BaseDiff: Differential Security Analysis of Cellular Basebands

Syed Rafiul Hussain

Assistant Professor

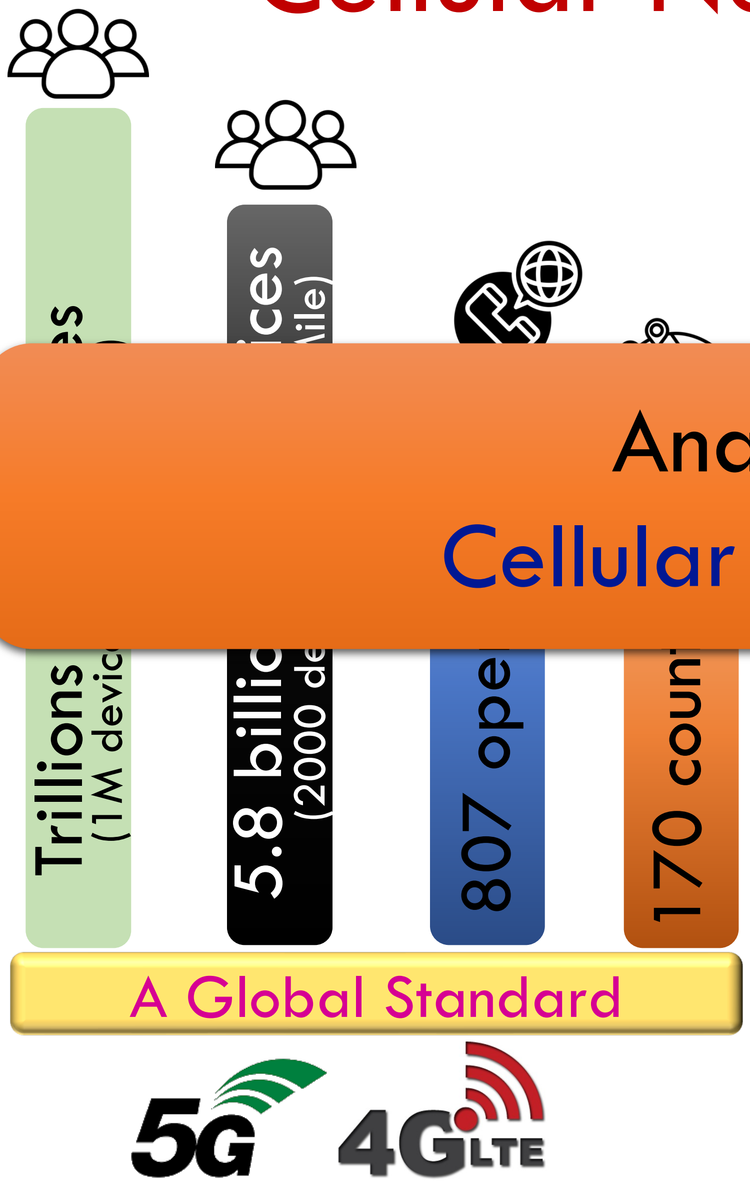
Department of Computer Science and Engineering

Pennsylvania State University

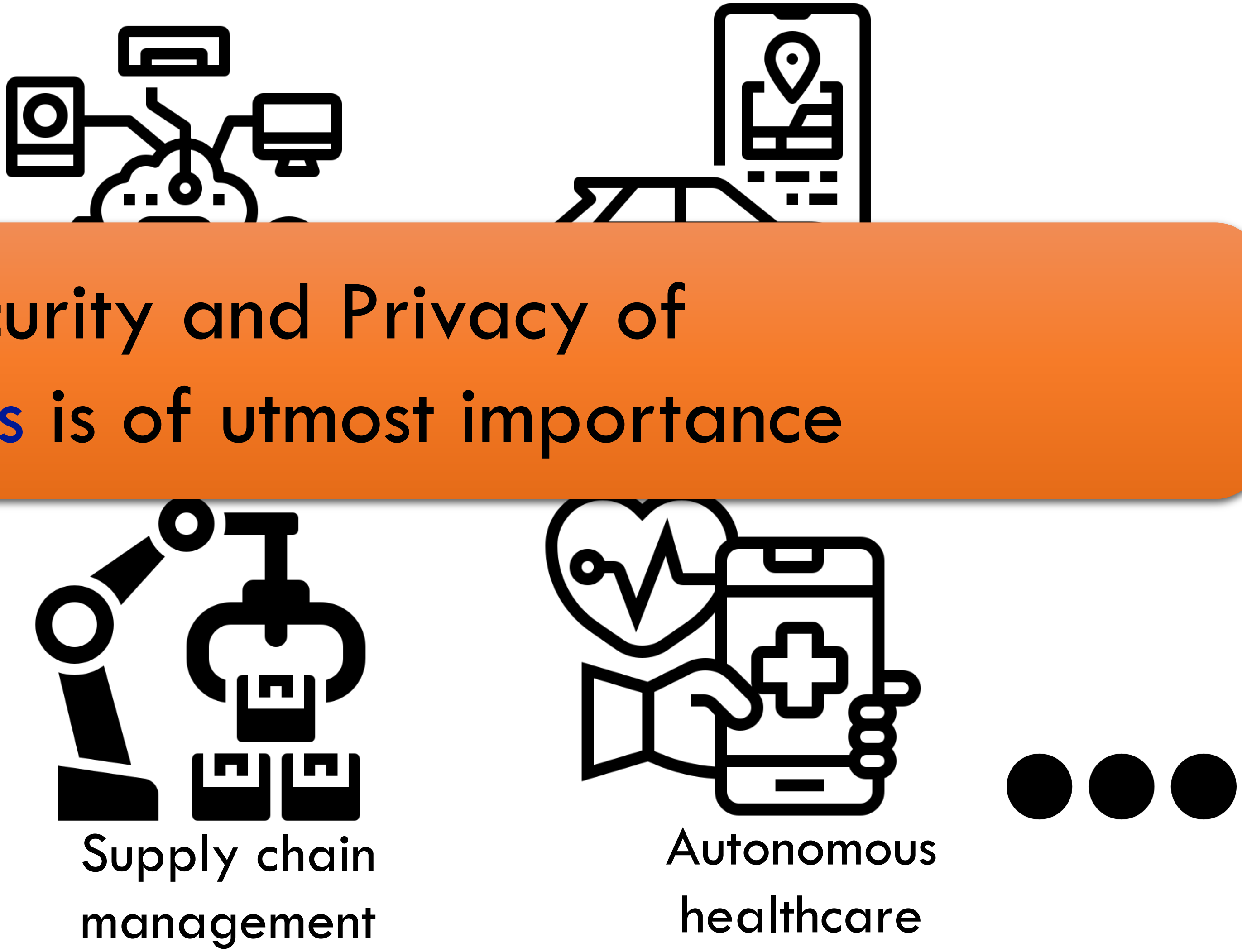
*Joint work with Imtiaz Karim, Abdullah Al Ishtiaq, Omar Chowdhury and Elisa Bertino

Qualcomm Product Security Summit 2022

Cellular Network Protocols: 4G and 5G



Analyzing Security and Privacy of
Cellular Basebands is of utmost importance



Security and Privacy Analysis Through Noncompliance Checking

Is it possible to design an **automated** security analysis framework that can uncover noncompliant behavior in protocol implementations of cellular (4G and 5G) basebands?

Deviating behavior

Interoperability issue

Challenges of Noncompliance Checking of Basebands

No formal specification

No formal Implementation

Black-box system

Stateful protocol

Limitations of Existing Approaches

Re-hosting and Reverse Engineering Basebands

(FirmWire - NDSS’22, BaseSpec – NDSS’21BaseSafe – WiSec’20)

✓ require a huge manual effort and expertise

✓ not general enough to implementations from different vendors

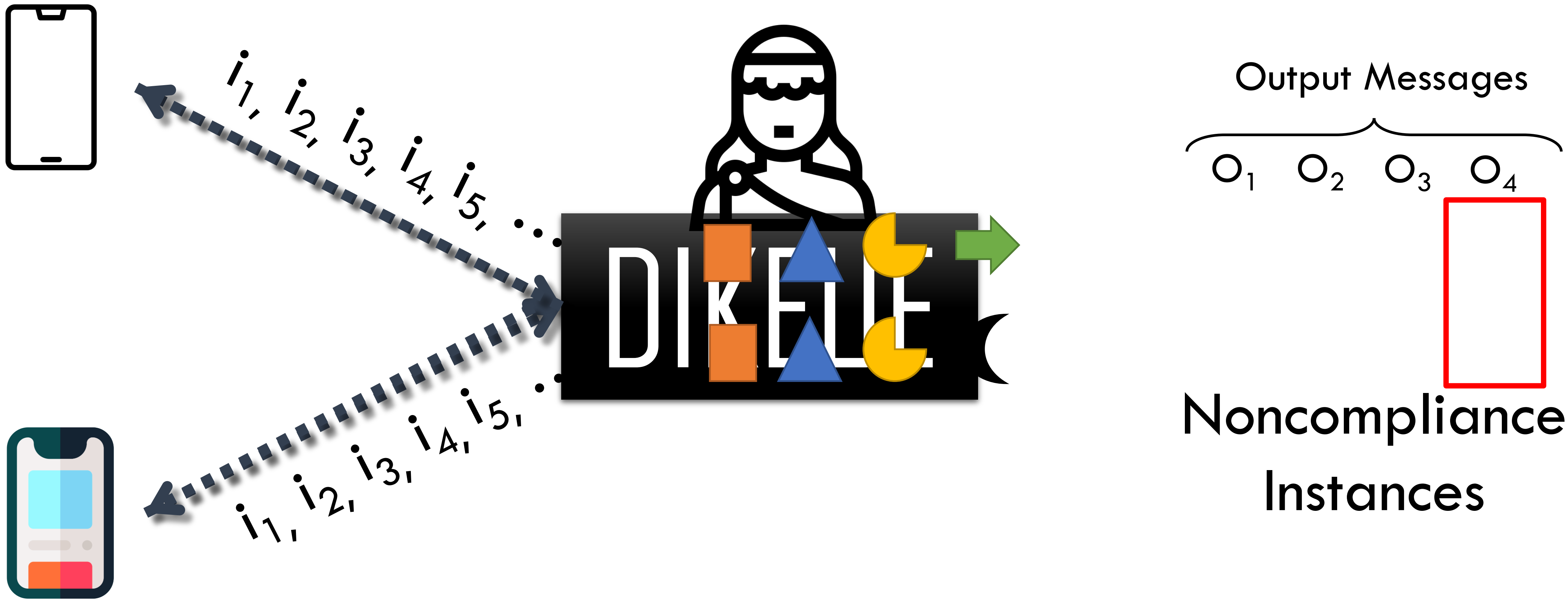
Stateless and Semiautomated Testing

(LTEFuzz-Oakland’19)

✓ Stateless testing is ineffective for stateful basebands

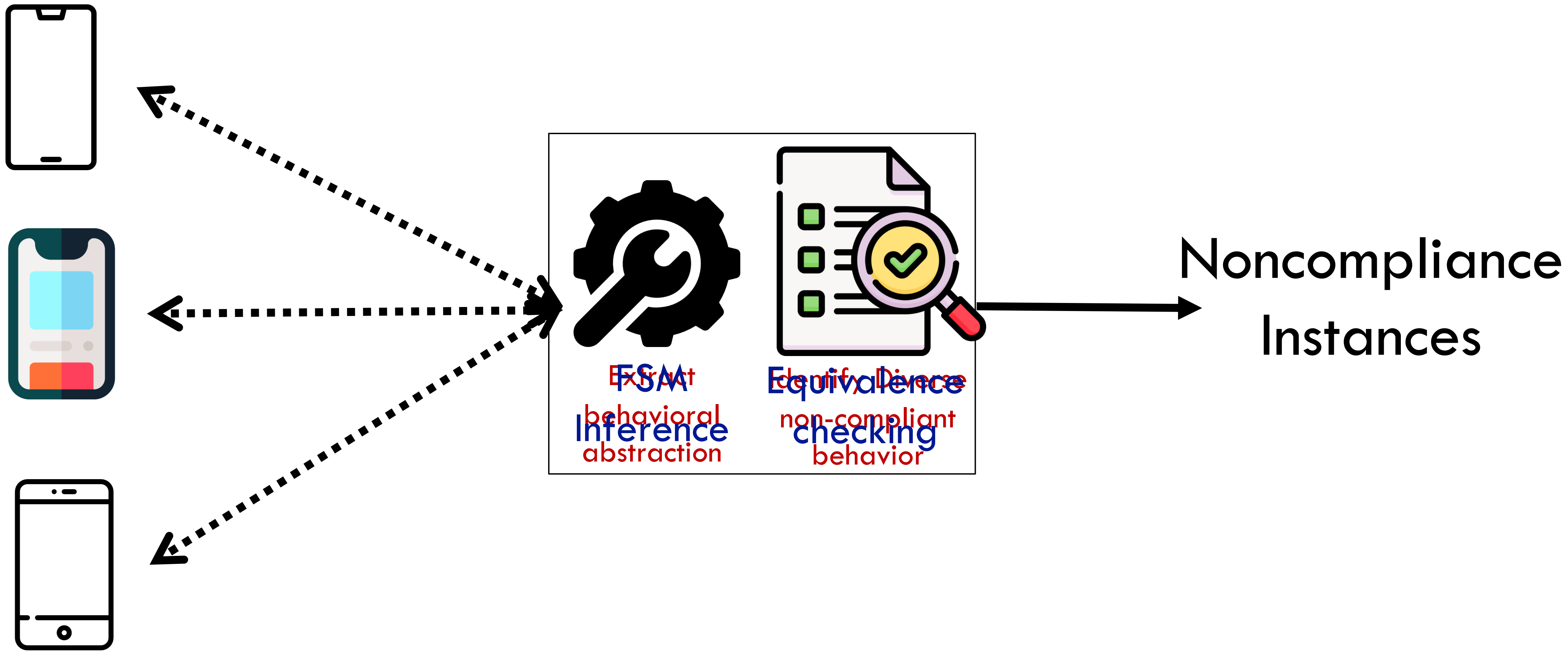
✓ Unable to find many flaws

Our Baseband Noncompliance Checker


$i_1, i_2, i_3, i_4, i_5, \dots$
$i_1, i_2, i_3, i_4, i_5, \dots$
Output Messages
O_1 O_2 O_3 O_4

Noncompliance Instances

Challenges of Developing DIKEUE



FSM Inference

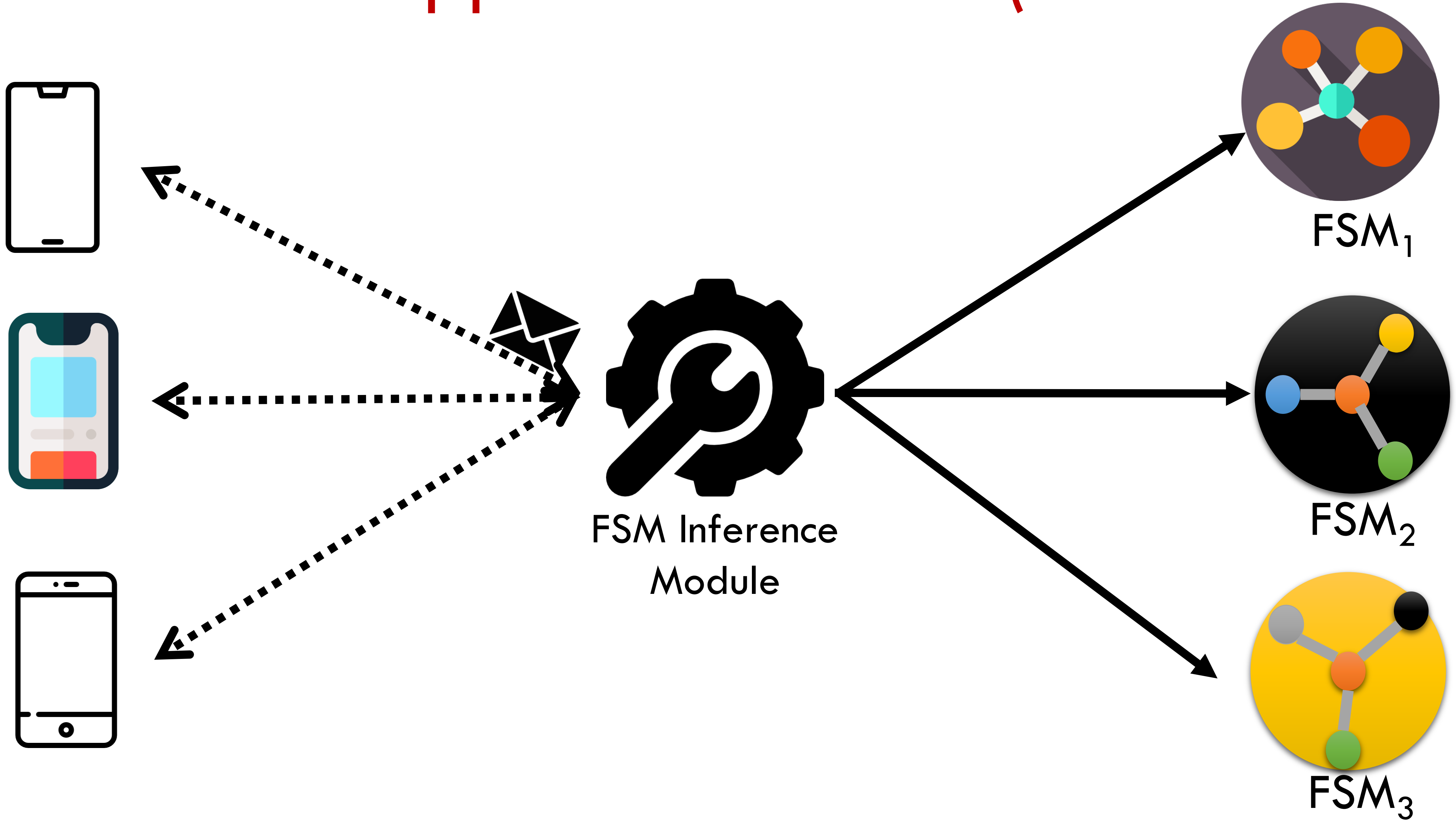
Extract behavioral abstraction

Equivalence checking

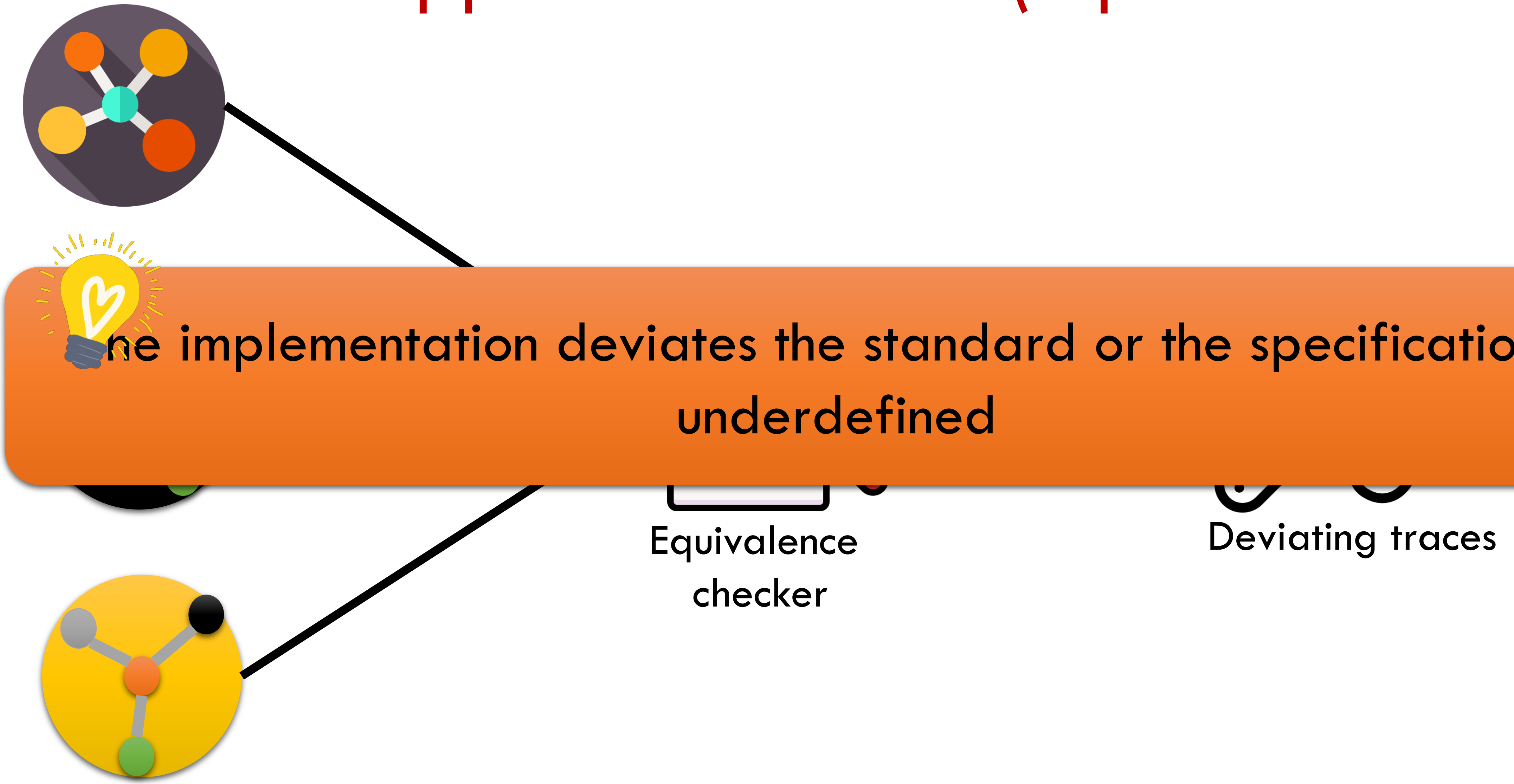
Identify Diverse non-compliant behavior

Noncompliance Instances

DIKEUE Approach Skeleton (FSM Inference)



DIKEUE Approach Skeleton (Equivalence Checker)



he implementation deviates the standard or the specification is underdefined

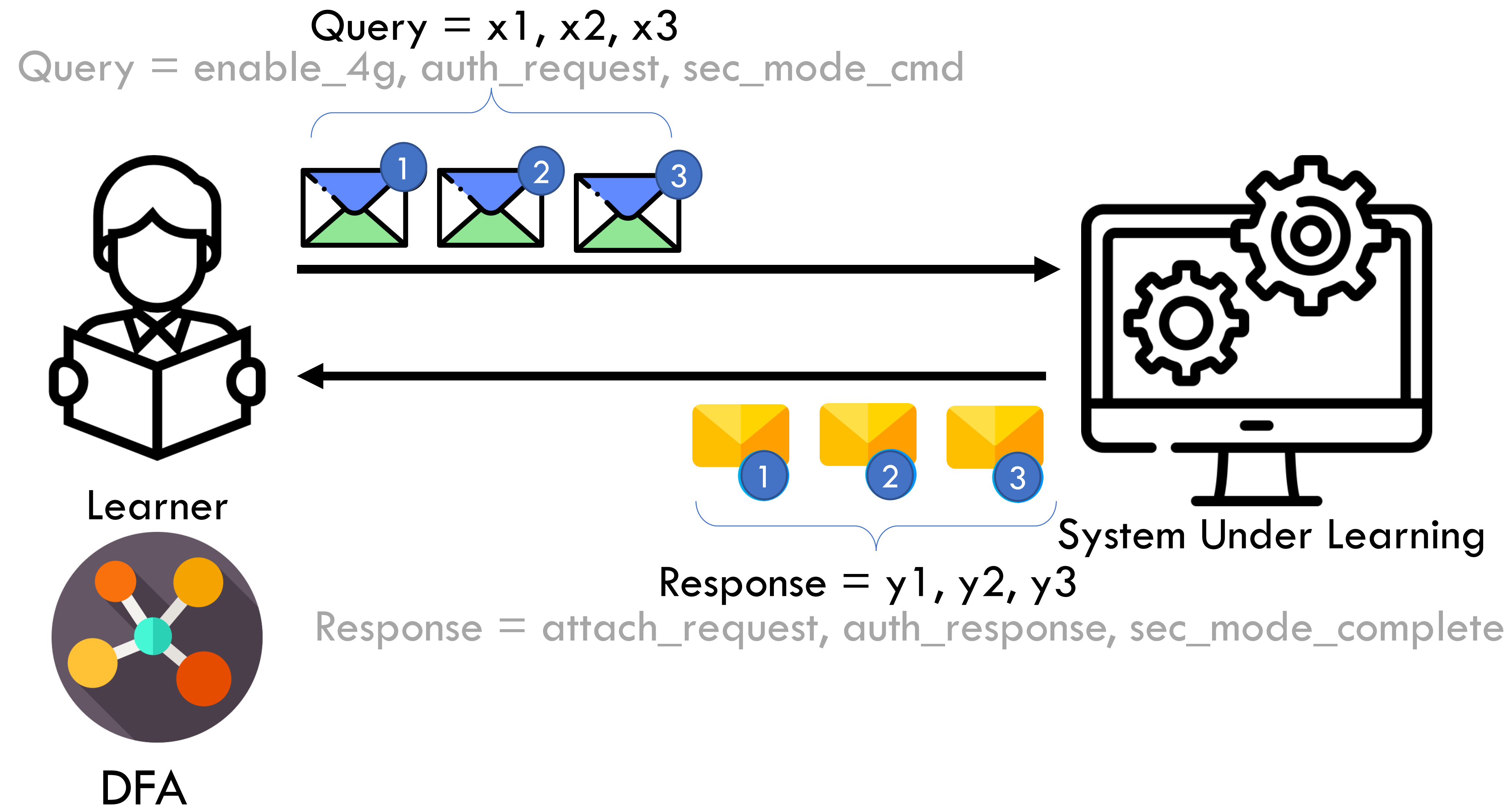
FSM Inference Module

FSM Equivalence Checker

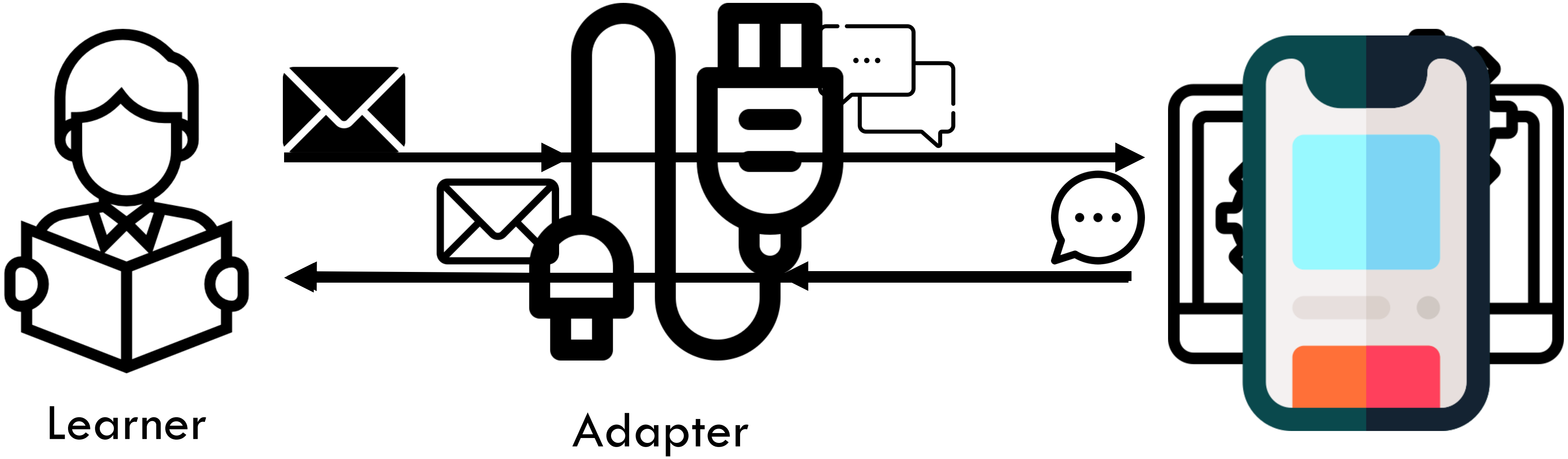
Findings

Extending DIKEUE to 5G

Active Automata Learning


Query = x1, x2, x3
Query = enable_4g, auth_request, sec_mode_cmd
1
2
3
Learner
System Under Learning
1
2
3
Response = y1, y2, y3
Response = attach_request, auth_response, sec_mode_complete
DFA

Active Automata Learning in 4G LTE and Instantiation of DIKEUE for 4G LTE



Challenges for 4G LTE Automata Learning

Pre-requisite of Automata Learning

- Input Output Alphabet Set Selection
- Nondeterminism
- Transparent Reset

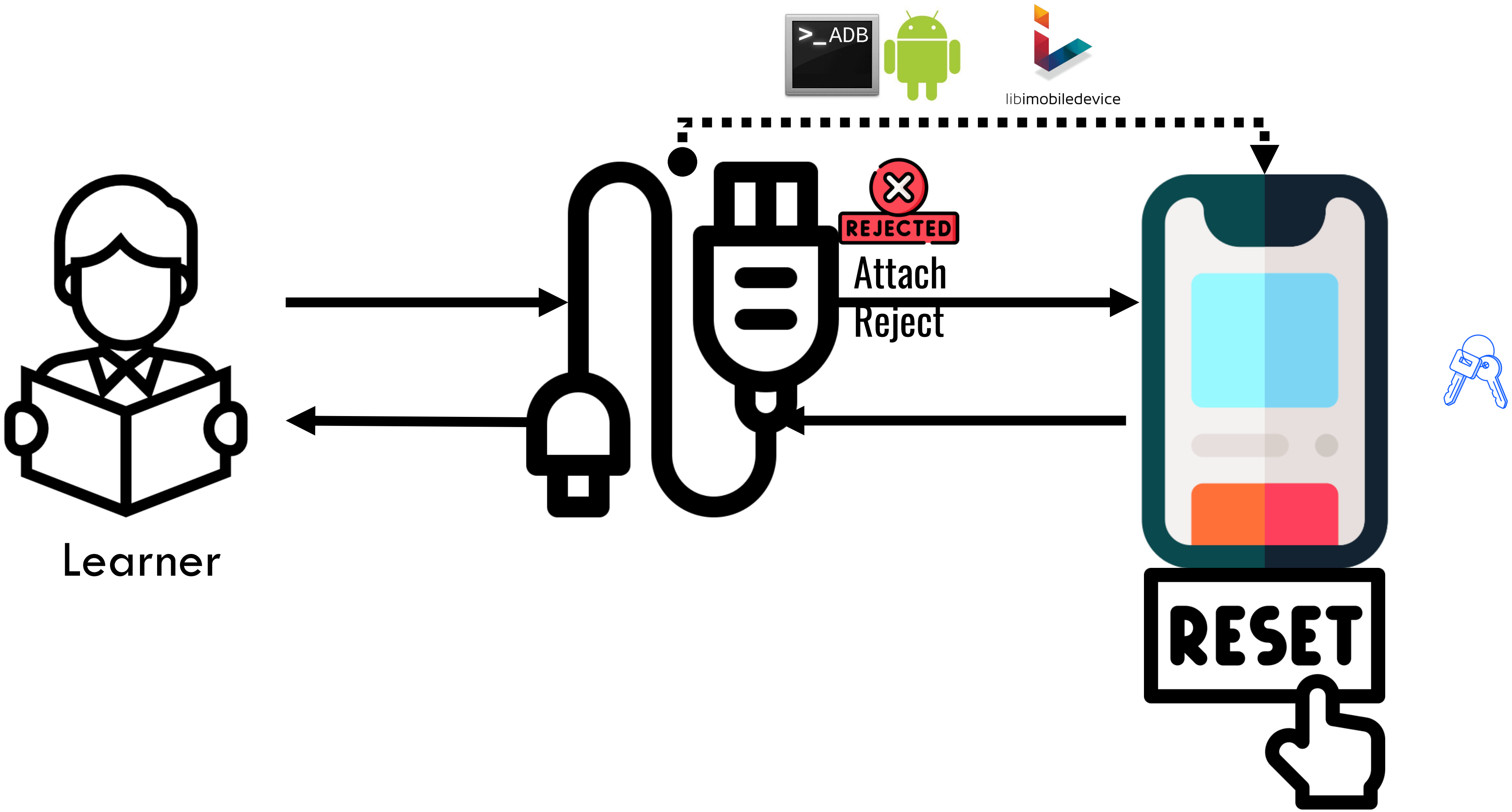
Balancing Termination and Coverage

- Optimized Alphabet Set
- Context Checker
- Caching Queries

LTE Specific Adapter

- Concrete Packet generation
- Triggering Complex Behaviors

Transparent Reset for LTE Devices



Challenges for 4G LTE Automata Learning

Pre-requisite of Automata Learning

- Input Output Alphabet Set Selection
- Nondeterminism
- Transparent Reset

Balancing Termination and Coverage

- Optimized Alphabet Set
- Context Checker
- Caching Queries

LTE Specific Adapter

- Concrete Packet generation
- Triggering Complex Behaviors

Design of Context Checker

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

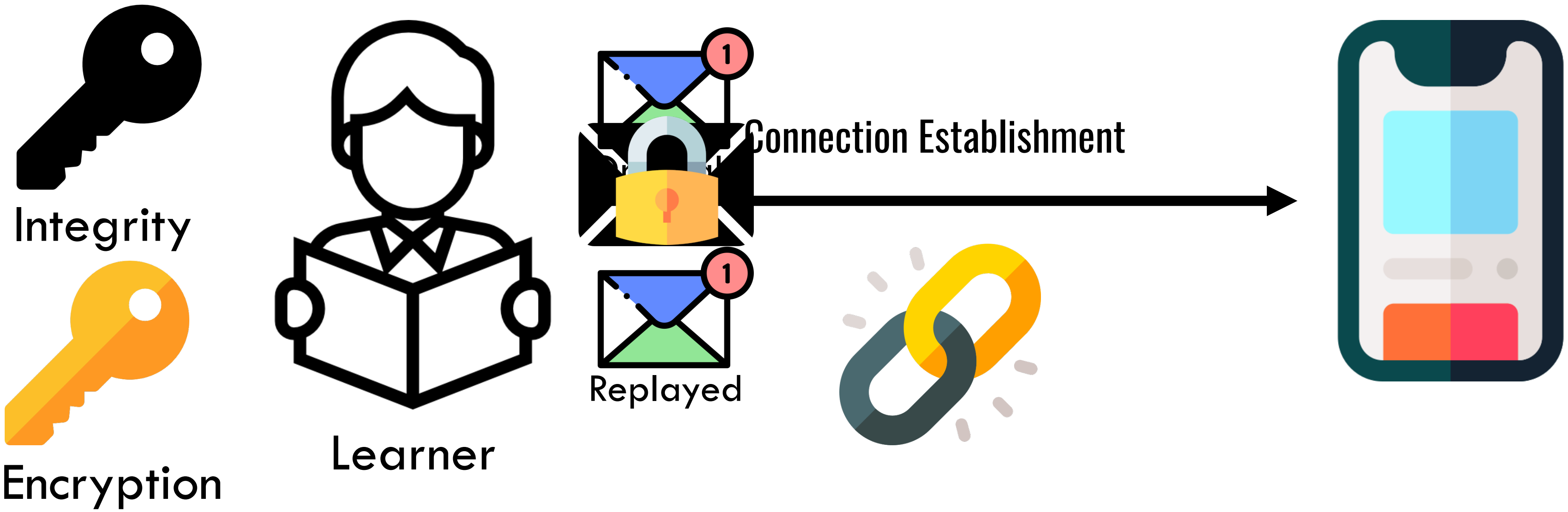
University Nijmegen

ence/usenixsecurity15/technical-sessions/presentation/de-ruiter

Generalization: Check context before sending message

Learner

Context Checker: Additional Invariants



FSM Inference Module

FSM Equivalence Checker

Findings

Extending DIKEUE for 5G

FSM Equivalence Checking: Converting to Model Checking

Output
Output$_2$

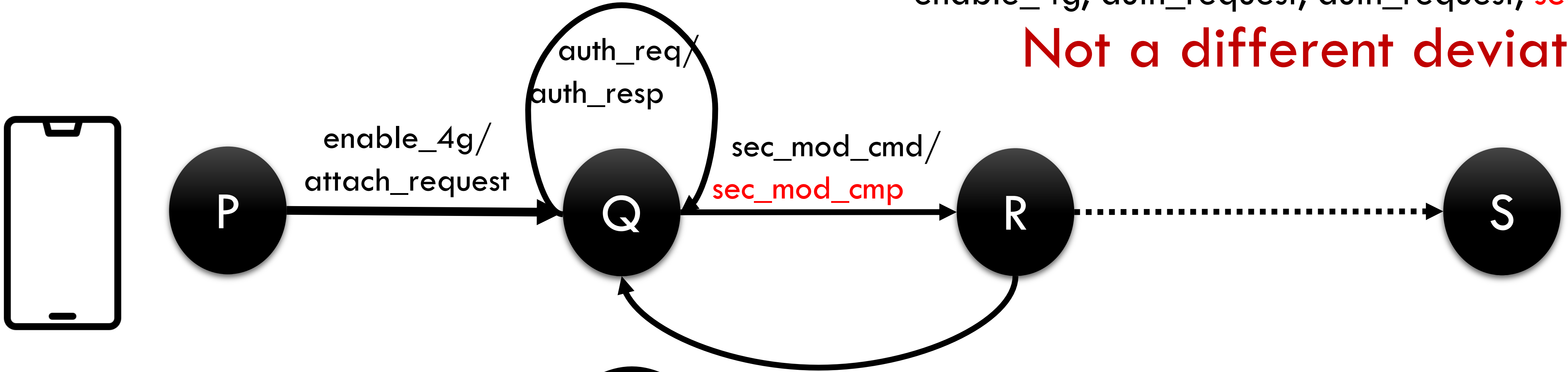
Our goal: discovering many diverse deviation inducing traces!

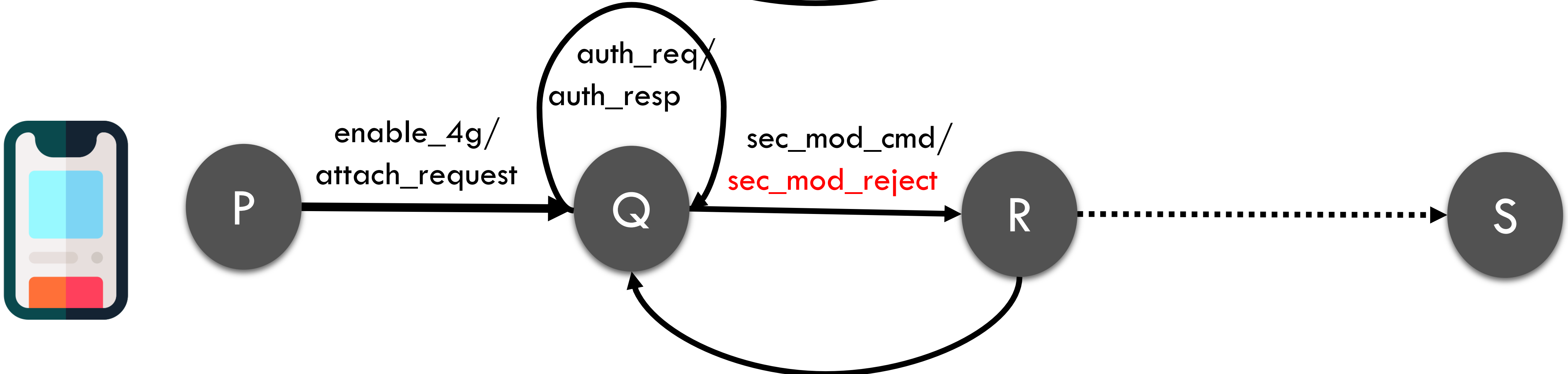
Challenge of Discovering Diverse Deviations

Input: ~~enable_4g, auth_request, sec_mod_cmd~~

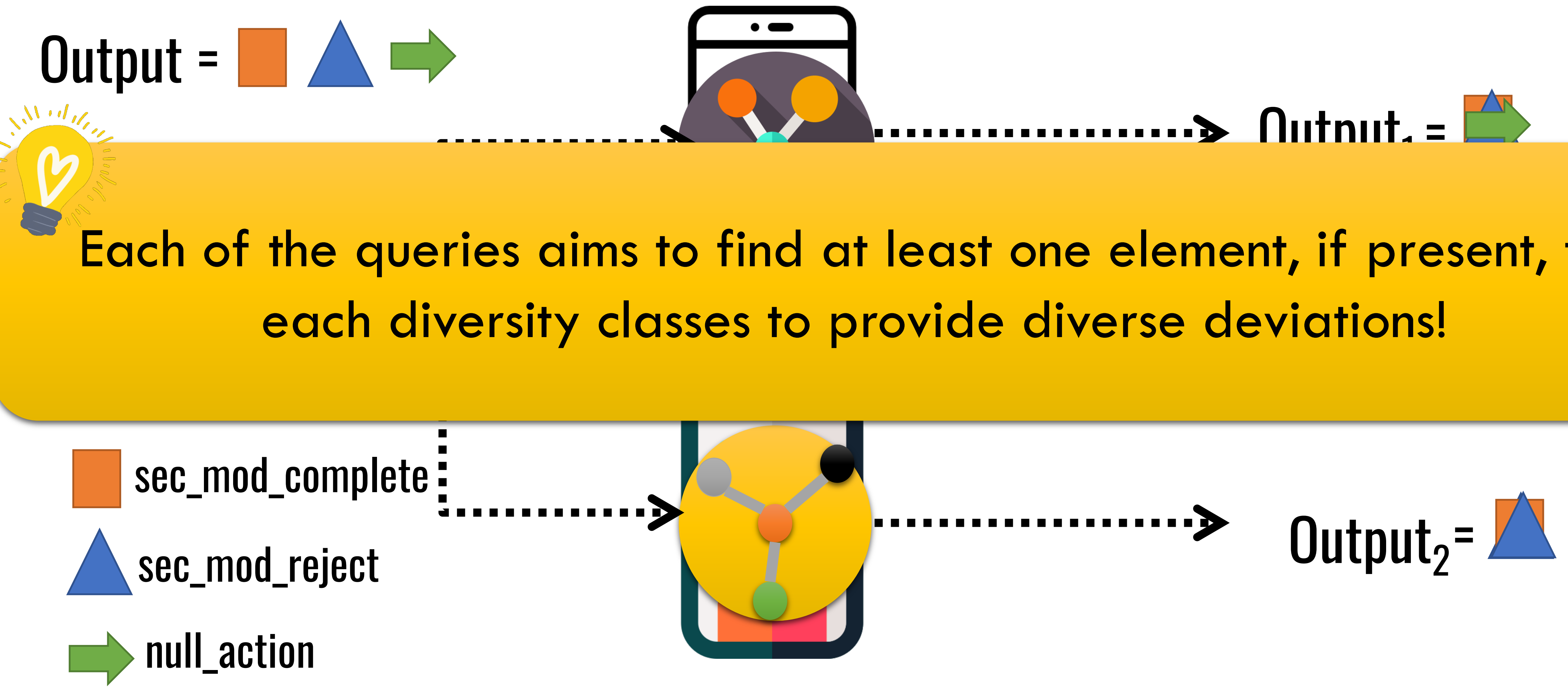
enable_4g, auth_request, auth_request, sec_mod_cmd

Not a different deviation!





Diversity Class of Deviation-Inducing Inputs



Each of the queries aims to find at least one element, if present, for each diversity classes to provide diverse deviations!

FSM Inference Module

FSM Equivalence Checker

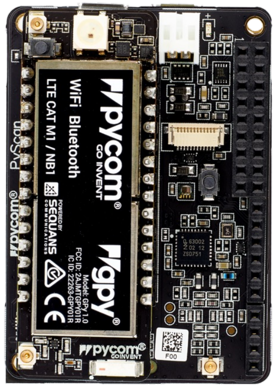
Findings

Extending DIKEUE for 5G

List of Devices Tested

14 Devices from 5 Vendors

android



MEDIATEK

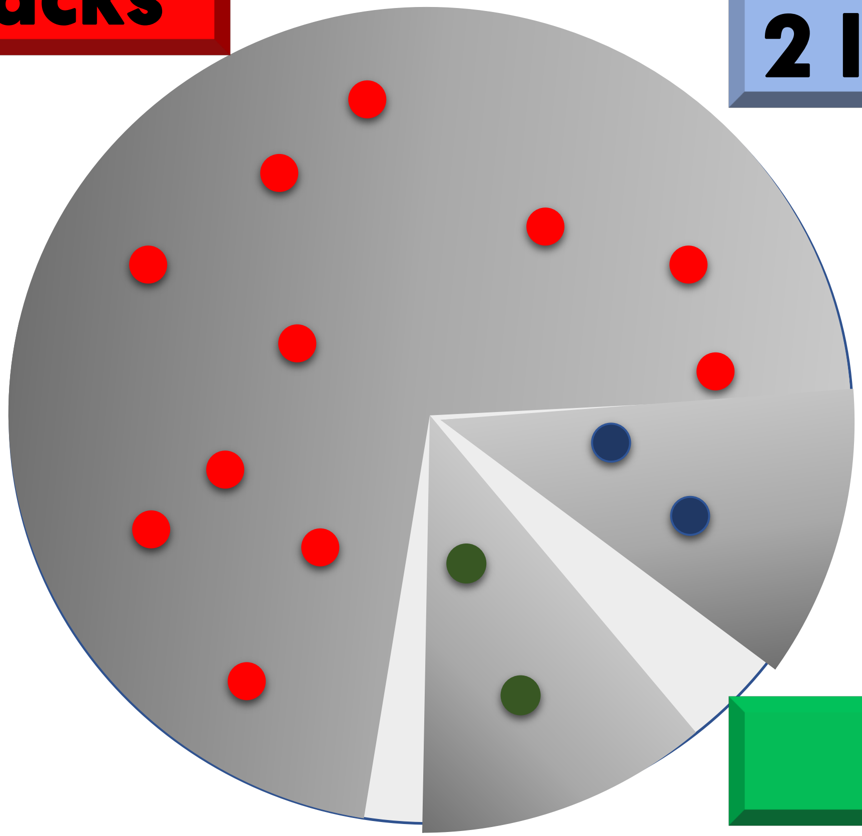
HUAWEI

intel

Qualcomm

HISILICON

Summary of Findings



11 Exploitable Attacks

2 Interoperability Issues

2 Other deviations

15 new deviating behavior

Summary of Findings

2 Previous Implementation Issues

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

David Rupprecht
Horst Görtz Institute for IT-Security
Ruhr-University Bochum, Germany
david.rupprecht@rub.de

Kai Jan
Horst Görtz Institu
Ruhr-University B
kai.jansen-

Christina Pöpper
New York University Abu Dhabi
christina.poepper@nyu.edu

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

Location tracking

Denial of service

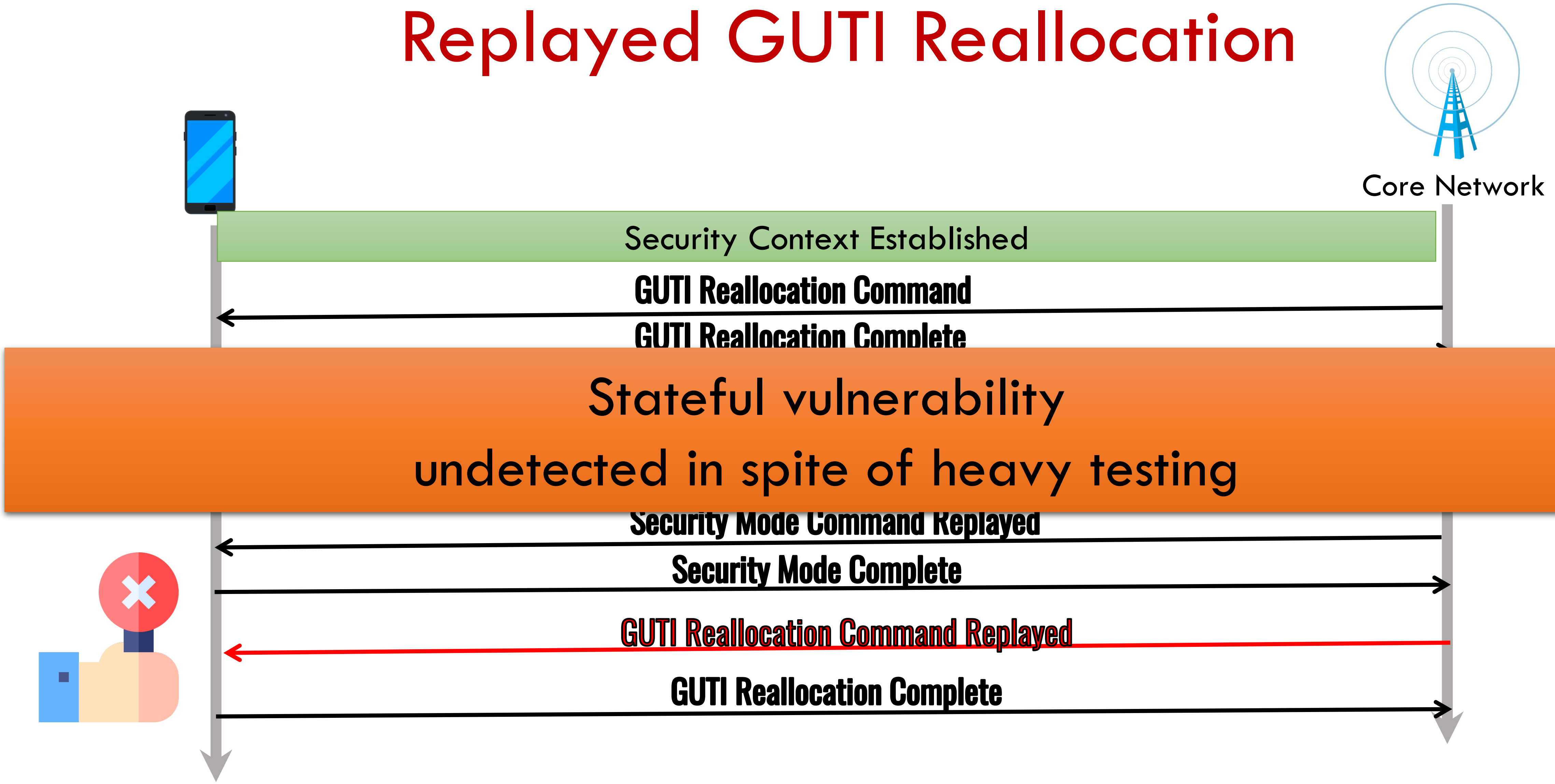
Security bypass

Key reinstallation attack

Deviations to Attack Strategy Generation

- Identify deviant behavior and traces automatically using DIKEUE
- Root cause analysis from the specification
- Exploitable attack generation
- Validation in testbed

Replayed GUTI Reallocation



Core Network

Security Context Established

GUTI Reallocation Command

GUTI Reallocation Complete

Security Mode Command Replayed

Security Mode Complete

GUTI Reallocation Command Replayed

GUTI Reallocation Complete

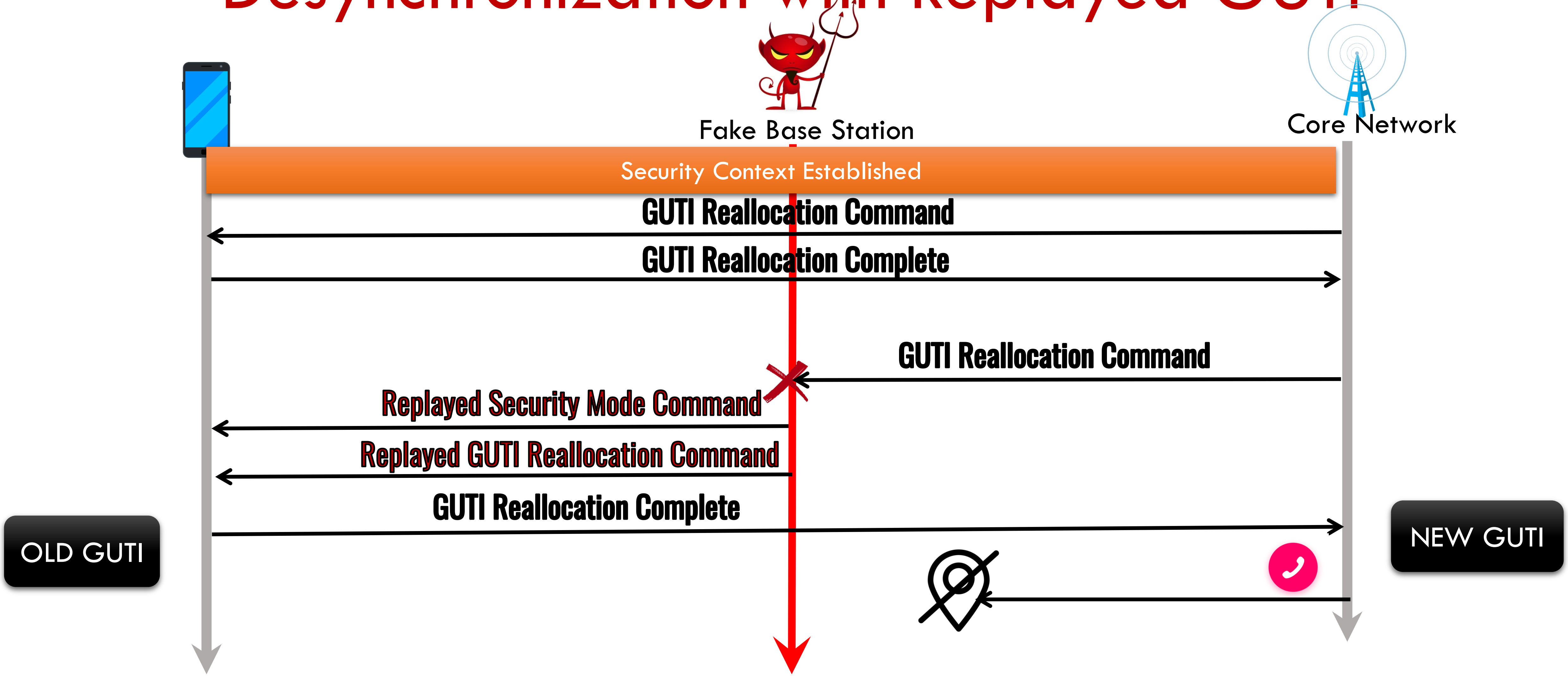
Stateful vulnerability
undetected in spite of heavy testing

Root cause analysis

"Replay protection must assure that one and the same NAS message is not accepted twice by the receiver. Specifically for a given security context."

—3GPP 24.301 NAS

Desynchronization with Replayed GUTI


Fake Base Station
Core Network
Security Context Established
GUTI Reallocation Command
GUTI Reallocation Complete
GUTI Reallocation Command
Replayed Security Mode Command
Replayed GUTI Reallocation Command
GUTI Reallocation Complete
OLD GUTI
NEW GUTI

Responsible Disclosure Update

✓ 9 High and Medium Severity Issue Confirmed

GSMA-CVD-2021-0050

CVE-2021-25471 (Samsung), CVE-2021-25480 (Samsung), CVE-2021-40148 (MediaTek)

Google Bug Bounty

Qualcomm, Samsung, and MediaTek are patching...

FSM Inference Module

FSM Equivalence Checker

Findings

Extending DIKEUE for 5G

Challenges and Possible Opportunities to Extend DIKEUE for 5G Basebands

NEW New Message Types, e.g., RRC Resume Request and Predicates

New logic for 5G Context Checker

Scalability
Combining Passive and Active Automata Learning

Key Takeaways

Blackbox security analysis techniques backed by sophisticated formal methods (automata learning and model checking) can be effective for basebands

Easy to deploy the technique to any cellular basebands from any vendors with almost no manual effort

The technique can also be applied to other wireless protocols

Summary

Designed an automatic, black-box, and stateful noncompliance checker for basebands

Implemented approach in a new tool, **DIKEUE**

DIKEUE identified 11 new attack on different device implementations