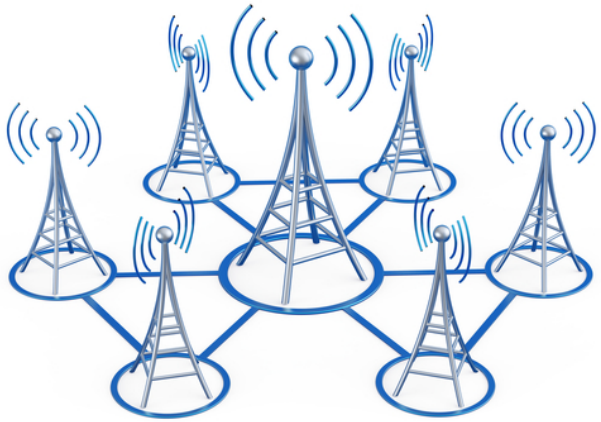
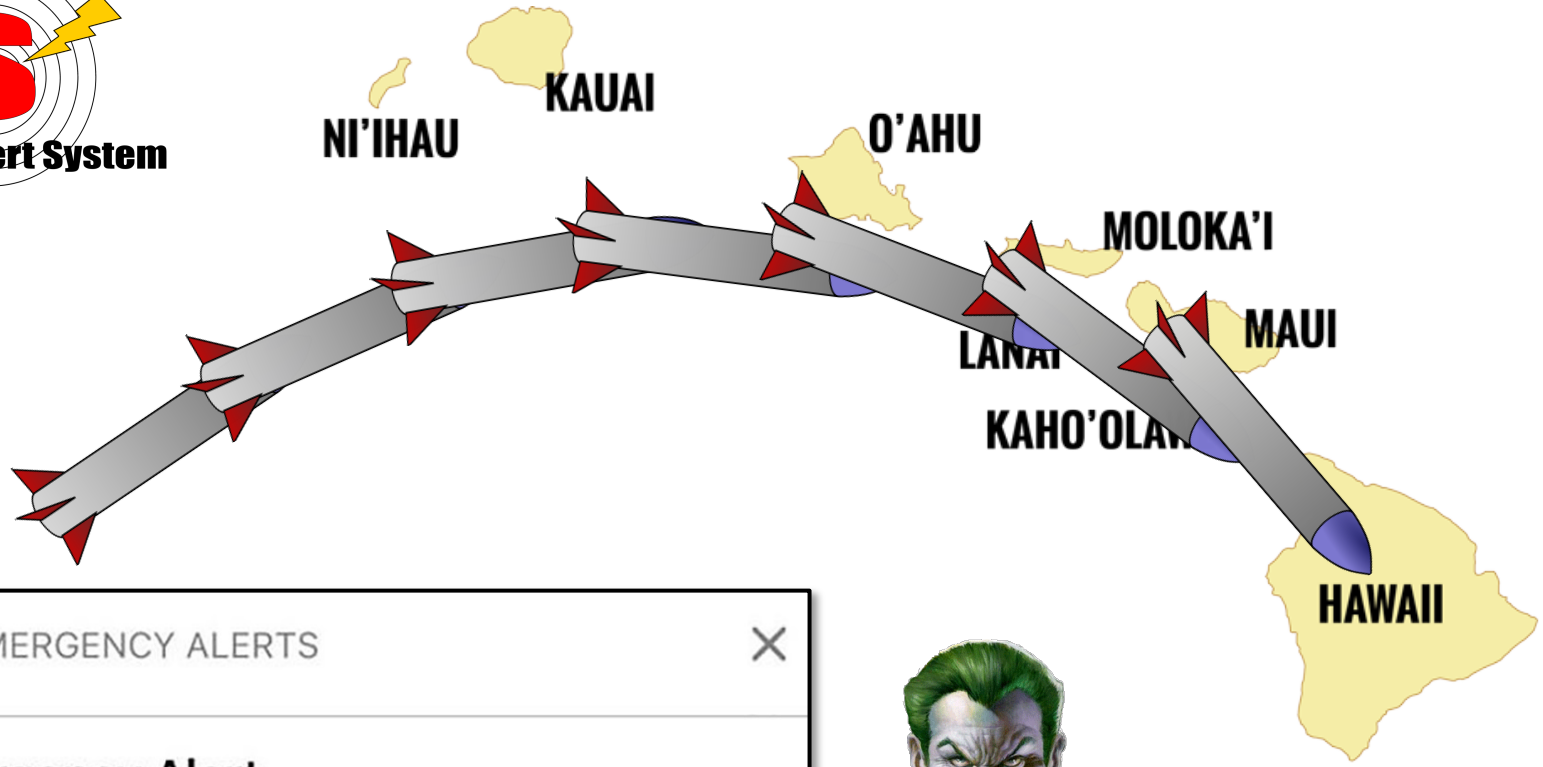
LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE

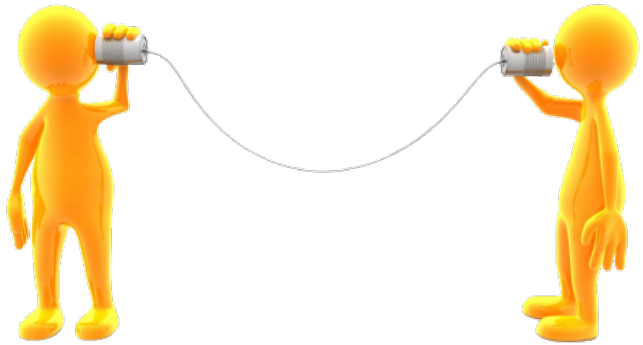
Syed Rafiul Hussain*, Omar Chowdhury†, Shagufta Mehnaz*, Elisa Bertino*
Purdue University*, University of Iowa†

Critical Infrastructure using Cellular Network



EAS
Emergency Alert System

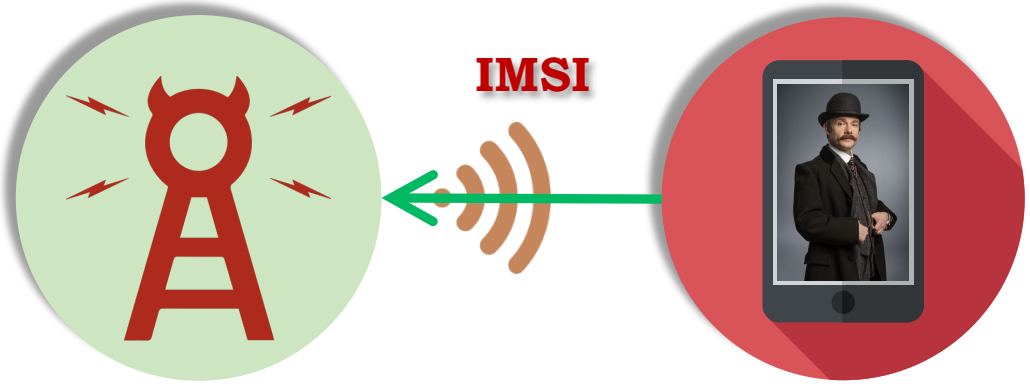




EMERGENCY ALERTS

Emergency Alert
BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.

Security and Privacy Threats on Cellular Network



IMSI = International Mobile Subscriber Identity

Location Leaks on the GSM Air Interface

Denis Foo Kune, John Koelndorfer, Nicholas Hopper, Yongdae Kim
University of Minnesota
foo@cs.umn.edu, koeln005@umn.edu, hopper@cs.umn.edu, kyd@cs.umn.edu

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

Altaf Shaik*, Ravishankar Borgaonkar†, N. Asokan‡, Valtteri Niemi§ and Jean-Pierre Seifert*

Limitations of Existing Attack Finding Strategies for Cellular Networks

No Systematic Approach

No adversary, just analyze the performance, and reliability

2G
3G

Location Leaks on the GSM Air

Denis Foo Kune, John Koelndorfer, Nicholas Ho

Control-Plane Protocol Interactions in C

Guan-Hua Tu†•, Yuanjie Li†; Chunyi Peng‡, Chi-Yu Li†, Hon
†University of California, Los Angeles ‡The Ohio State U
†{ghtu, yuanjie.li, lichiyu, hywang, slu}@cs.ucla.edu ‡chunyi@cse.ohio-state.edu

New Privacy Issues in Mobile Telephony: Fix and Verification

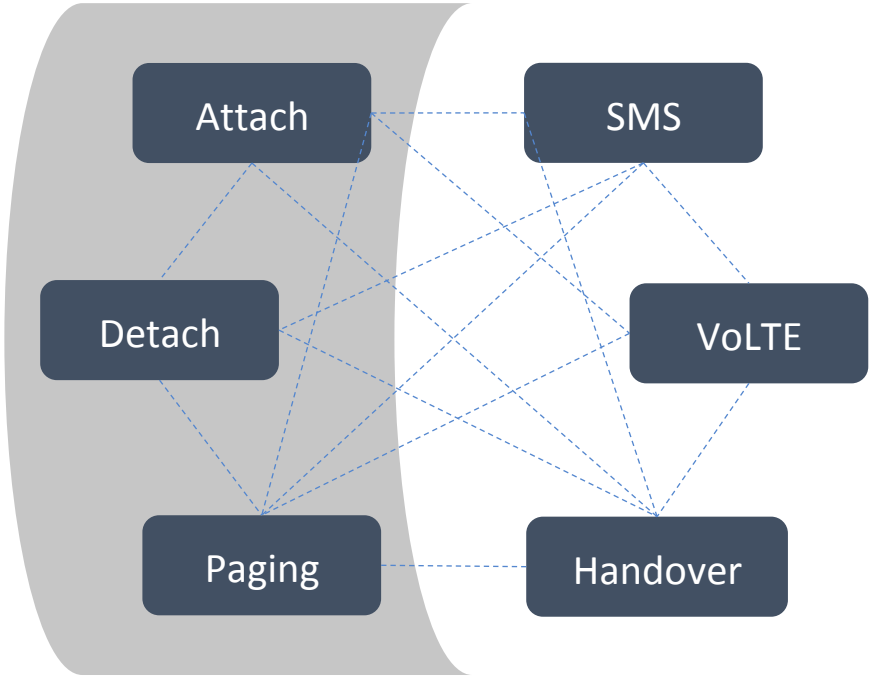
Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan
Nico Golde, Kevin Redon, Ravishankar Borgaonkar

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

Altaf Shaik*, Ravishankar Borgaonkar†, N. Asokan‡, Valtteri Niemi§ and Jean-Pierre Seifert*

❑ Is it possible to build a ***Systematic framework*** for ***adversarially analyzing the cellular network specification*** in order to ***find security and privacy related problems?***

Scope



Man-in-the-Middle Attacker

Spurious billing

Life threatening risks

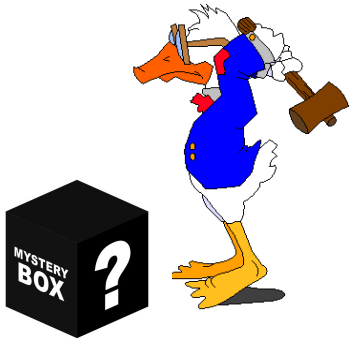

Challenges
1
Preliminaries
2
LTEInspector
3
Findings &
Attack Validation
4
Responsible Disclosure
and Impact
5
Future Work
6
Conclusion
7

Challenges

- ❑ Stateful procedures and multiple participants

- ❑ 4G LTE lacks formal specification
  - ✓written in natural language

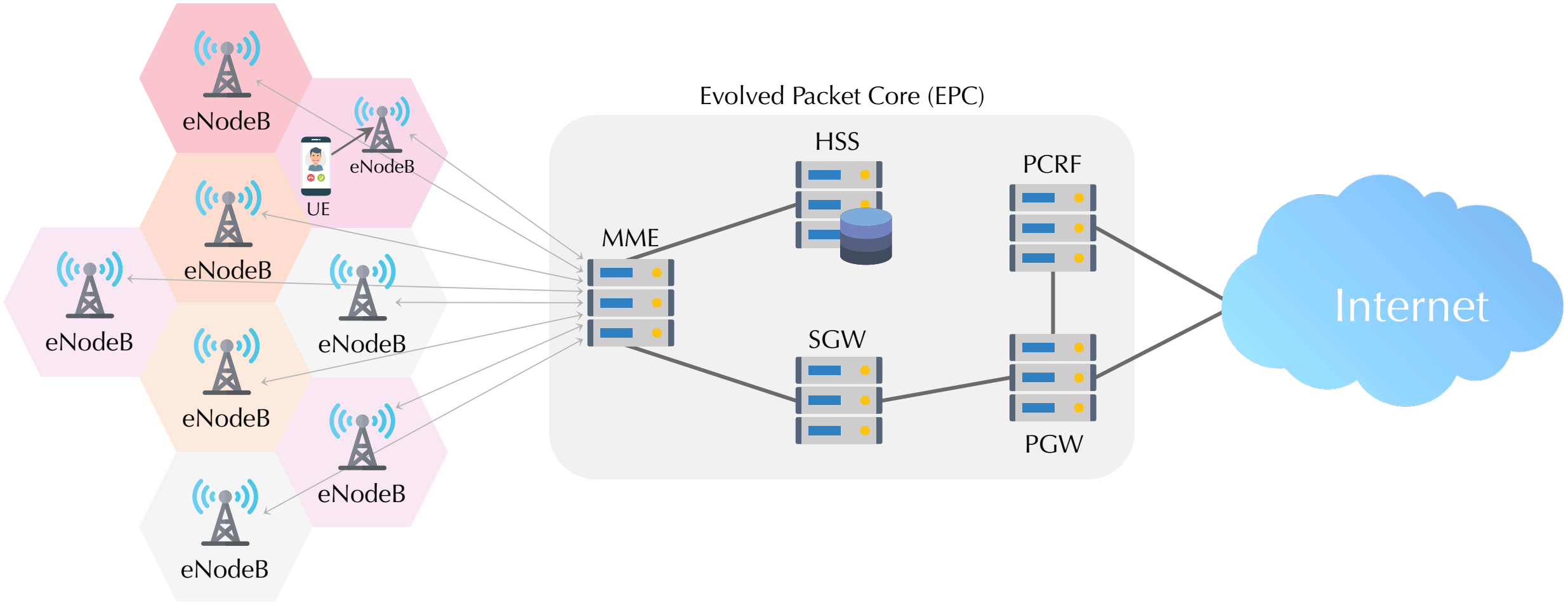
- ❑ Closed system
  - ✓Proprietary



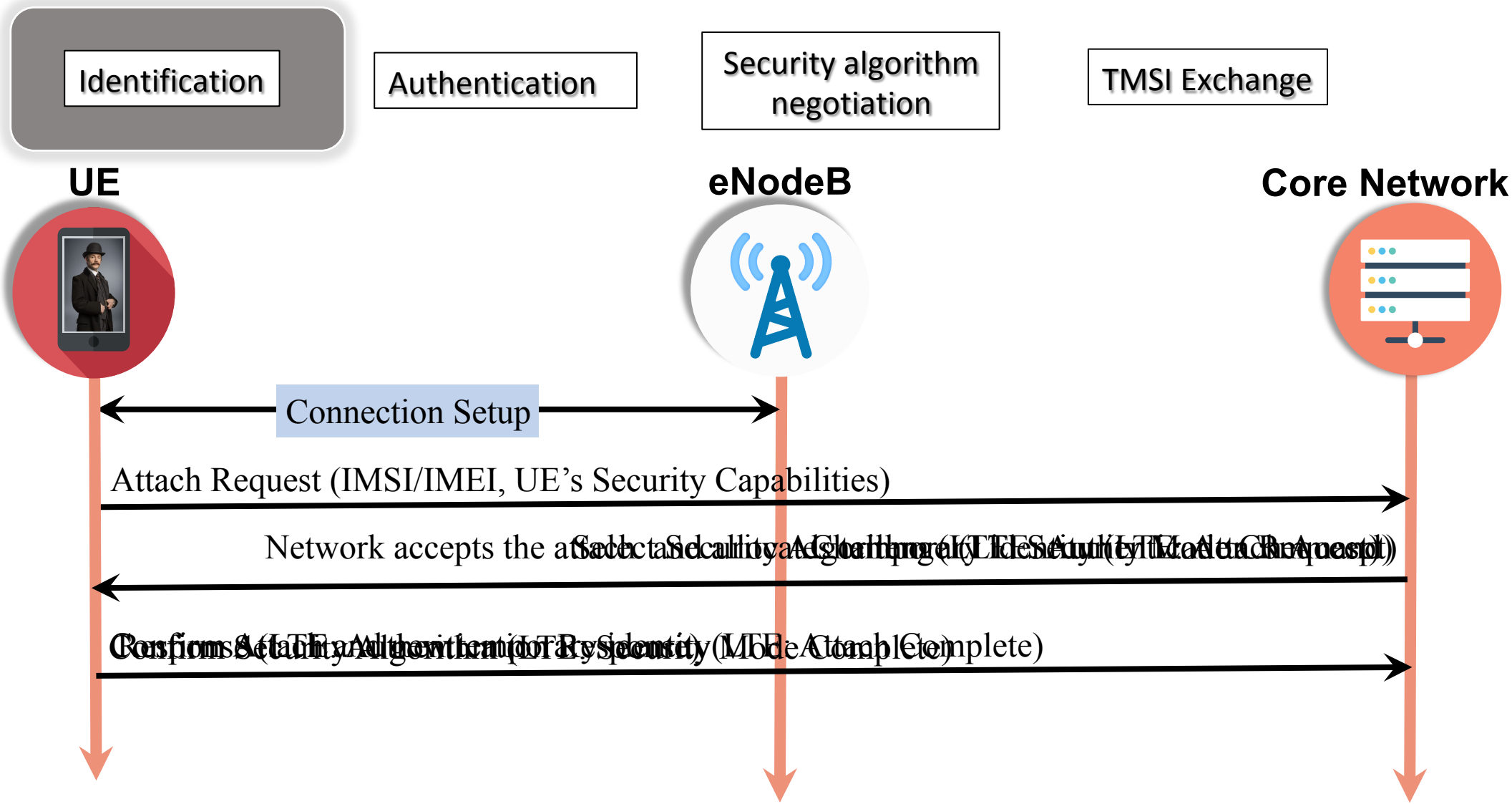
- ❑ Legal barrier
  - ✓Licensed spectrum


Challenges
1
2
Preliminaries
LTEInspector
3
4
Findings &
Attack Validation
Responsible Disclosure
and Impact
5
6
Future Work
Conclusion
7

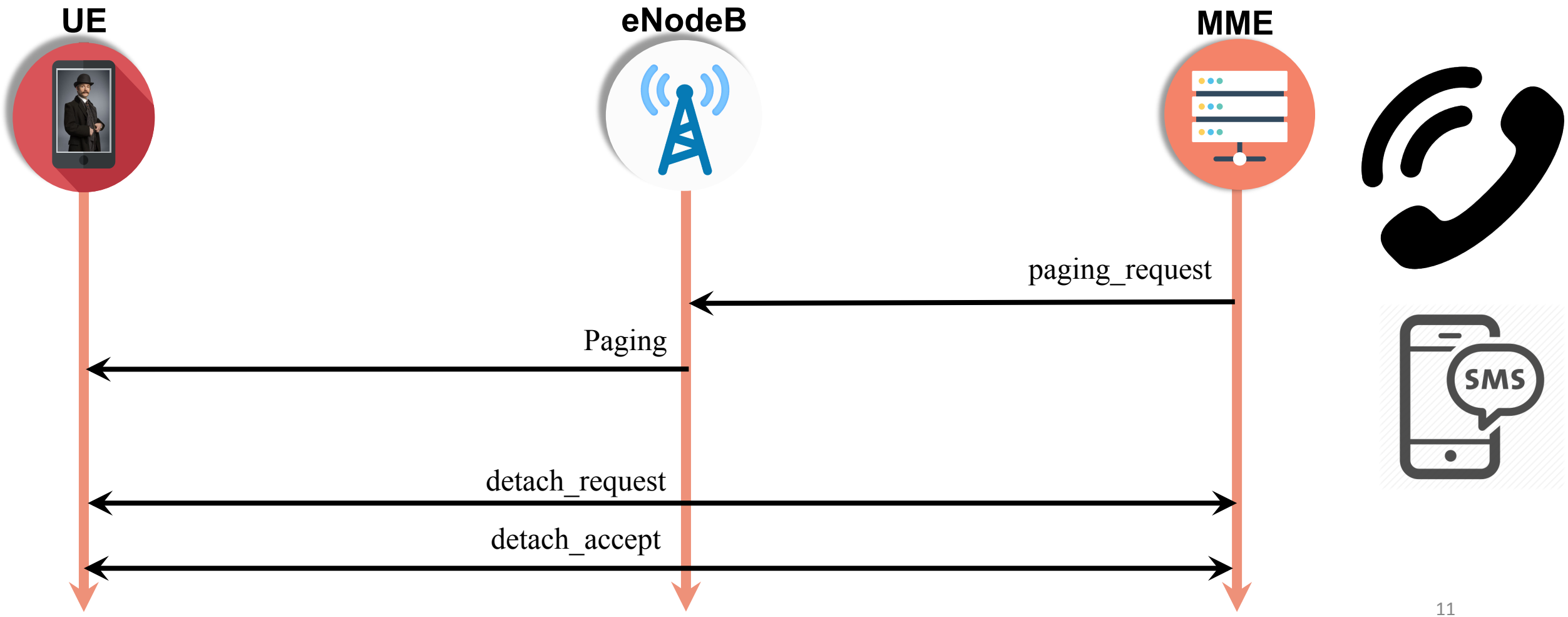
Background: LTE Architecture



Background (Attach)



Background (Paging & Detach)




Challenges
1
Preliminaries
2
LTEInspector
3
Findings &
Attack Validation
4
Responsible Disclosure
and Impact
5
Future Work
6
Conclusion
7

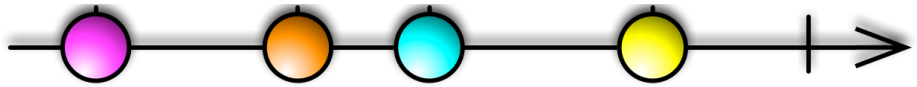
Adversary Model

- Dolev-Yao model
  - Eavesdrop
  - Drop or modify
  - Inject
  - Adheres to cryptographic assumptions

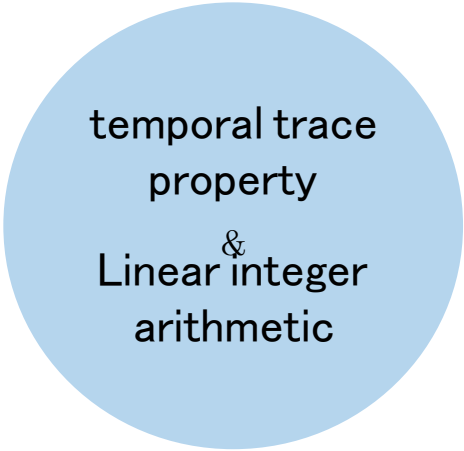
- Why Dolev-Yao model?
  - Powerful adversary
  - Automatic tools (ProVerif, Tamarin) can leverage

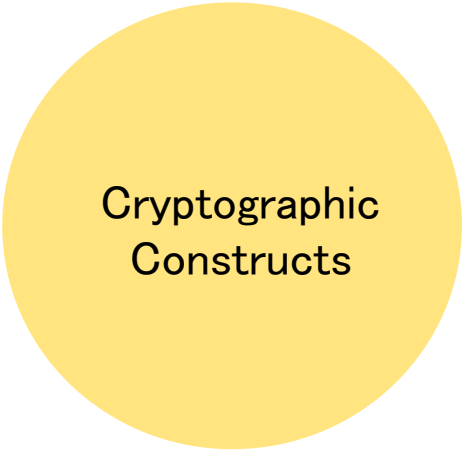
Insight

- Property characteristics
  - Temporal ordering of events
  - Cryptographic constructs
  - Linear integer arithmetic and other predicates



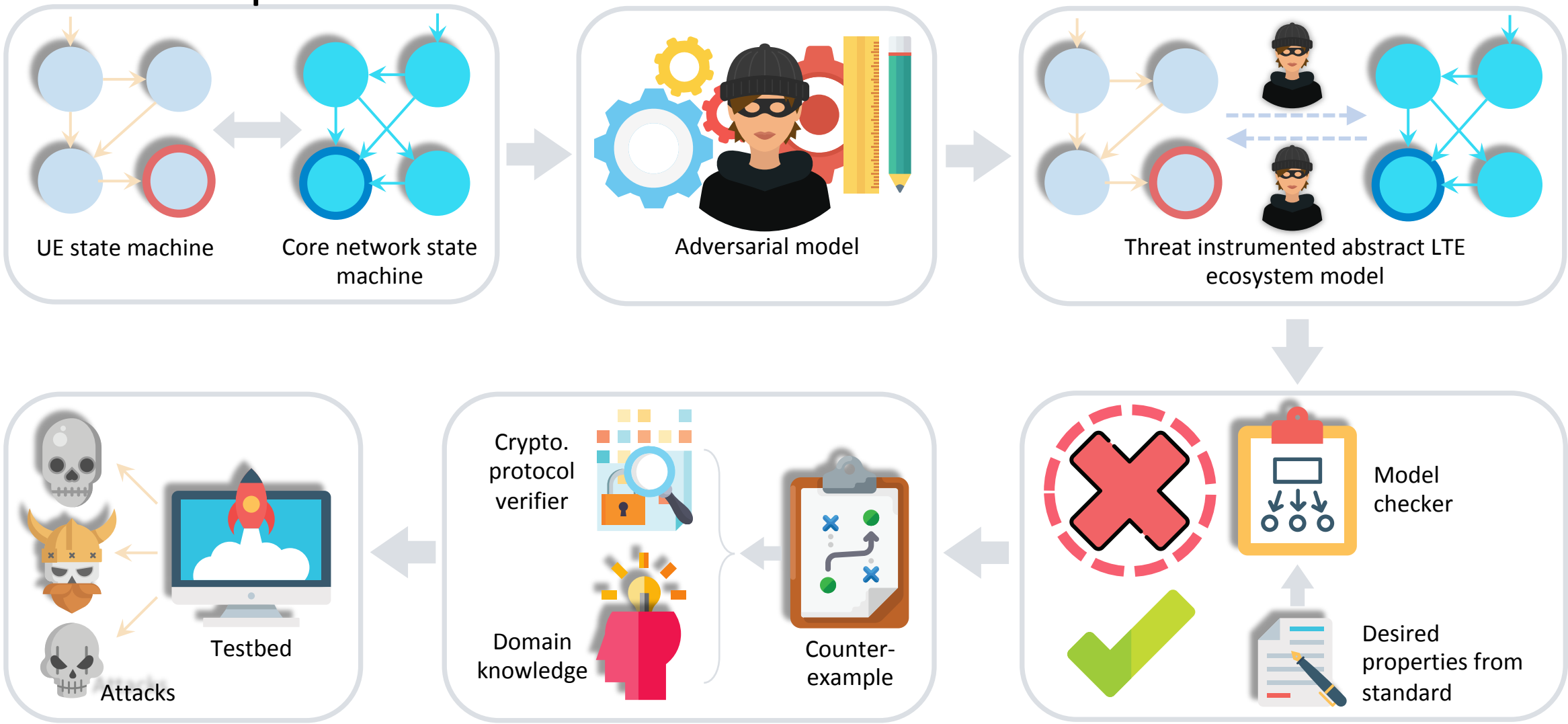
- Intuition:
  - ✓ Model checker
  - ✓ Cryptographic protocol verifier





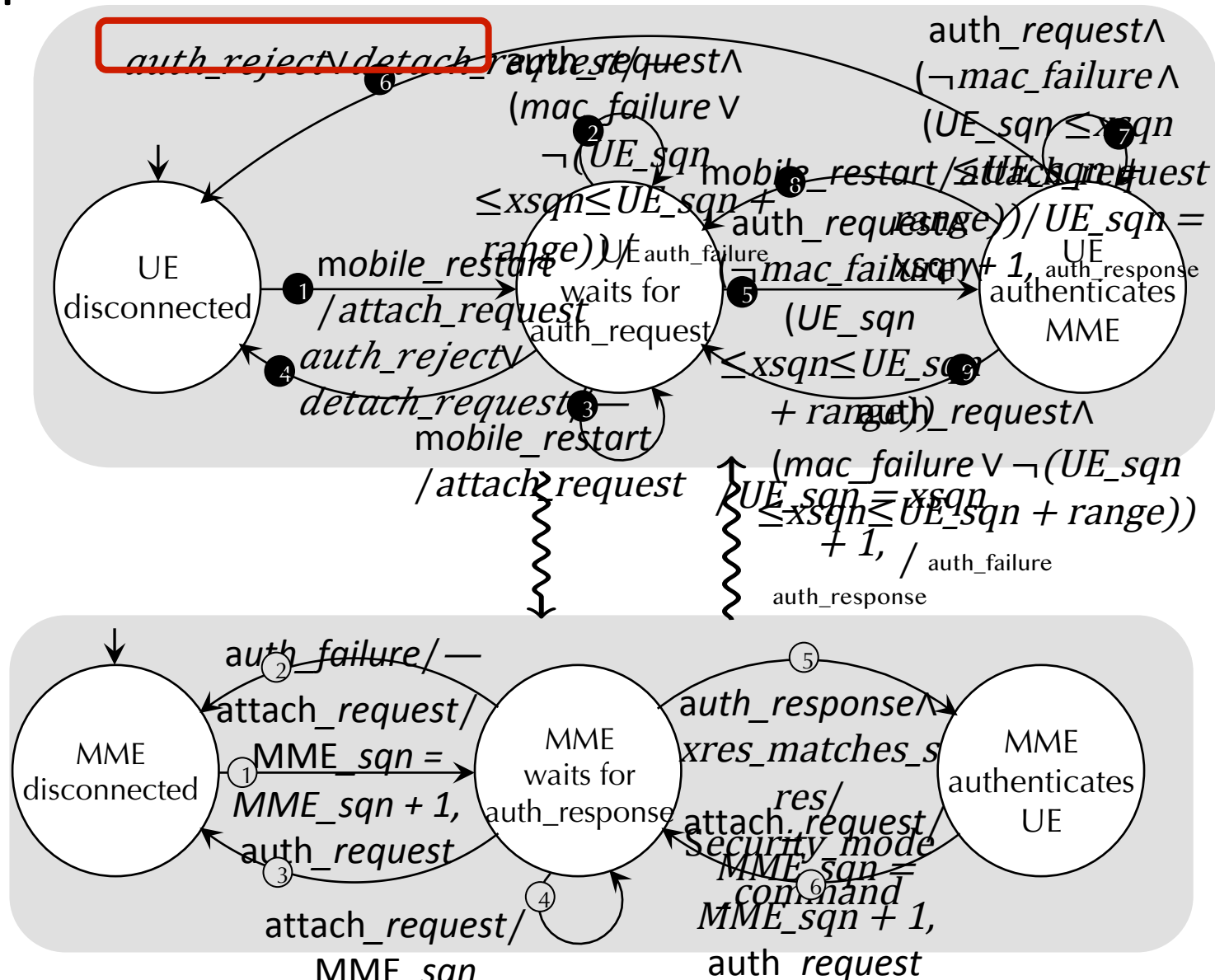
How can we leverage reasoning power of these two?

LTEInspector

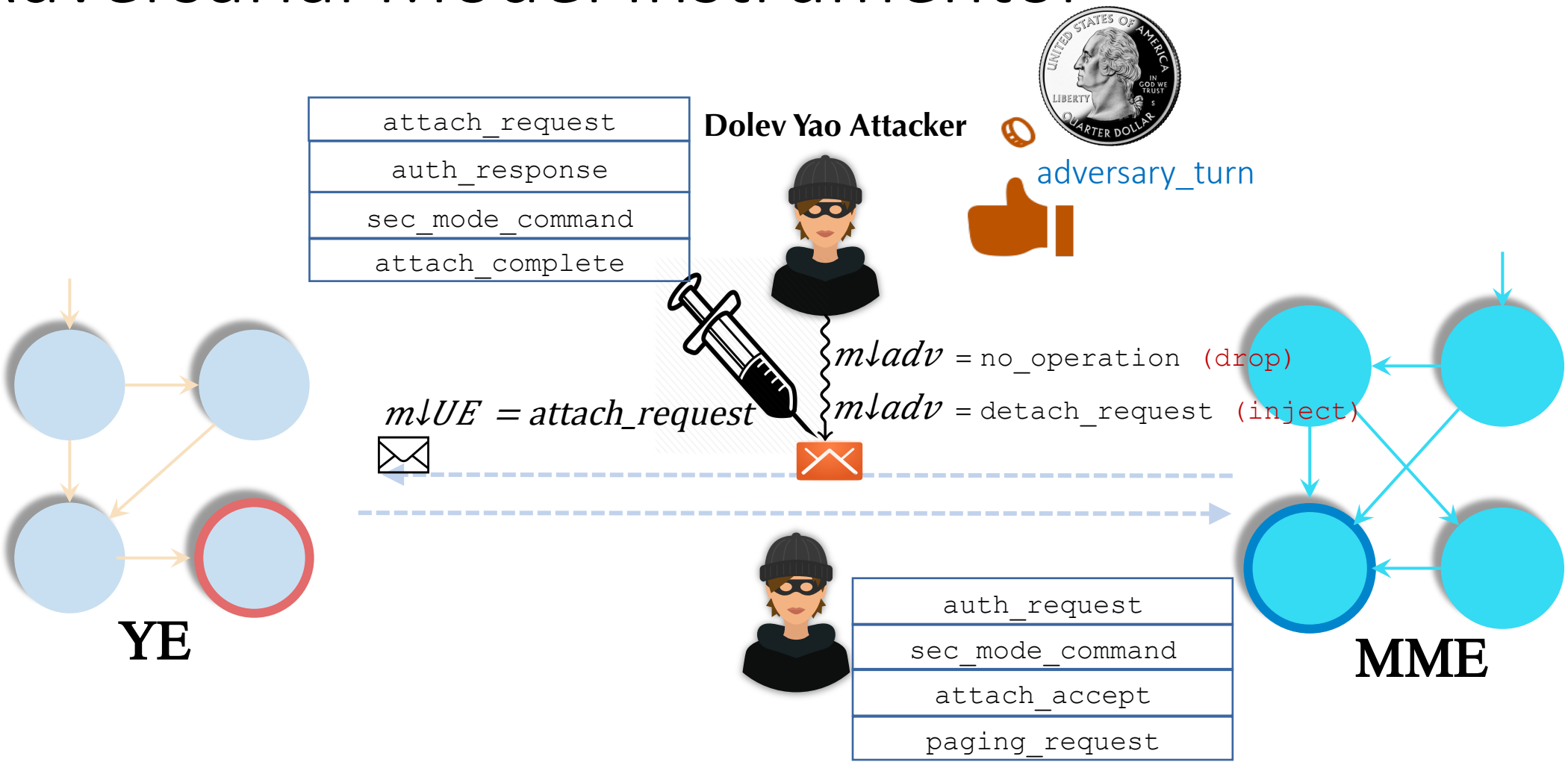


Abstract LTE Model

- Specification Model for NAS layer (UE-MME) interactions
  - Propositional logic level
  - Model message types only, not message data
  - Abstract away cryptographic constructs
  - Two unidirectional channels



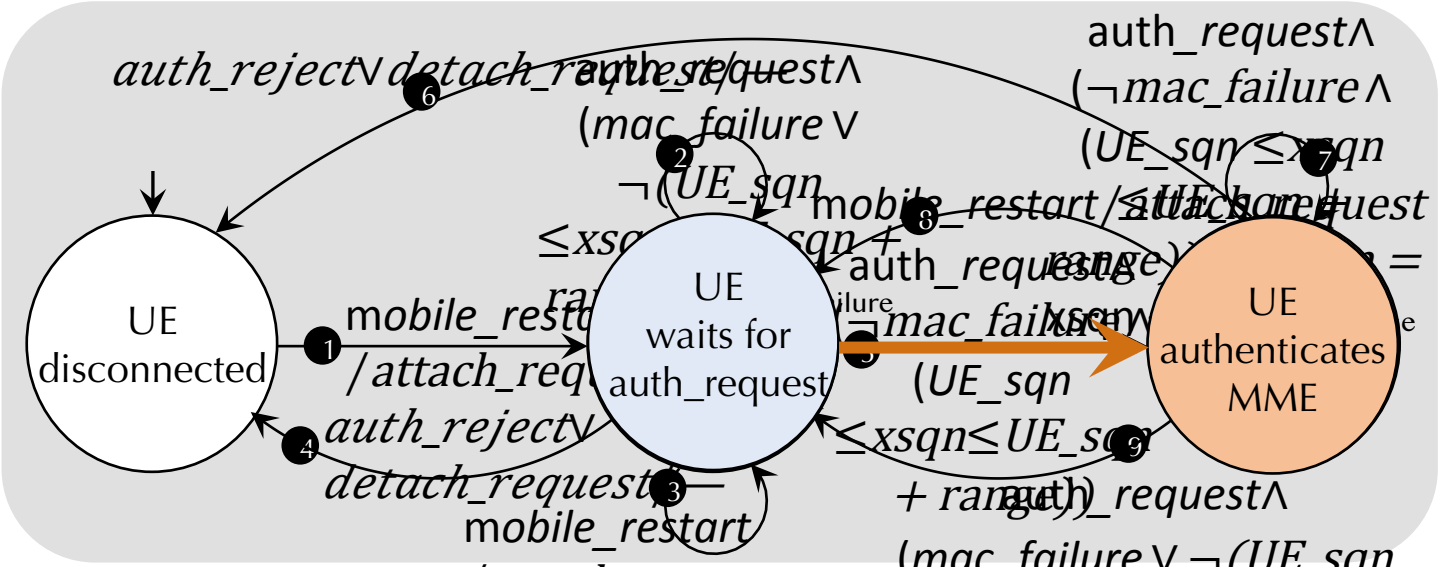
Adversarial Model Instrumentor

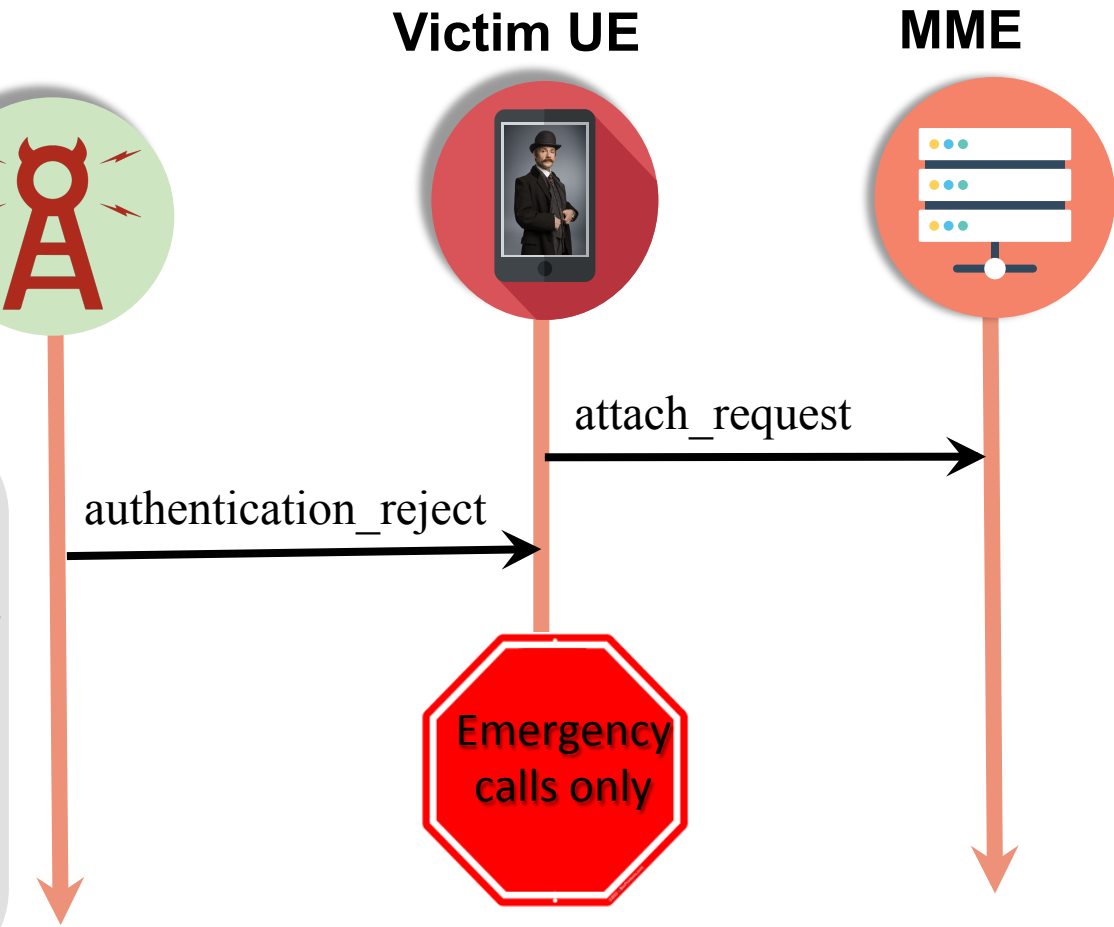


Model Checker

- Temporal trace properties
  - Liveness – *something good eventually happens*
  - Safety – *nothing bad happens*
- NuSMV

> $\varphi\downarrow 1$: It is always the case that whenever UE is in the *wait for auth request*, it will eventually *authenticate MME*.





Cryptographic Protocol Verifier

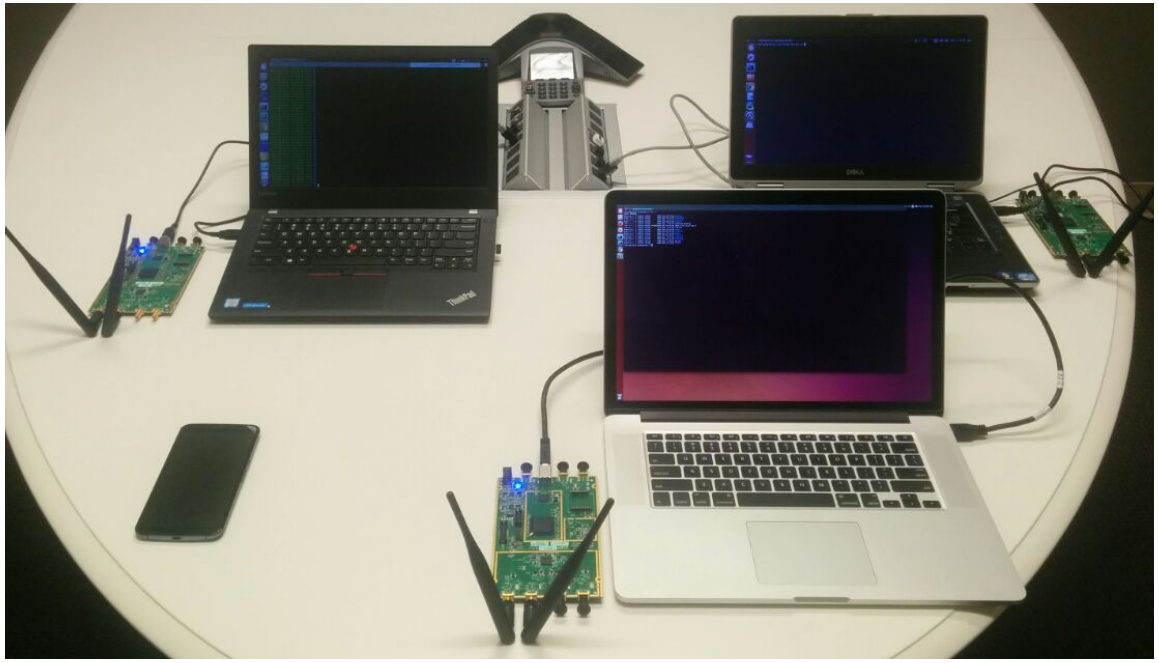
- Injective-correspondence (authentication)

  Every authentication_reject message received by UE must be sent by the core network

- ProVerif
  - Secrecy
  - Authenticity
  - Observational equivalence

Testbed Validation

- Malicious eNodeB setup (USRP, OpenLTE, srsLTE)
- Malicious UE setup (USRP, srsUE)
- COTS smartphones
- SIM cards of four major US carriers
- Custom-built core network
  - USRP, OpenLTE, srsLTE, and USIM




Challenges
1
Preliminaries
2
LTEInspector
3
Findings &
Attack Validation
4
Responsible Disclosure
and Impact
5
Future Work
6
Conclusion
7

Findings

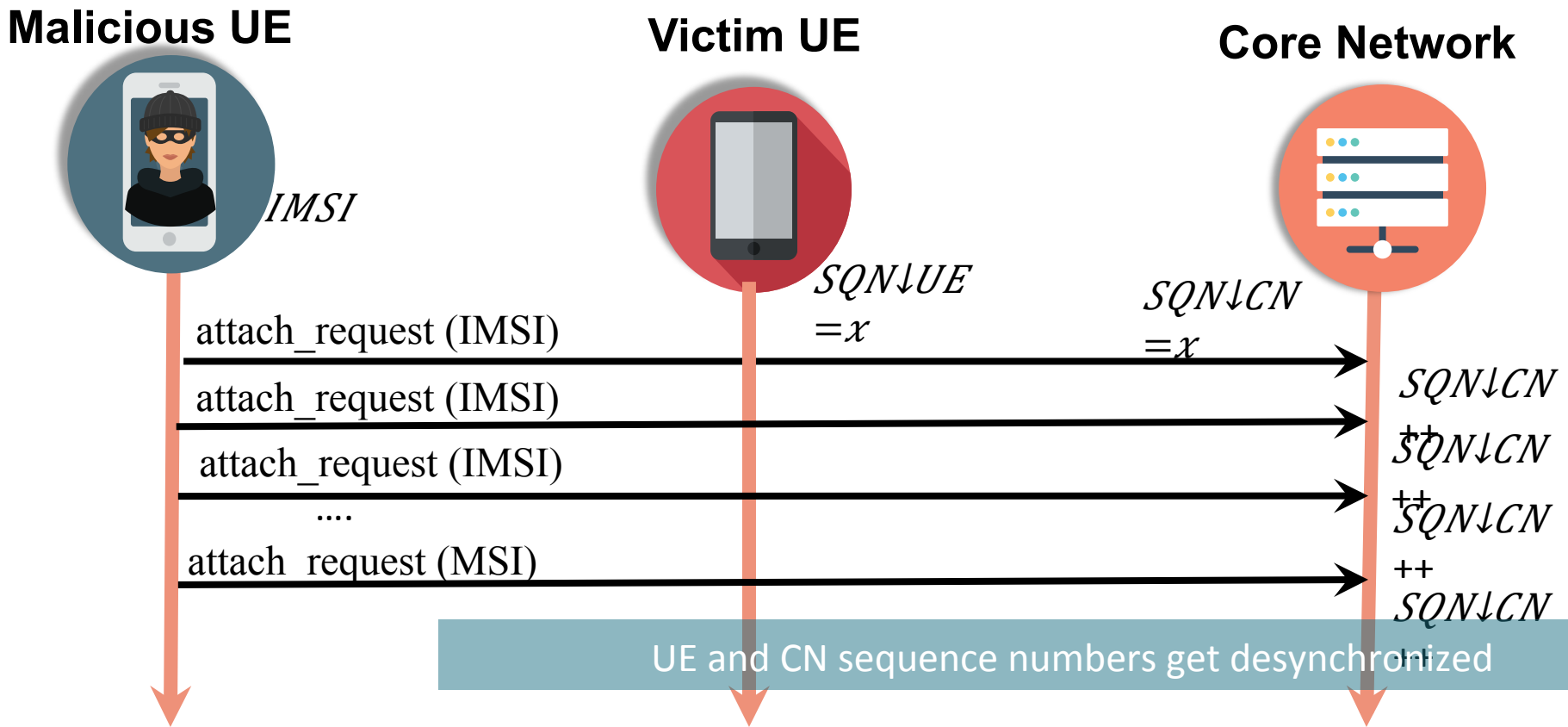
❑ Uncovered **10** new attacks

Attack	Procedures	Responsible	Notable Impacts
Auth Sync. Failure	Attach	3GPP	DoS
Traceability	Attach	carriers	Coarse-grained location tracking
Numb using auth_reject	Attach	3GPP, smartphones	DoS
Authentication relay	Attach	3GPP	Location spoofing
Paging Channel Hijacking	Paging	3GPP	DoS
Stealthy Kicking-off	Paging	3GPP	DoS, coarse-grained location tracking
Panic	Paging	3GPP	Artificial chaos for terrorist activity
Energy Depletion	Paging	3GPP	Battery depletion/DoS
Linkability	Paging	3GPP	Coarse-grained location tracking
Targeted/Non-targeted Detach	Detach	3GPP	DoS

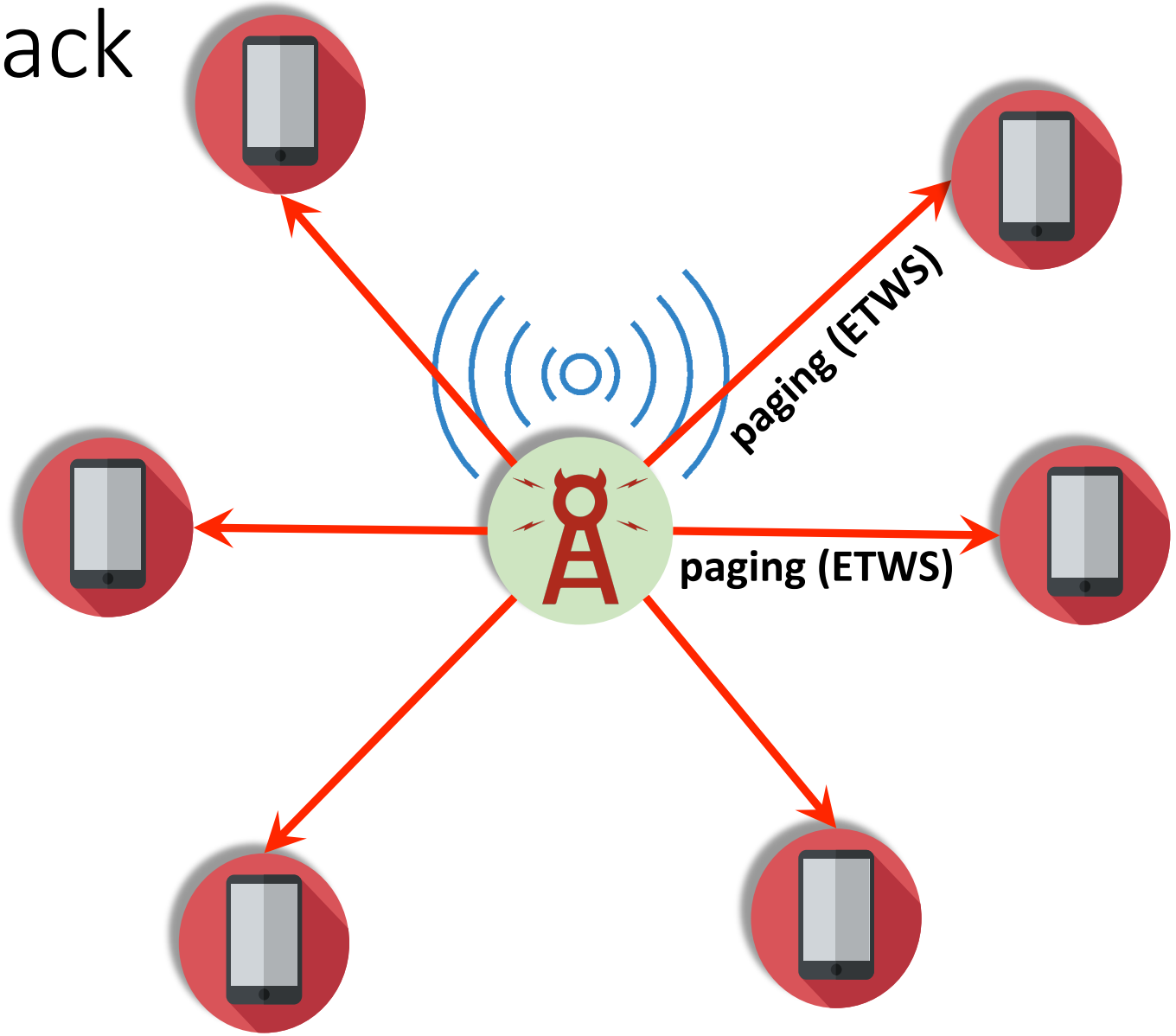
❑ Identified **9** prior attacks: IMSI-catching, DoS, Linkability, MitM in 3G and 2G, etc.

Authentication Synchronization Failure Attack

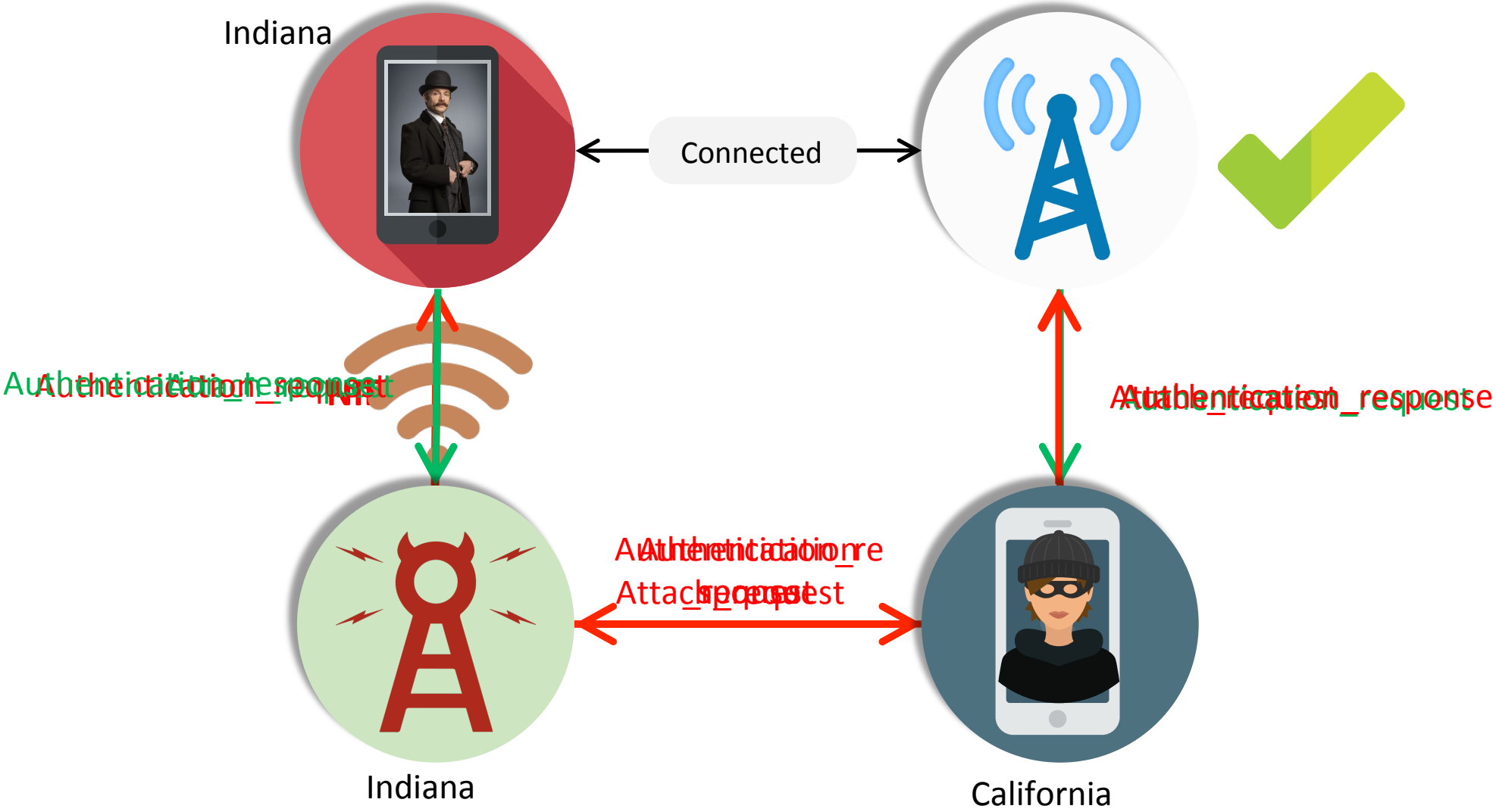
- Assumption:
  - Victim UE's IMSI
  - Malicious UE setup



Panic Attack



Attack Chaining (Authentication Relay or Mafia Attack)




Challenges
1
Preliminaries
2
LTEInspector
3
Findings &
Attack Validation
4
Responsible Disclosure
and Impact
5
Future Work
6
Conclusion
7

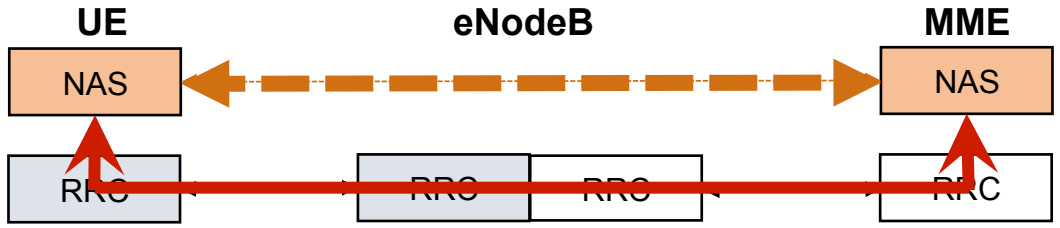
Responsible Disclosure and Impacts

- ❑ Mobile network operators
- ❑ Resolved the issue of using **EEA0 (no encryption)**
- ❑ **Other issues are in progress**

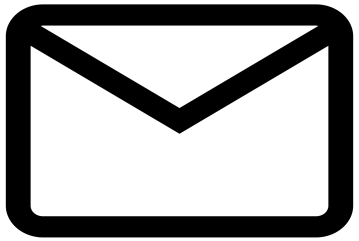

Challenges
1
Preliminaries
2
LTEInspector
3
Findings &
Attack Validation
4
Responsible Disclosure
and Impact
5
Future Work
6
Conclusion
7

Future Work

1



2



```
PCCH-Message ::= SEQUENCE
  +-message ::= CHOICE [c1]
    +-c1 ::= CHOICE [paging]
      +-paging ::= SEQUENCE [0110]
        +-pagingRecordList ::= SEQUENCE OF OPTIONAL:Omit
        +-systemInfoModification ::= ENUMERATED [true]
OPTIONAL:Exist
        +-etws-Indication ::= ENUMERATED [true] OPTIONAL:Exist
        +-nonCriticalExtension ::= SEQUENCE OPTIONAL:Omit
```

3


Challenges
1
Preliminaries
2
LTEInspector
3
Findings &
Attack Validation
4
Responsible Disclosure
and Impact
5
Future Work
6
Conclusion
7

Conclusion

Proposed a systematic approach for analyzing the specification

Jncovered 10 new attacks and 9 prior attacks

Validated most of the attacks in a testbed

https://github.com/relentless_warrior/LTEInspector

Questions

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

Syed Rafiul Hussain*, Omar Chowdhury†, Shagufta Mehnaz*, Elisa Bertino*

Purdue University*, University of Iowa†

Cryptographic Protocol Verifier

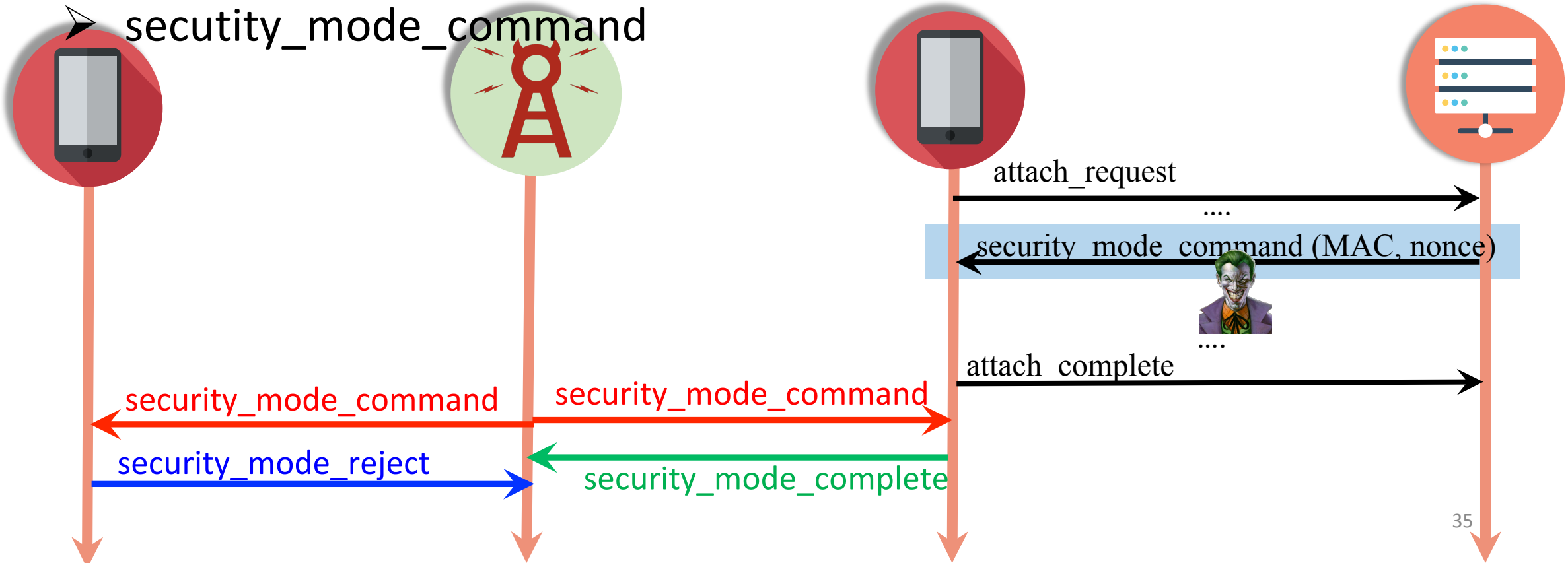
- Injective-correspondence (authentication)

  Every authentication_reject message received by UE must be sent by the core network

- ProVerif
  - Secrecy
  - Authenticity
  - Observational equivalence (hyper-properties)
- Why not ProVerif only?
  - Rich temporal trace properties
  - Constraints on linear integer arithmetic

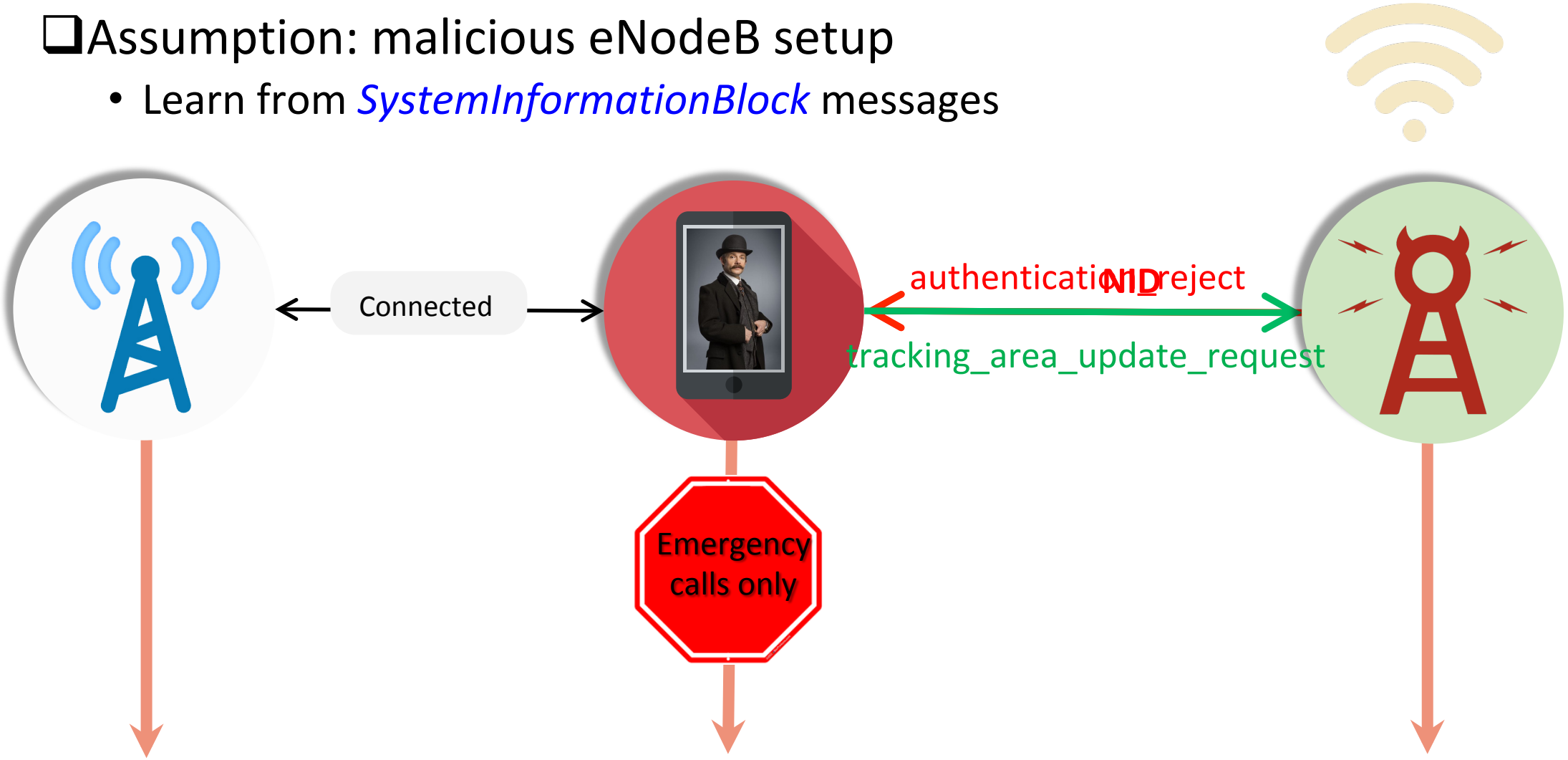
Traceability attack

- Assumption:
  - Victim UE's IMSI
  - Malicious UE setup
  - secutity_mode_command



Numb Attack

- Assumption: malicious eNodeB setup
  - Learn from *SystemInformationBlock* messages



Background (Attach)