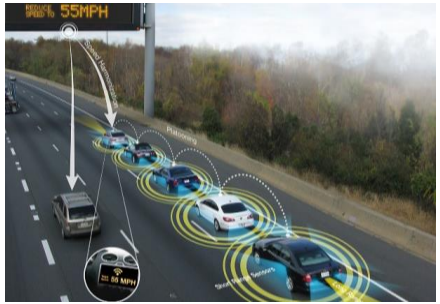
Touching the Untouchables:
Dynamic Security Analysis of the LTE Control Plane

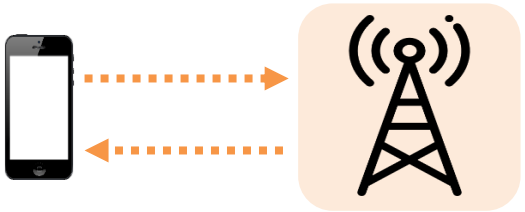
Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim

2019 IEEE Symposium on Security and Privacy

LTE communication is everywhere



Autonomous driving
(Cellular V2X)



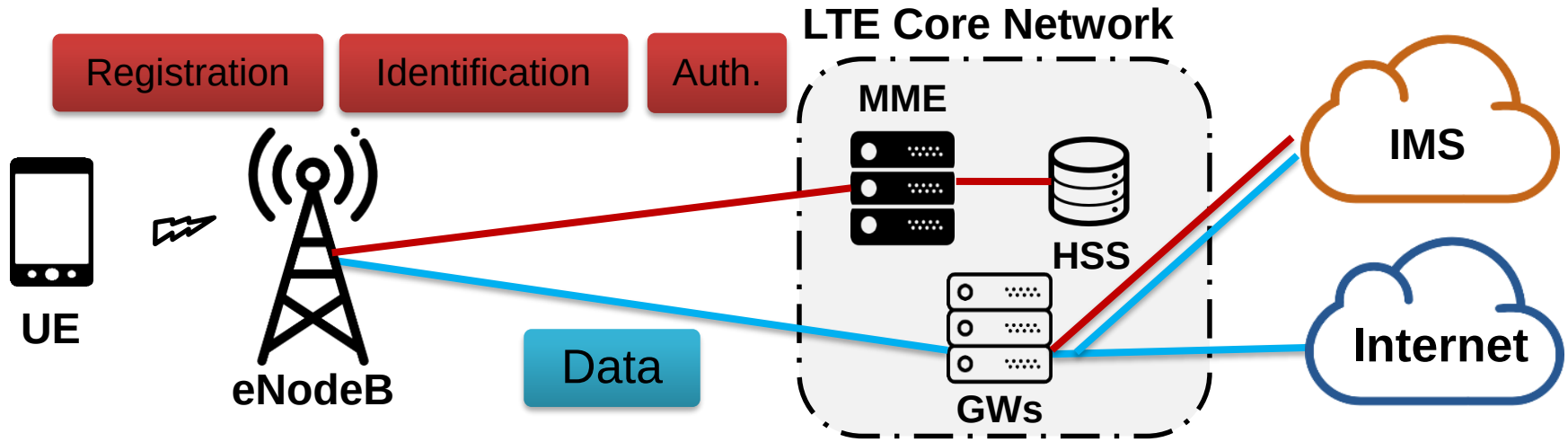
Public safety services
(PS-LTE)

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

Related work

❖ **Formal analysis**

- "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE"(NDSS), 2018.

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

❖ **Fake base station(FBS) & Implementation bugs**

- "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems," (NDSS), 2016.

What about a fake LTE phone to inspect commercial networks?

Challenges in active network testing

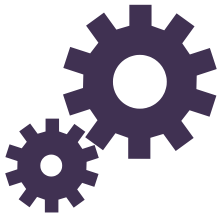
- Difficulties to actively inspect operational LTE networks
  1. Sending malicious signal to a commercial network is not allowed
     - ➔ Got Carriers' Testbed access
  2. It is hard to control baseband chipsets for simulating malicious behavior
     - ➔ Use open-source LTE software (srsLTE, openLTE,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

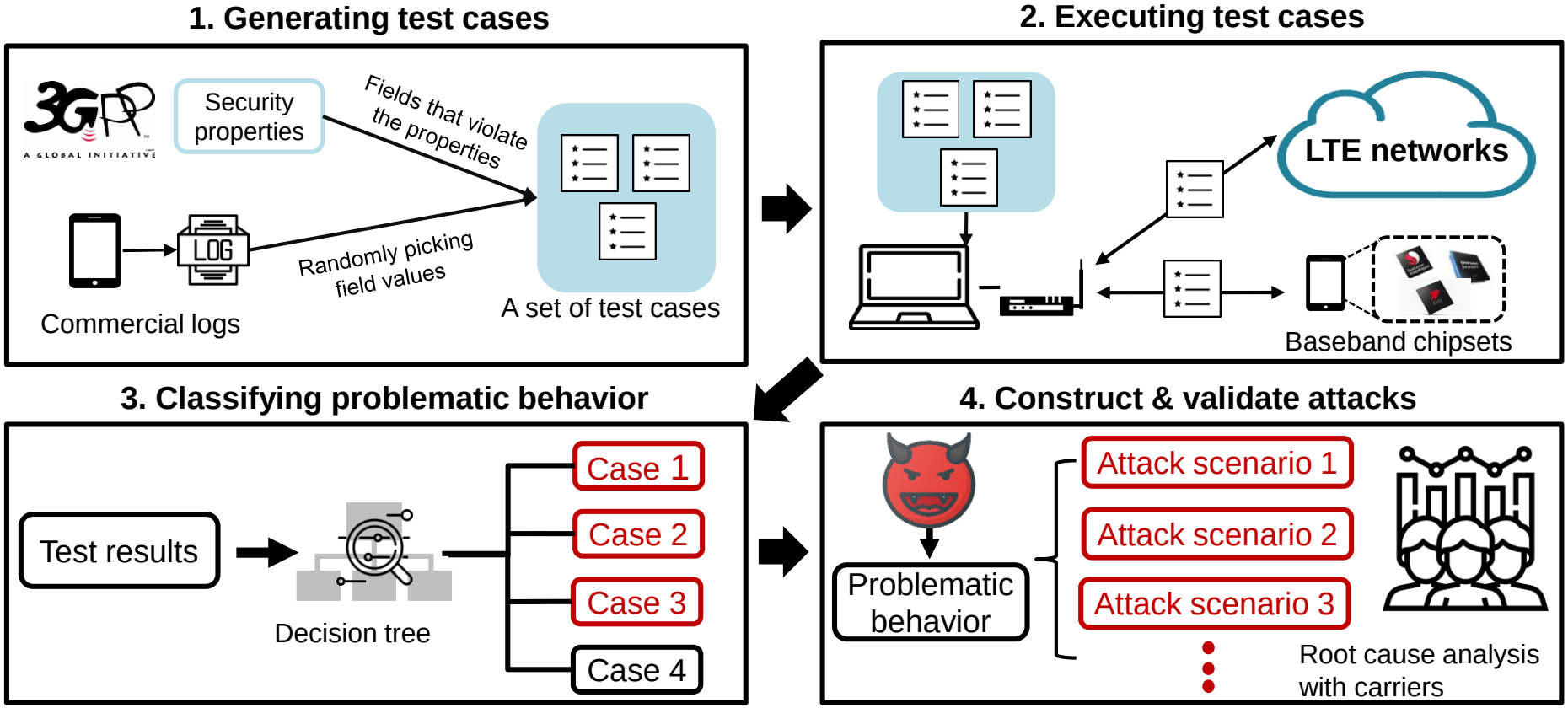


Configuration bug

  - **How?**

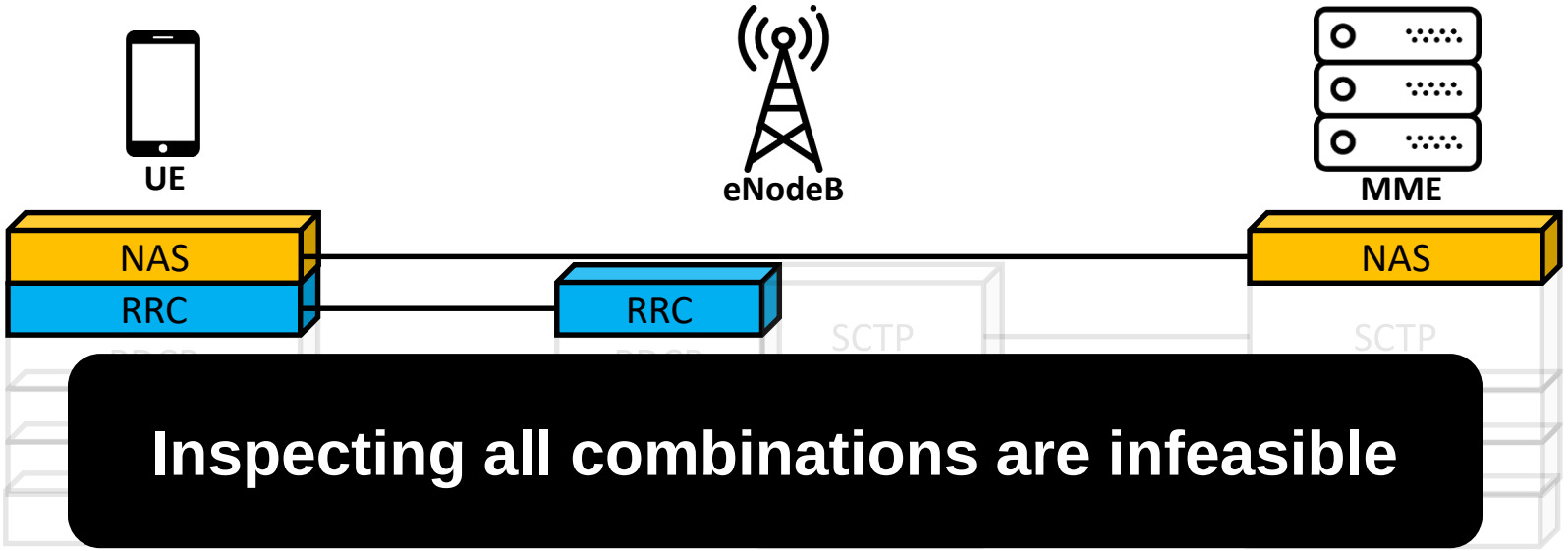
Comprehensive dynamic testing against commercial LTE networks

Overview of LTEFuzz



Generating test cases

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



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

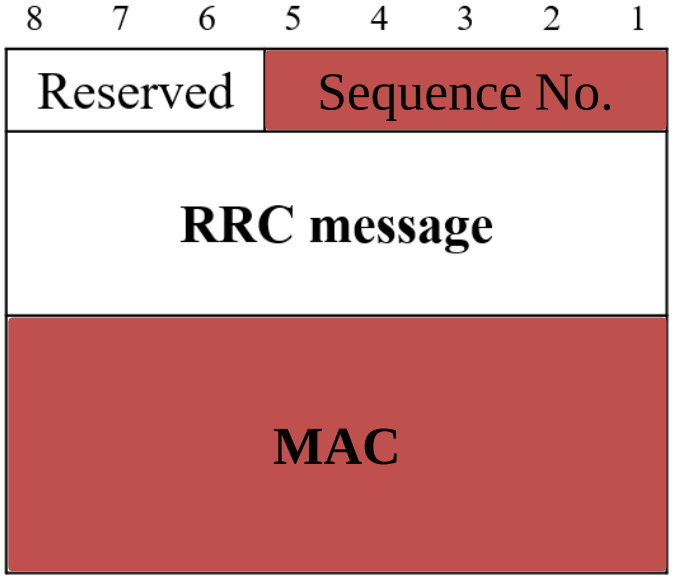
Generate test cases that violate the properties

Plain message : unencrypted message

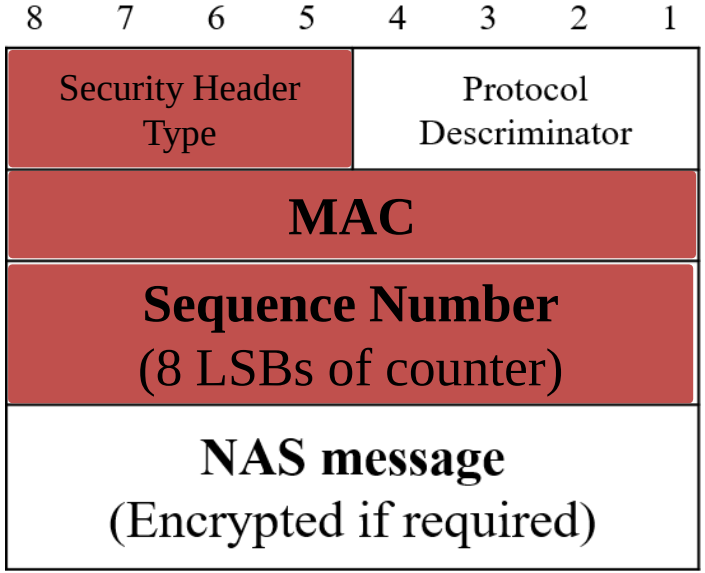
Generating test cases

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

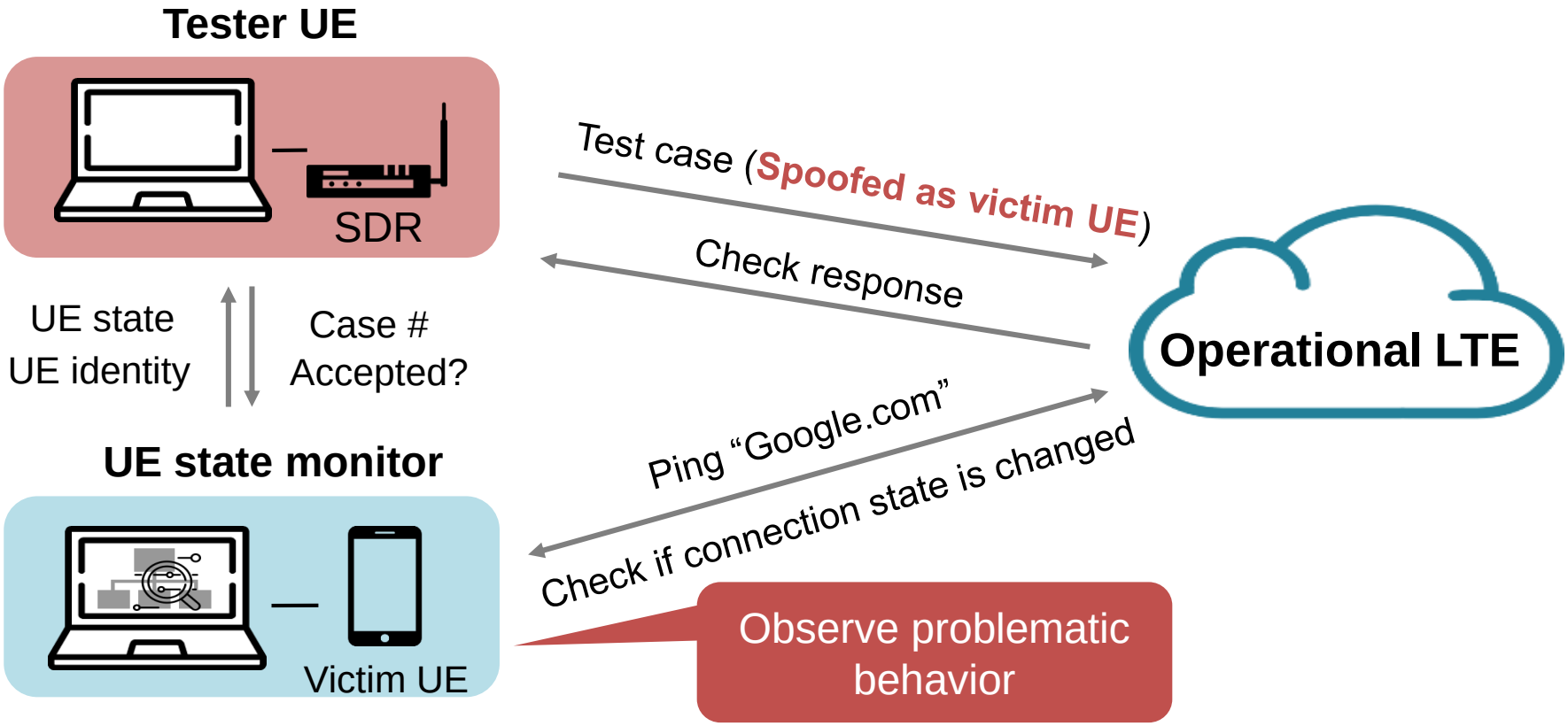
RRC test case



NAS test case



Executing test cases



LTEFuzz test environment

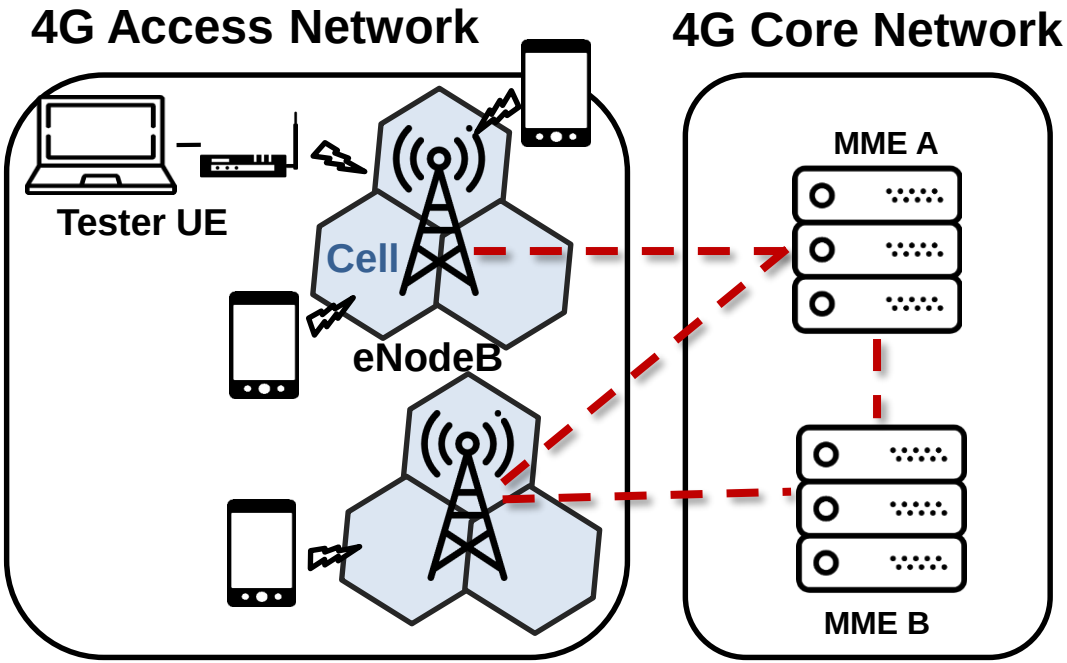
Network testing

- 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

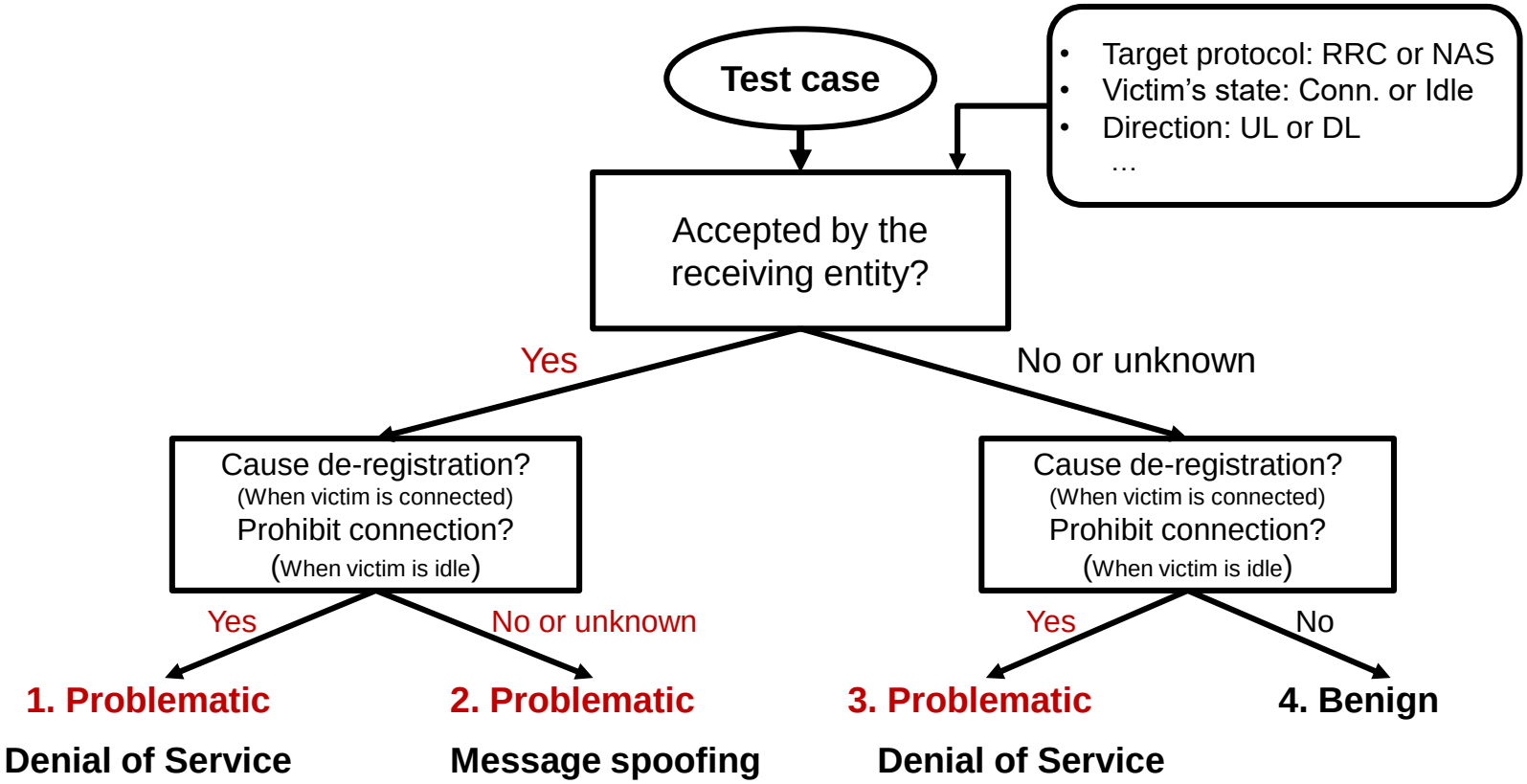
Operational networks are complicated



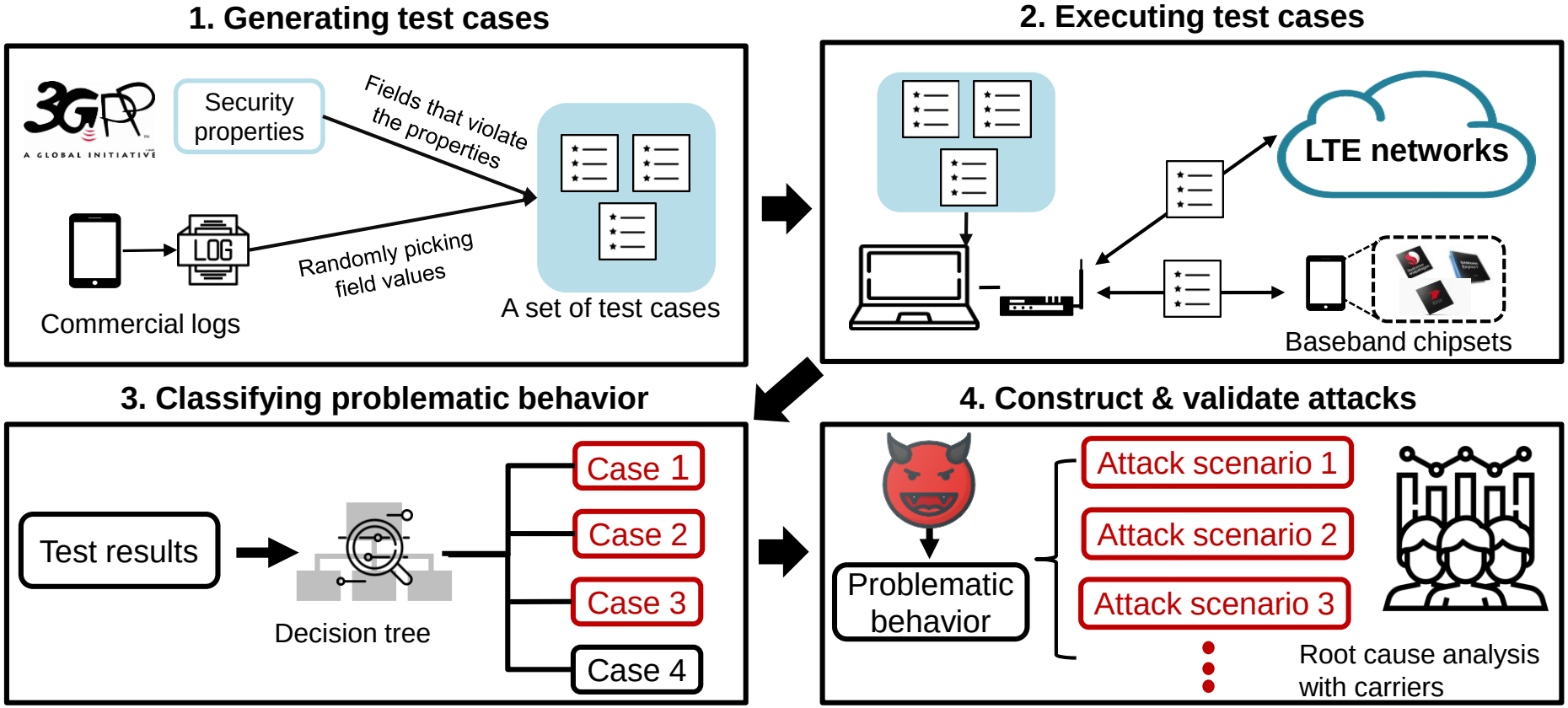
- Each carrier has different configurations
- Each carrier deploys different network equipment

Hard to manually analyze which case is problem

Classifying the problematic behavior



Overview of LTEFuzz



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

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

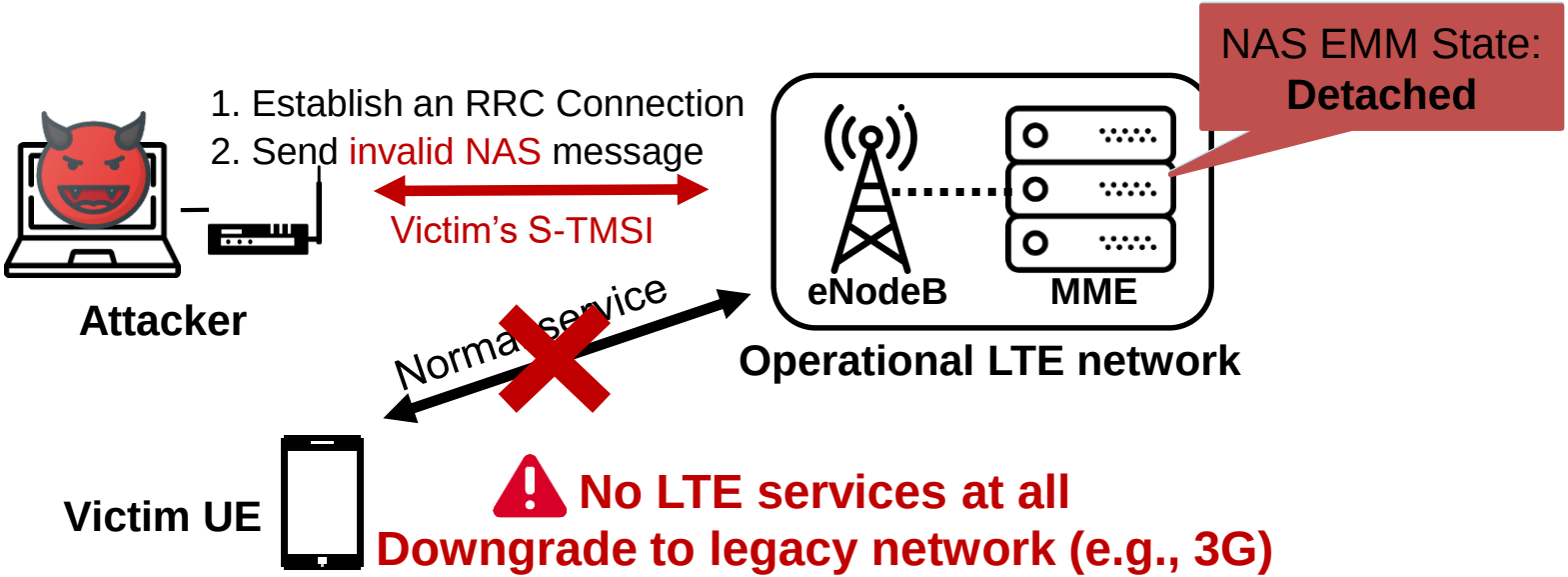
I: Invalid MAC

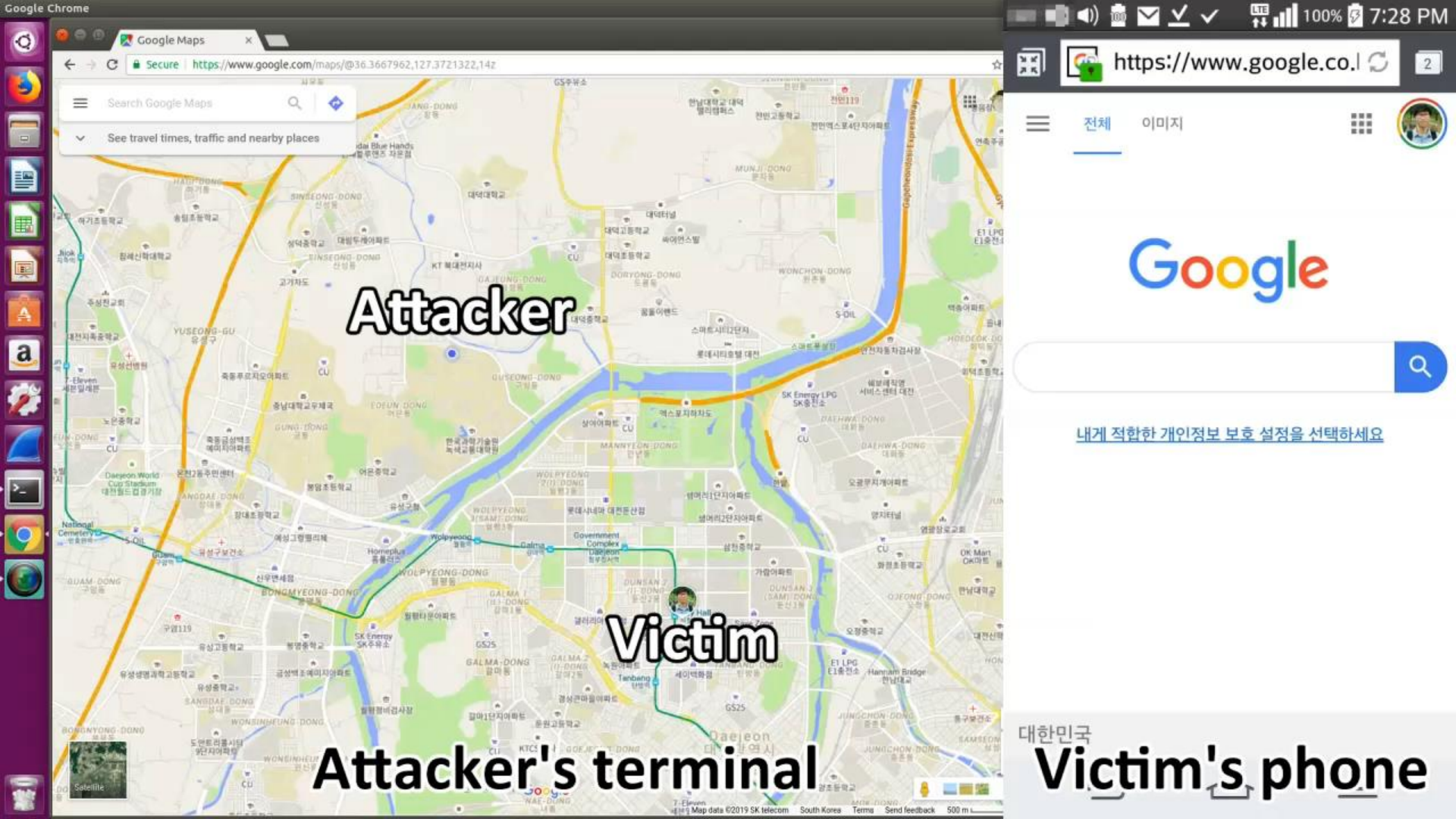
R: Replay

ATTACKS

Remote de-register attack

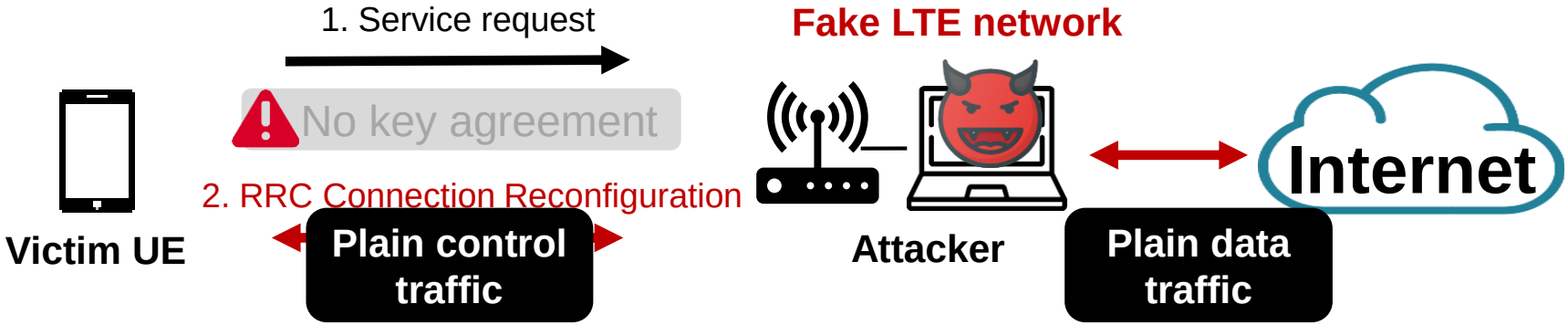
- **Exploited test case:** 15 cases in NAS (Attach, Detach, TAU, PDN con/discon…)
- Implementation bugs & configuration mistakes




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
Satellite
Map data ©2019 SK telecom South Korea Terms Send feedback 500 m
100% 7:28 PM
https://www.google.co.
전체
이미지
Google
내게 적합한 개인정보 보호 설정을 선택하세요
대한민국
Victim's phone

AKA Bypass attack

- Exploited test cases
  - RRC Security Mode Command bypass (key agreement procedure)
- Implications
  - Eavesdropping user data traffic
  - Redirecting to fake online payment websites



Countermeasure

- Attacks exploiting **eNB**
  - Reduce the inactivity timer value to allow an RRC Connection that is unresponsive to the Authentication request to expire.
  - re-assign the S-TMSI when a number of RRC Connection requests using the same S-TMSI are received.
- Attacks exploiting **MME and UE**
  - MMEs, UE should be carefully implemented **by strictly following the 3GPP standard**

Conclusion

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

- They have implemented LTEFuzz
  - A **semi-automated dynamic testing tool** for both networks and devices
  - Specification problems: 16, Implementation bugs + configuration issues: 35
  - **LTEFuzz considers realistic attack assumptions in operational LTE network**

Follow-up work

- **Bookworm Game: Automatic Discovery of LTE Vulnerabilities Through Documentation Analysis (IEEE S&P 2021)**
  - utilizes NLP and ML techniques to scan a large amount of LTE documentation for hazard indicators(HIs).
  - The HIs discovered are analyzed to generate test cases.

- **DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices (Usenix 22)**
  - Stateful negative testing : tests the content by defining negative testing that is not properly defined in the specification.

Questions

❖ **1. Hyunsik Jeong (Best question)**

- LTEFuzz can be classified as a black-box, stateless fuzzer. What is the main difficulty to make it stateful, and which method can be applied for the stateful fuzzer?

- Will take a lot of time and there will be difficulties in classifying the response.
- DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices (Usenix 22)

Questions

- 2. Youngjin Jin
  - In this paper, LTEFuzz is introduced as a stateless fuzzer. Traditional fuzzers usually take randomly generated inputs to look for potential bugs. Does this fuzzer only utilize crafted test cases through the use of security properties or are there any random explorations involved?

  - They generated the test cases with the intention of not causing a crash.

- 3. Wooyoung Go
  - If the author replace the simple decision tree algorithm to recent deep learning algorithm, the performance will be better??

  - will not help much and only consume time and resources

Thank you