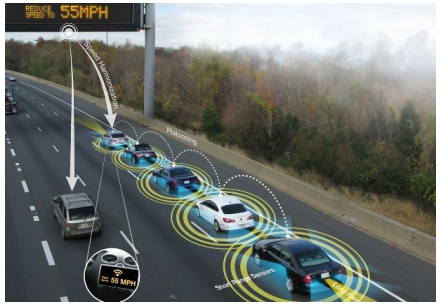
Touching the Untouchables:
Dynamic Security Analysis of the LTE Control Plane

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

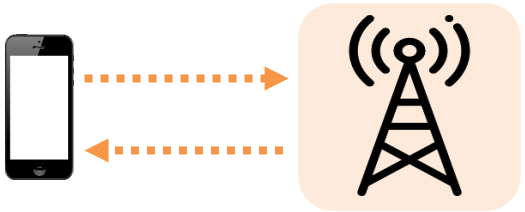
2019 IEEE Symposium on Security and Privacy

Presenter: Kwangmin Kim

LTE communication is everywhere



Autonomous driving
(Cellular V2X)



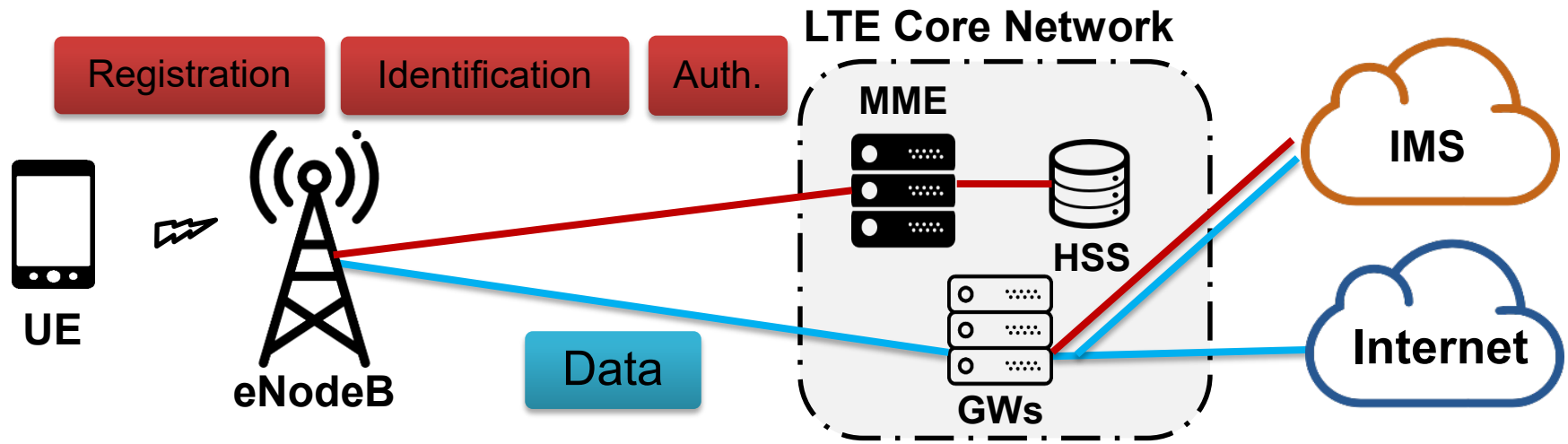
Public safety services
(PS-LTE)

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

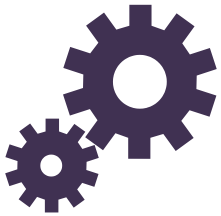
- Difficulties to actively inspect operational LTE networks
  1. Sending malicious signal to a commercial network is not allowed
     - ➔ Got Carriers' Testbed access
  2. It is hard to control baseband chipsets for simulating malicious behavior
     - ➔ Use open-source LTE software (srsLTE, openLTE,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

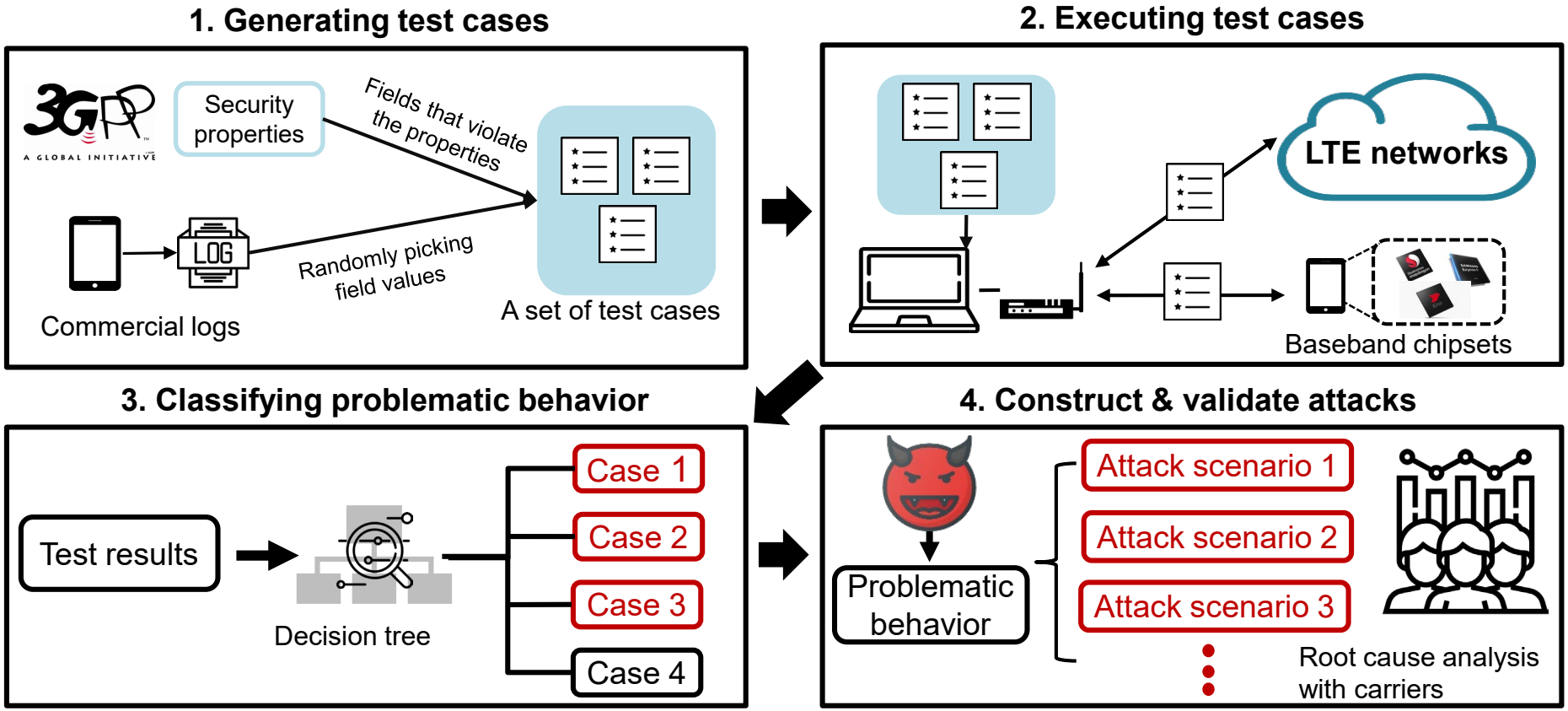


Configuration bug

  - **How?**

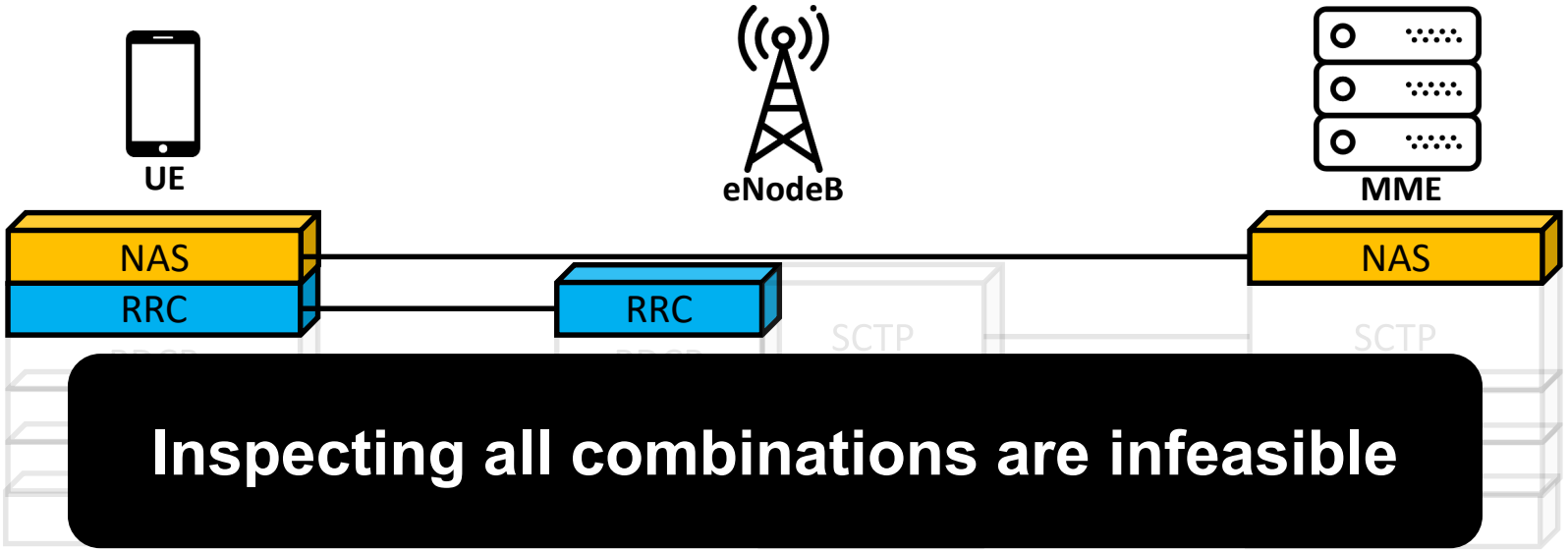
Comprehensive dynamic testing against commercial LTE networks

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

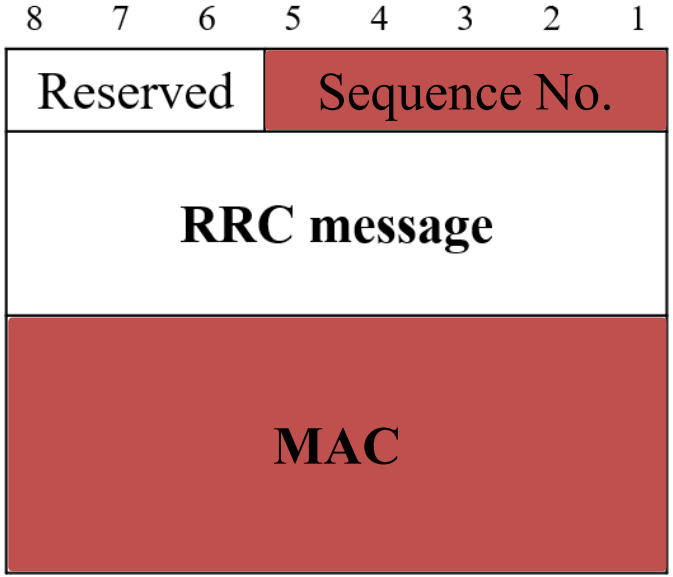
Generate test cases that violate the properties

Plain message : unencrypted message

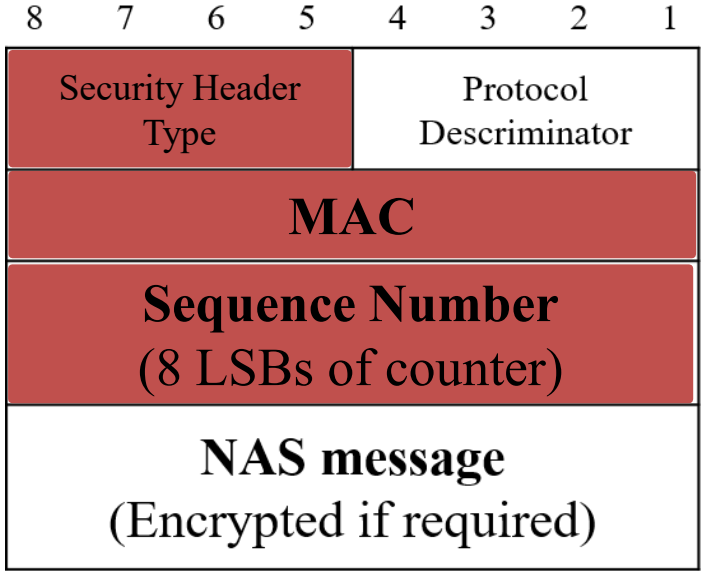
Generating test cases

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

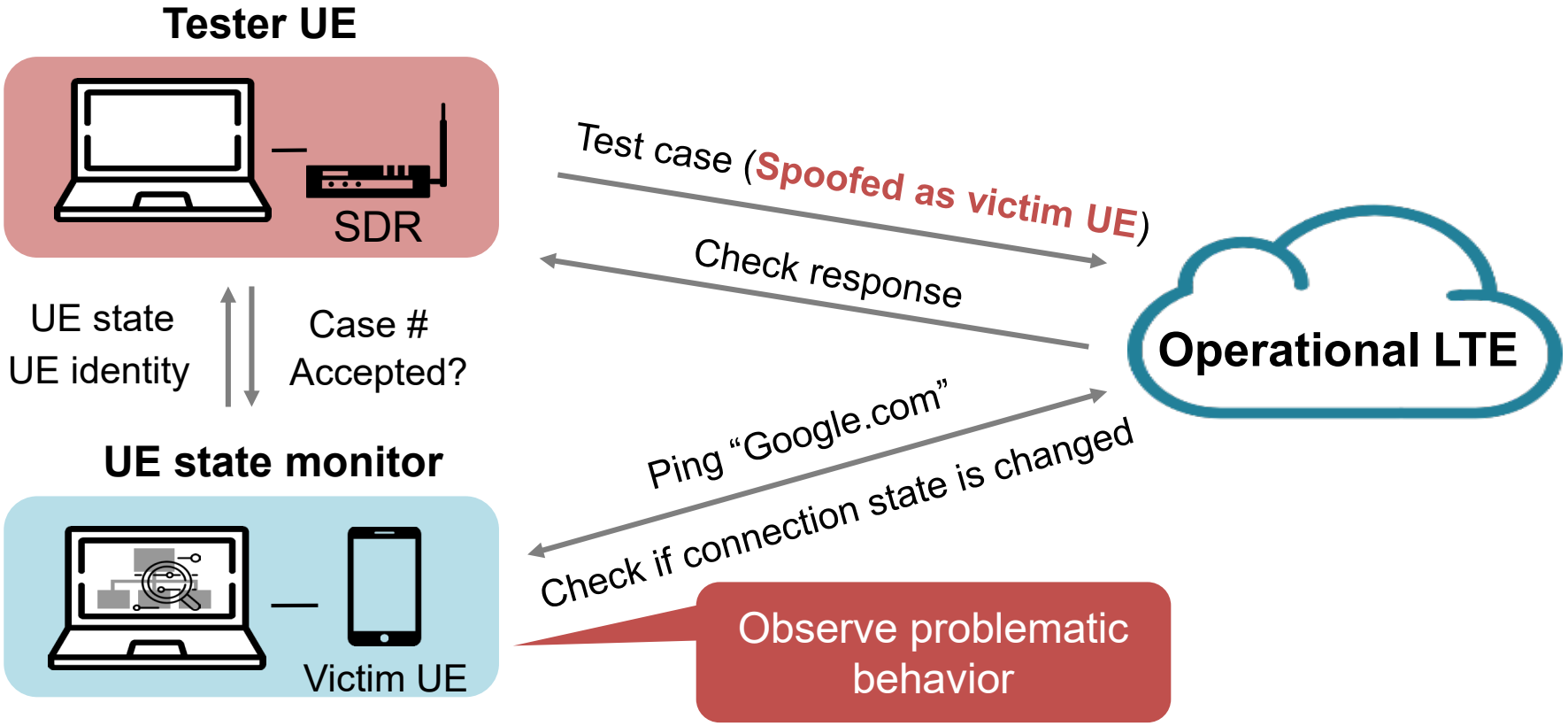
RRC test case



NAS test case



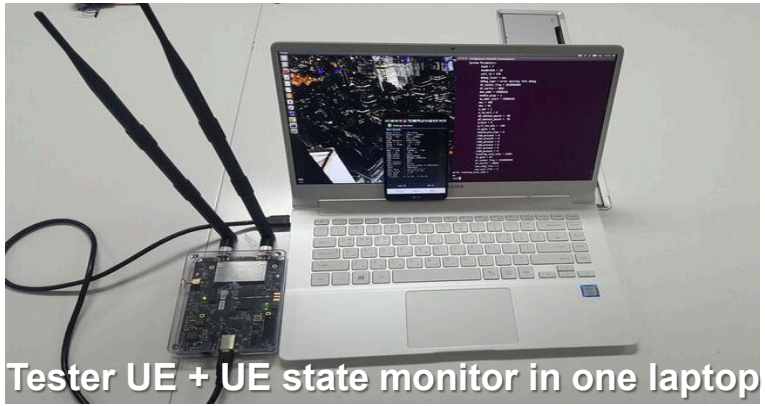
Executing test cases



LTEFuzz test environment

Network testing

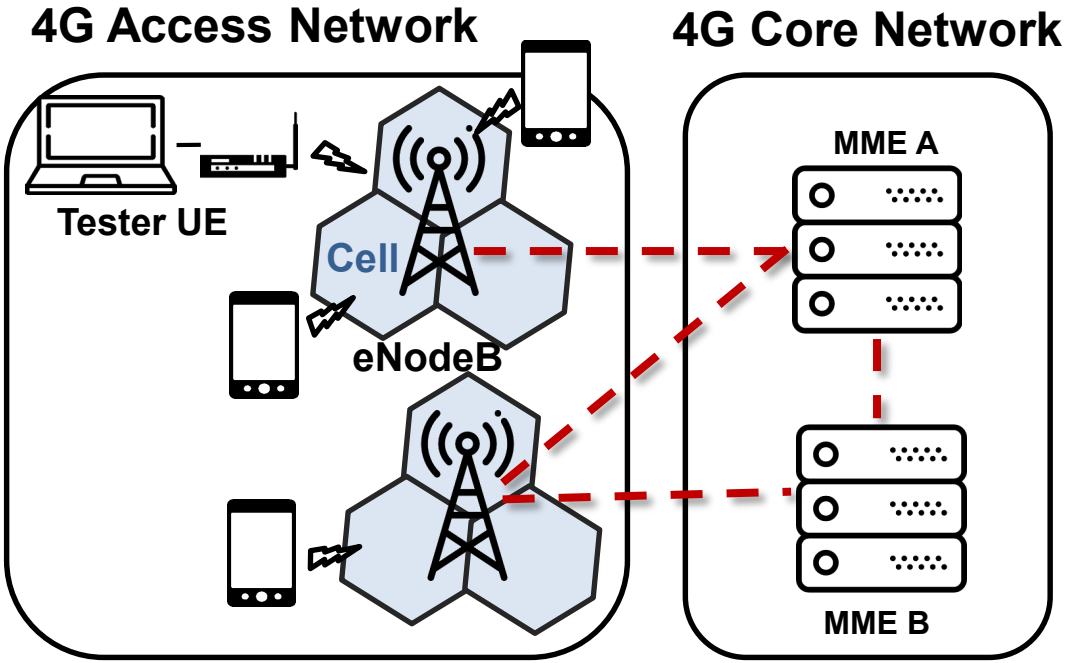
- Target network vendors
  - Carrier A: two MME vendors, one eNB vendor
  - Carrier B: one MME vendor, two eNB vendors



Baseband testing

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

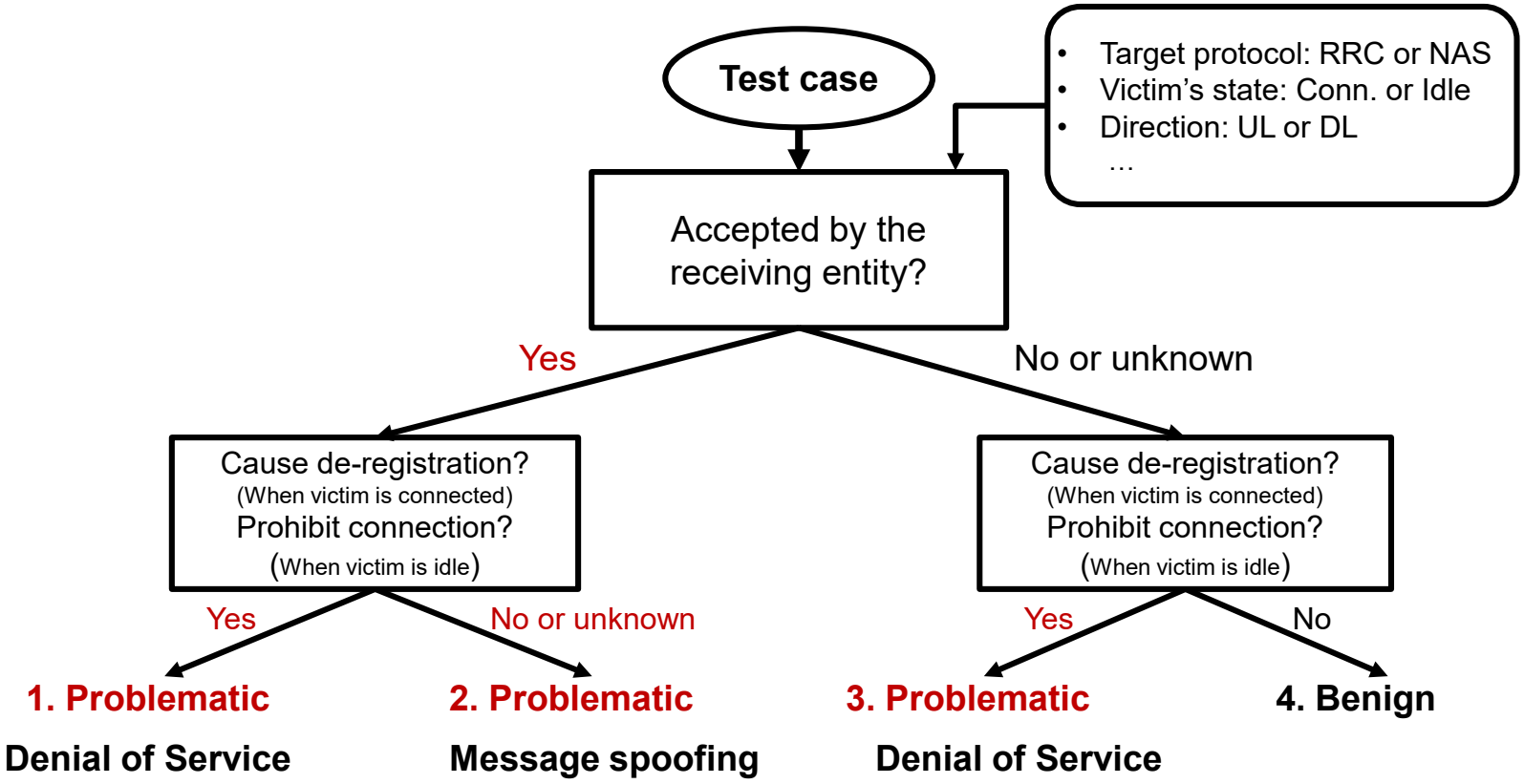
Operational networks are complicated



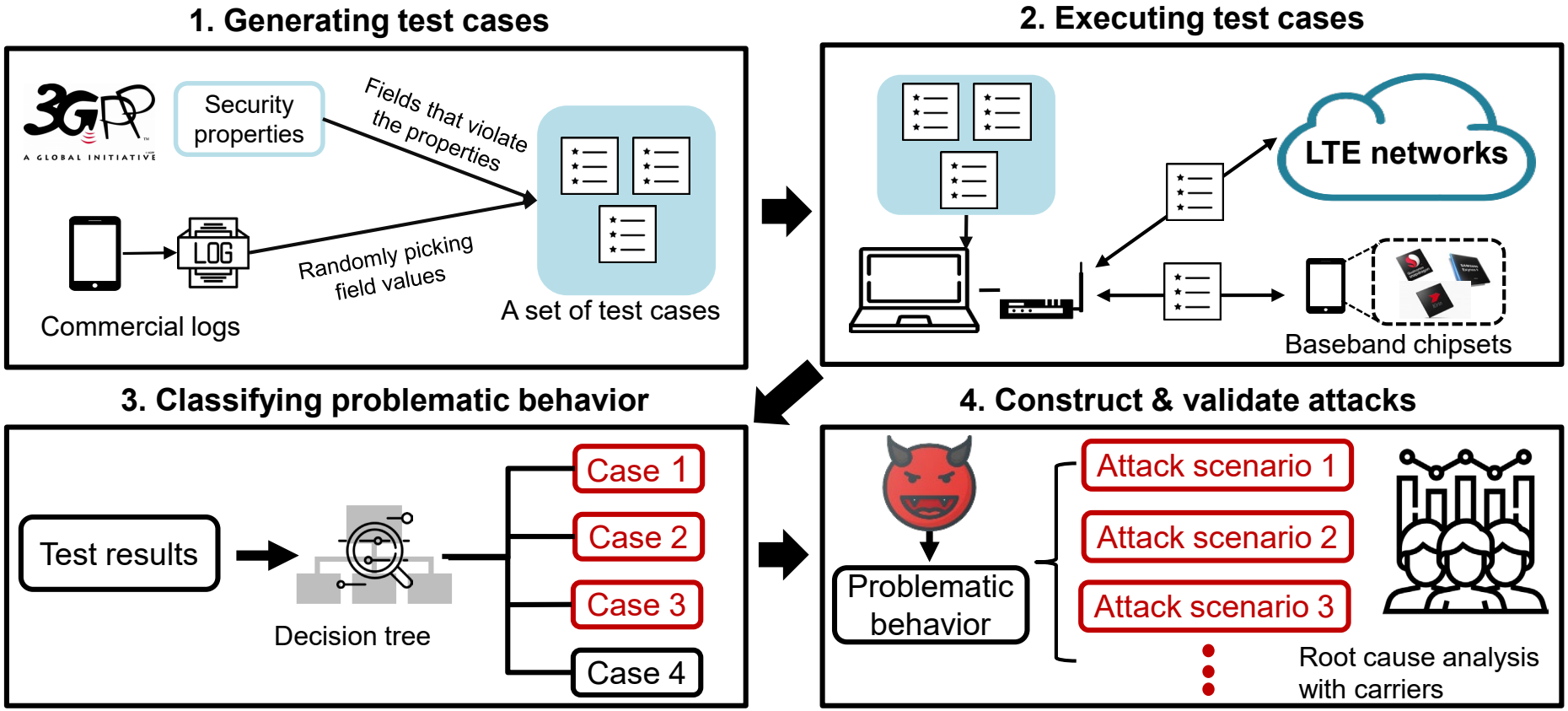
- Each carrier has different configurations
- Each carrier deploys different network equipment

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

Findings

- Result of dynamic testing against different MME types
  - Carrier 1: MME1, MME2, Carrier2: MME3 (MME1 & MME3: the same vendor)

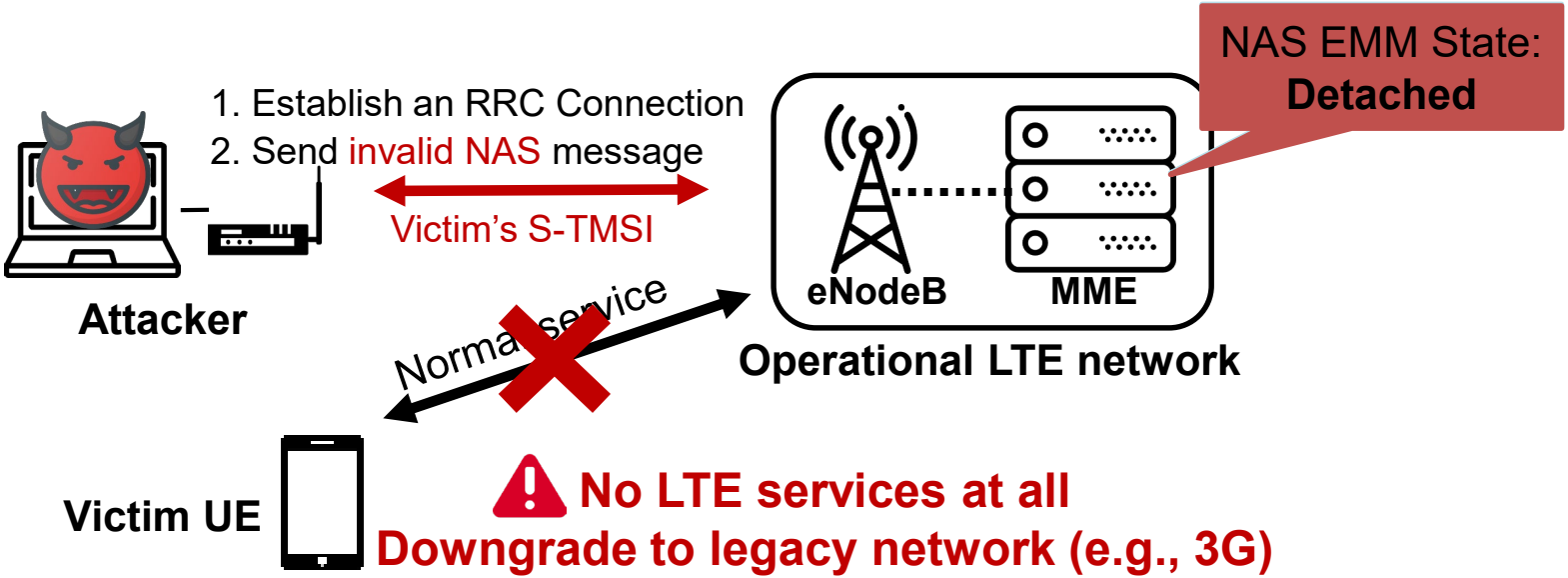
Exploited NAS Messages	Implications		
	MME_1	MME_2	MME_3
Attach Request	DoS (**P**, **I**, **R**)	×	DoS (**P**, **I**, **R**)
TAU Request	DoS (**P**, **I**, **R**)	×	DoS (**I**), False location update (**R**)
Uplink NAS Transport	DoS (**P**, **I**), SMS phishing (**R**)	SMS phishing (**P**, **I**, **R**)	-
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

ATTACKS

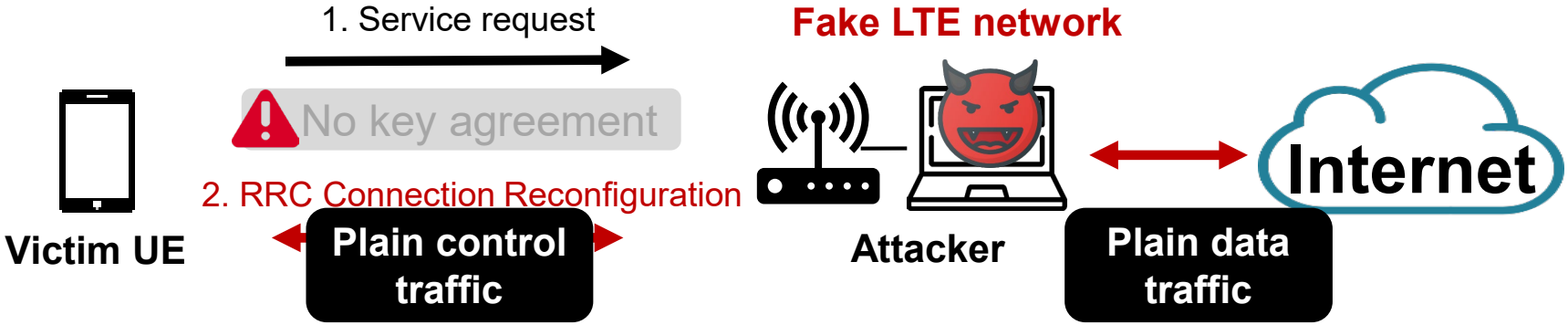
Remote de-register attack

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



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.

- **Noncompliance as Deviant Behavior: An Automated Black-box Noncompliance Checker for 4G LTE Cellular Devices (ACM CCS 2021)**
  - Extract a behavioral abstraction of the protocol implementation
  - Identify diverse noncompliant behavior in a property-agnostic way

Follow-up work

- **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.
  - Post-AKA flaw: accept unprotected messages with certain message types after security activation

S: Security header type mishandling		D	L	B	A
S1	Accept invalid security header types for certain message types	5	0	0	0
S2	Accept invalid security header type for certain UE states	3	2	0	0
S3	Mishandle reserved security header type	1	0	0	0
M: Message type mishandling		**D**	**L**	**B**	**A**
M1	Accept prohibited message types before security activation	2	2	0	0
M2	Accept unprotected messages with certain message types after security activation	6	0	0	20
I: IE/value mishandling		**D**	**L**	**B**	**A**
I1	Accept prohibited IEs	3	1	0	0
I2	Accept prohibited values	3	0	0	0
I3	Mishandle reserved values	3	0	2	0
I4	Mishandle reserved IEs	0	0	47	0

D: DoLTEst, **L**: LTEFuzz, **B**: BaseSpec, **A**: Atomic

Best Question

- **What difficulties exists to make a stateful fuzzer? (Jaehyun Ha)**
  - DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices (Usenix 22)

- **The follow up work use the Machine Learning technique to find the vulnerability, will it also make this work perform even better? (Zhixian Jin)**
  - Bookworm Game: Automatic Discovery of LTE Vulnerabilities Through Documentation Analysis (IEEE S&P 2021)
  - Sherlock on Specs: Building LTE Conformance Tests through Automated Reasoning (Usenix 23)
  - Hermes: Unlocking Security Analysis of Cellular Network Protocols by Synthesizing Finite State Machines from Natural Language Specifications (Usenix 24, to appear)

Best Question

- **Considering that multiple UEs, eNBs and MMEs are all required to follow a specific LTE standard, how would differential testing fare compared to the given methods in identifying problematic behaviors? (Seunghyun Lee)**
  - Noncompliance as Deviant Behavior: An Automated Black-box Noncompliance Checker for 4G LTE Cellular Devices (ACM CCS 2021)

Thank you ☺