: open source vs. commercial

- Commercial testbed
  - Expensive
  - Hard to change, modify the behaviors
- Open source testbed
  - **Cheap** (Laptop + SDR = 3,500,000 KRW)
  - **Fully controllable** from PHY to A PP layer

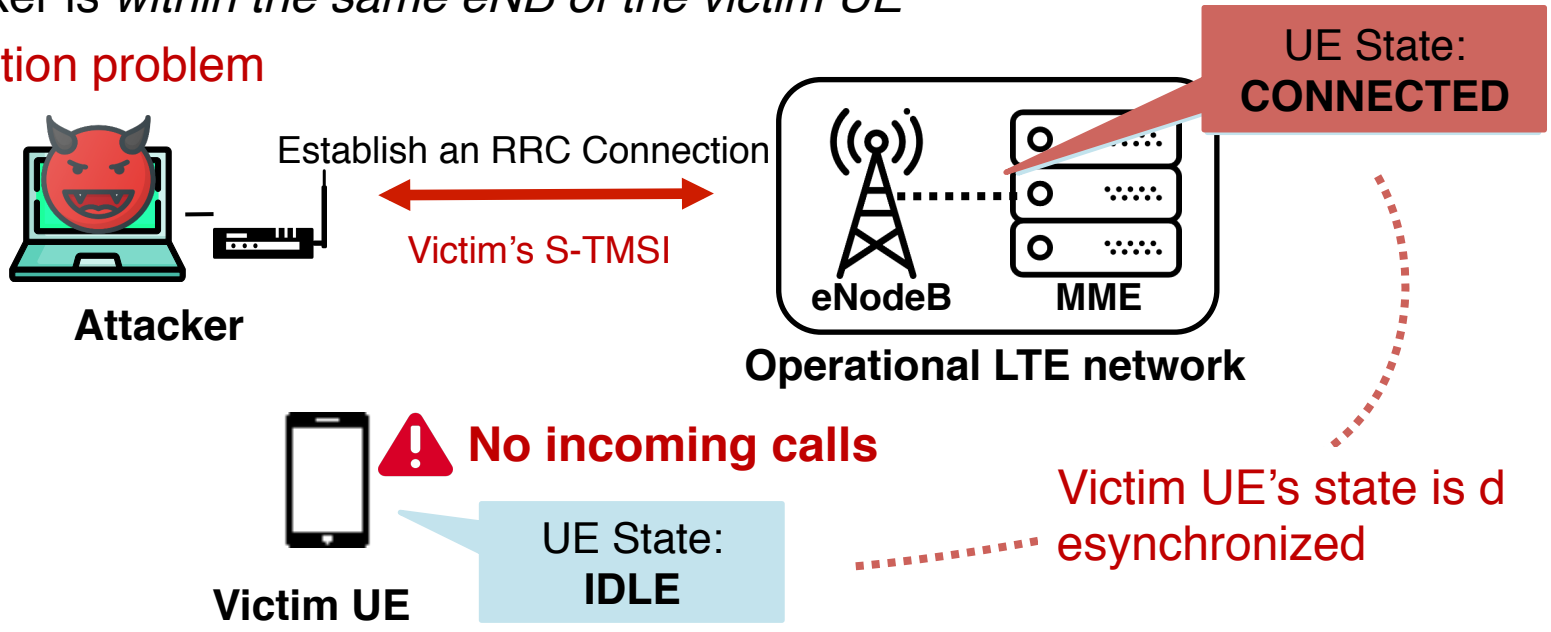
Future work

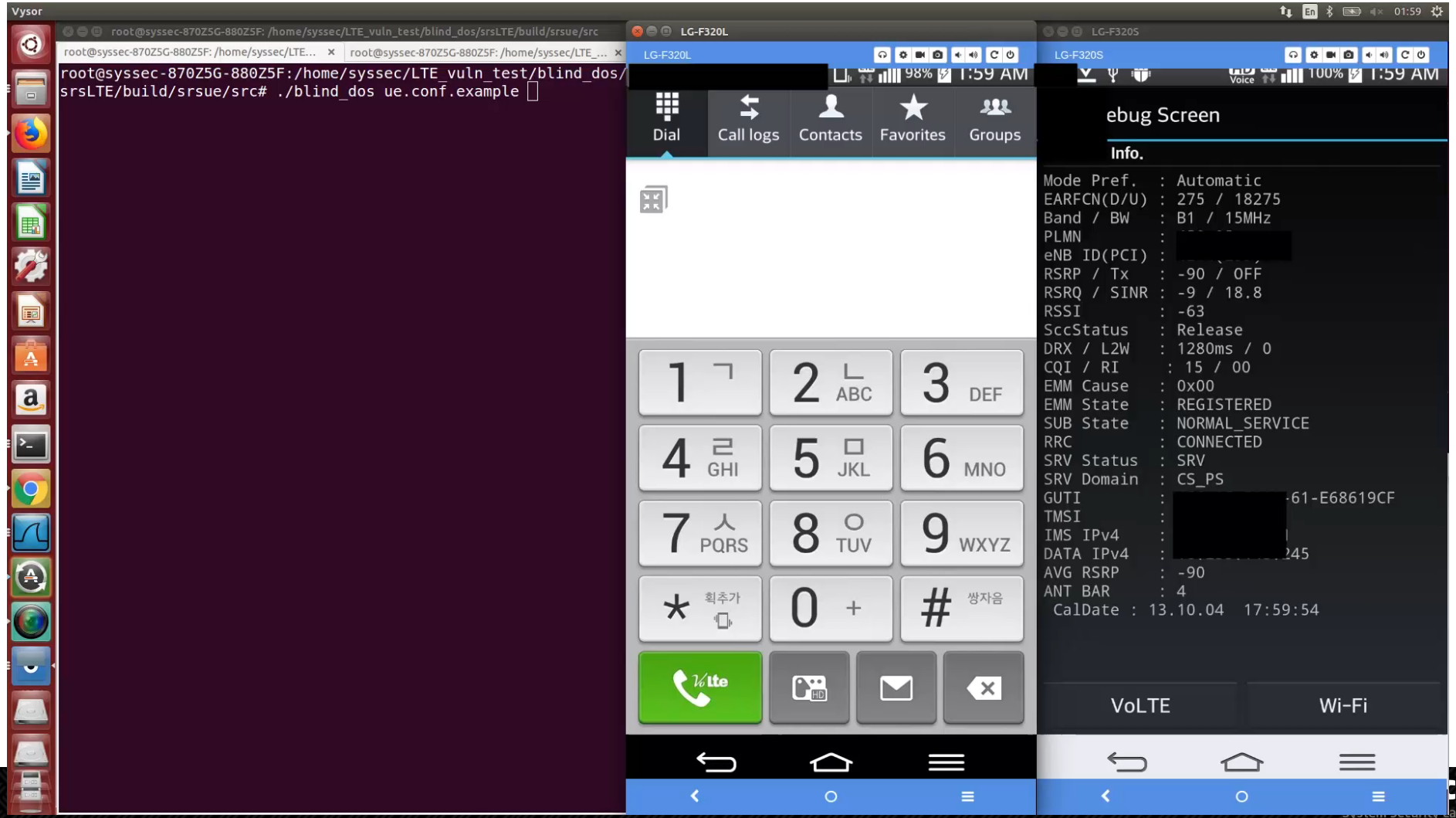
- Extend LTEFuzz to
  - support other protocol layers and interfaces
  - support 5G Non-Standalone (NSA) and Standalone (SA)
  - identify memory corruption b ugs in the baseband chipsets and core networks, if allowe d



Blind DoS attack

- **Exploited test case:** Invalid *RRC Connection request*
- An Attacker deceives the network that the victim UE is in connected state
- An Attacker is *within the same eNB of the victim UE*
- Specification problem



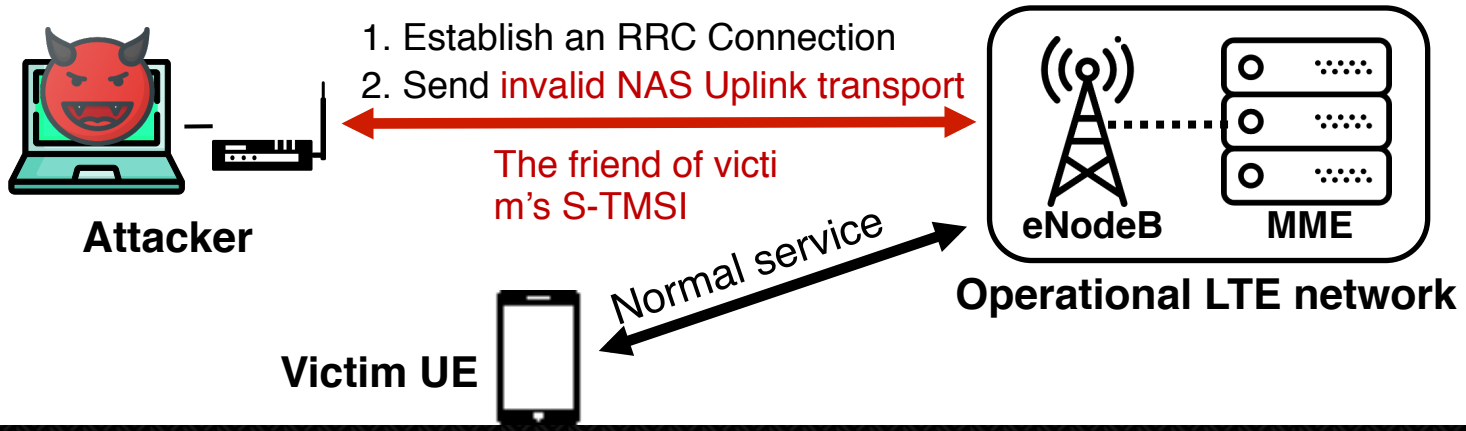

Vysor
root@syssec-870Z5G-880Z5F: /home/syssec/LTE_vuln_test/blind_dos/srsLTE/build/srsue/src
root@syssec-870Z5G-880Z5F: /home/syssec/LTE...
root@syssec-870Z5G-880Z5F: /home/syssec/LTE_...
root@syssec-870Z5G-880Z5F:/home/syssec/LTE_vuln_test/blind_dos/srsLTE/build/srsue/src# ./blind_dos ue.conf.example
LG-F320L
LG-F320L
98% 1:59 AM
Dial
Call logs
Contacts
Favorites
Groups
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
* 확추가
0 +
쌍자음
LG-F320S
LG-F320S
100% 1:59 AM
ebug Screen
Info.
Mode Pref. : Automatic
EARFCN(D/U) : 275 / 18275
Band / BW : B1 / 15MHz
PLMN :
eNB ID(PCI) :
RSRP / Tx : -90 / OFF
RSRQ / SINR : -9 / 18.8
RSSI : -63
SccStatus : Release
DRX / L2W : 1280ms / 0
CQI / RI : 15 / 00
EMM Cause : 0x00
EMM State : REGISTERED
SUB State : NORMAL_SERVICE
RRC : CONNECTED
SRV Status : SRV
SRV Domain : CS_PS
GUTI :
TMSI :
IMS IPv4 :
DATA IPv4 :
AVG RSRP : -90
ANT BAR : 4
CalDate : 13.10.04 17:59:54
VoLTE
Wi-Fi

SMS phishing

- **Exploited test case:** Invalid Uplink NAS transport (SMS transport)
- Message with either no encryption, invalid MAC, or invalid seq. are all accepted
- An Attacker is *within the same MME pool of the victim UE's friend*
- Implementation

Sender: victim's friend
Content: Visit http://evil.com

Does not check the validity



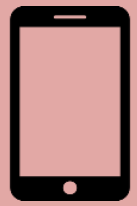
Attacker model

Attacker (Malicious UE)

- No keys for enc./integrity
- Knows the victim UE's identity
- Attacker can locate victim UE:
  - Same cell area
  - Different cell, same eNodeB
  - Different eNodeB, but same MME pool
  - Different MME pool

Malicious behavior as if it is the victim UE

Registered



Victim UE