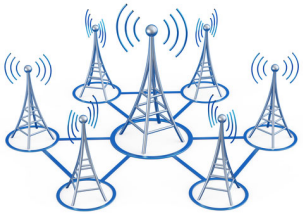
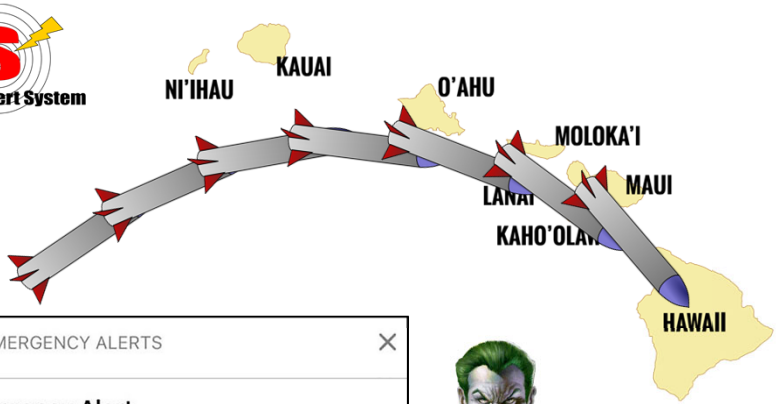
Security of 4G and 5G Cellular Networks

Elisa Bertino
Purdue University

In collaboration with
Syed Rafiul Hussain*, Omar Chowdhury†, Shagufta Mehnaz*
Purdue University*, University of Iowa†

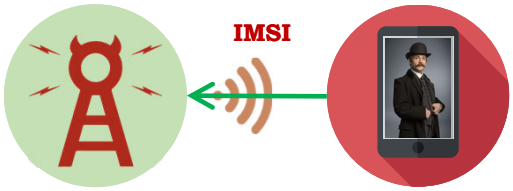
Cellular Network – a Critical Infrastructure





2

Security and Privacy Threats on Cellular Network



IMSI = International Mobile Subscriber Identity


CBCnews | Technology & Science

CBC INVESTIGATES | **RCMP reveals use of secretive cellphone surveillance technology for the first time**

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*

3

Limitations of Existing Attack Finding Strategies for Cellular Networks

No Systematic Approach

No adversary, just analyze the performance, and reliability

Location Leaks on the GSM Air

Denis Foo Kune, John Koelndorfer, Nicholas Ho

Control-Plane Protocol Interactions in

Guan-Hua Tu†*, Yuanjie Li†; Chunyi Peng†, Chi-Yu Li†, Hon
†University of California, Los Angeles ‡The Ohio State
†{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

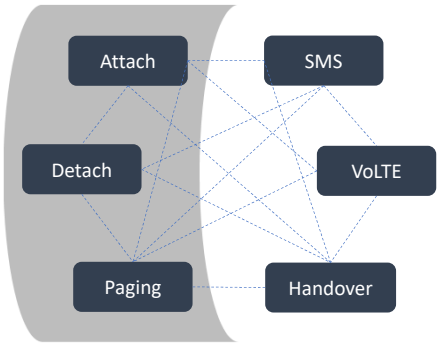
Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems

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?***

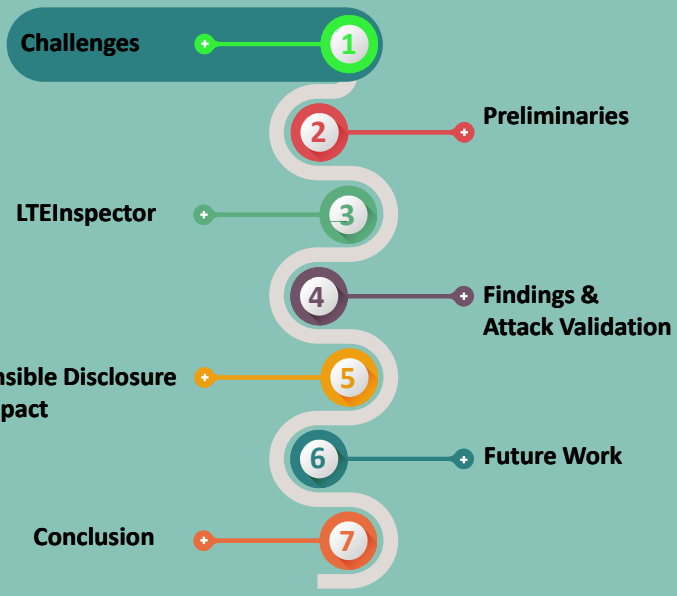
4

Scope



Man-in-the-Middle Attacker

Life threatening risks



Challenges

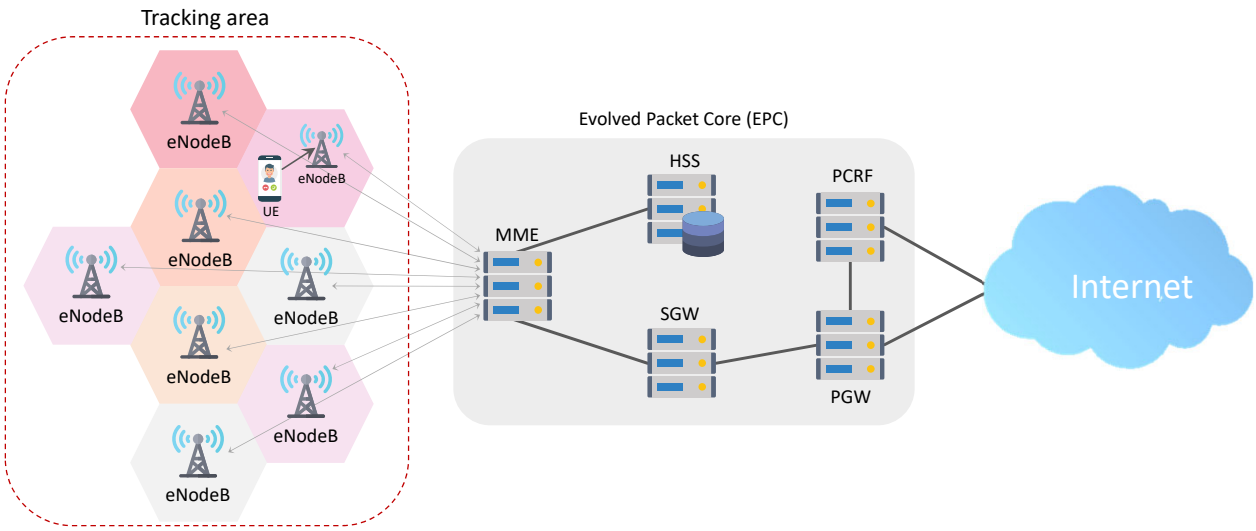
- ❑ Stateful procedures and multiple participants
- ❑ 4G LTE lacks formal specification
  - ✓written in natural language
- ❑ Closed system
  - ✓Proprietary
- ❑ Legal barrier
  - ✓Licensed spectrum

7

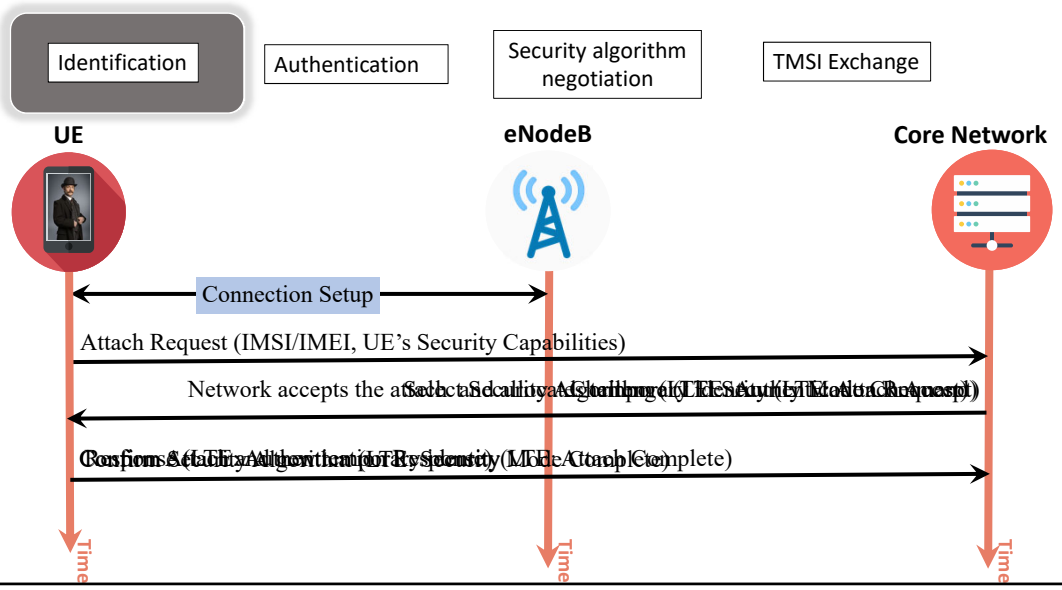
1. Challenges
2. Preliminaries
3. LTEInspector
4. Findings & Attack Validation
5. Responsible Disclosure and Impact
6. Future Work
7. Conclusion

8

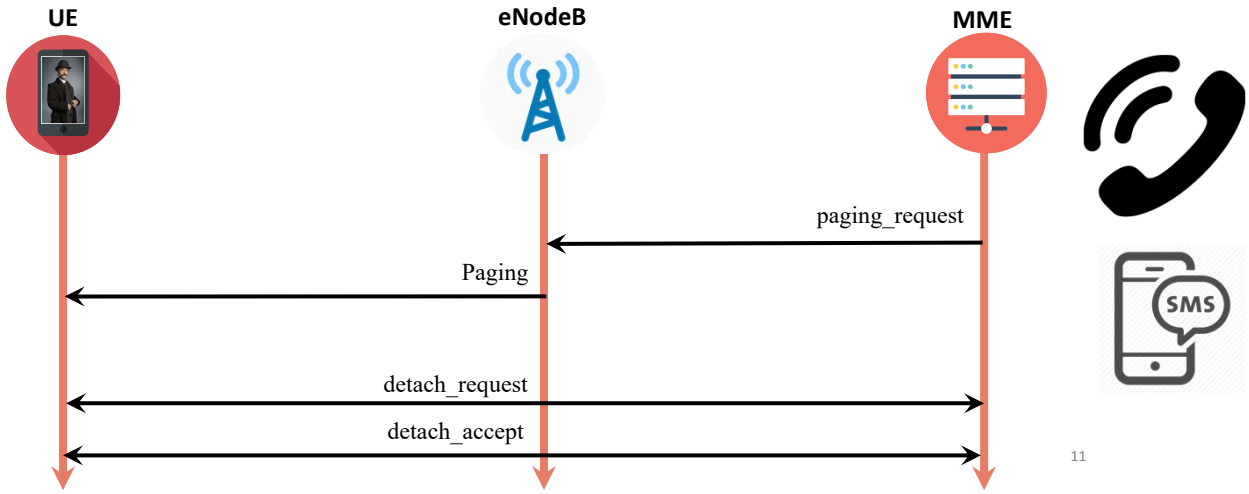
Background: LTE Architecture

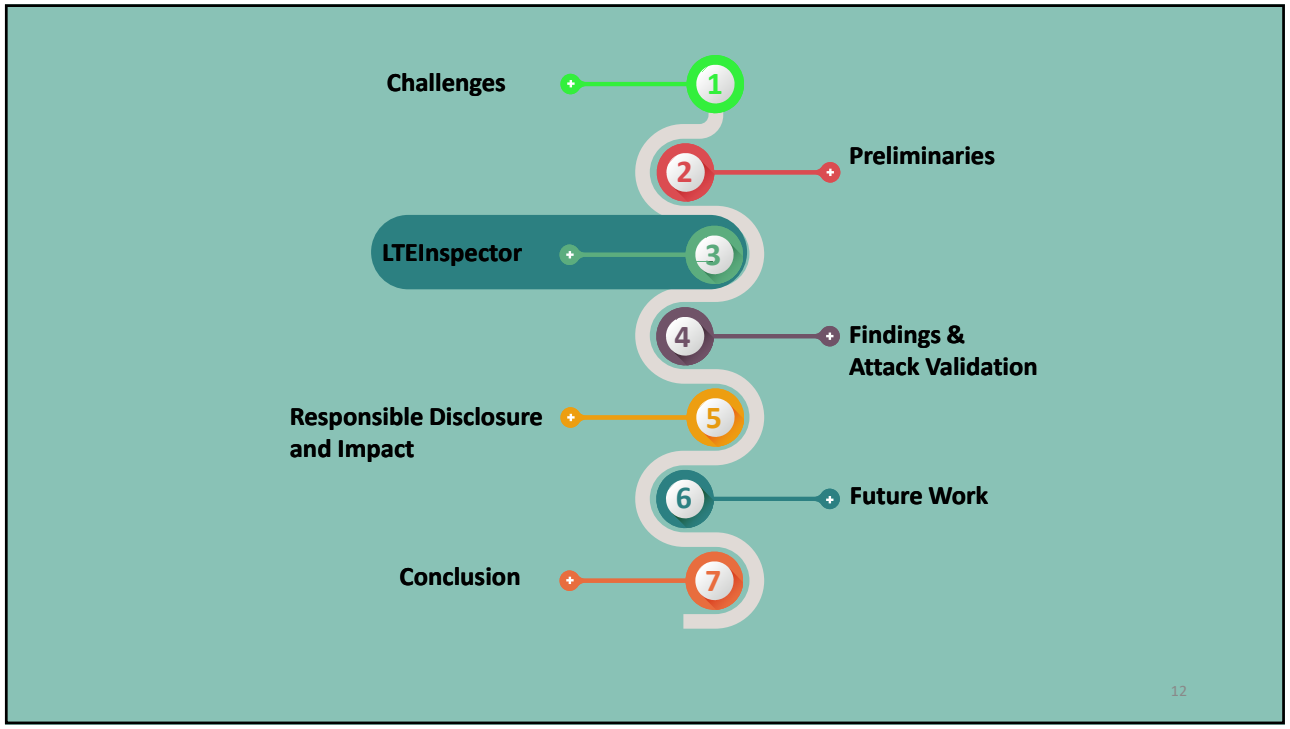


Background (Attach)

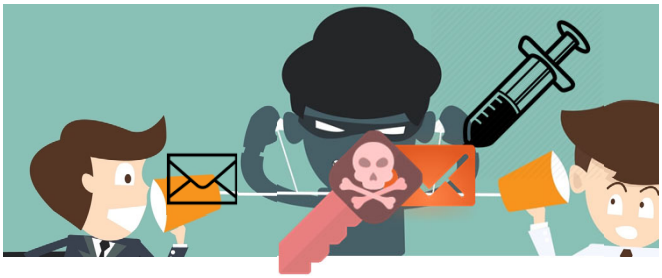


Background (Paging & Detach)





Adversary Model

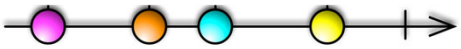


- Dolev-Yao model
  - Eavesdrop
  - Drop or modify
  - Inject
  - Adheres to cryptographic assumptions
- Why Dolev-Yao model?
  - Powerful adversary
  - Automatic tools (ProVerif, Tamarin) can be leveraged

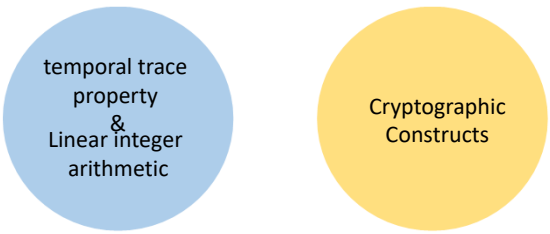
13

Insight

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



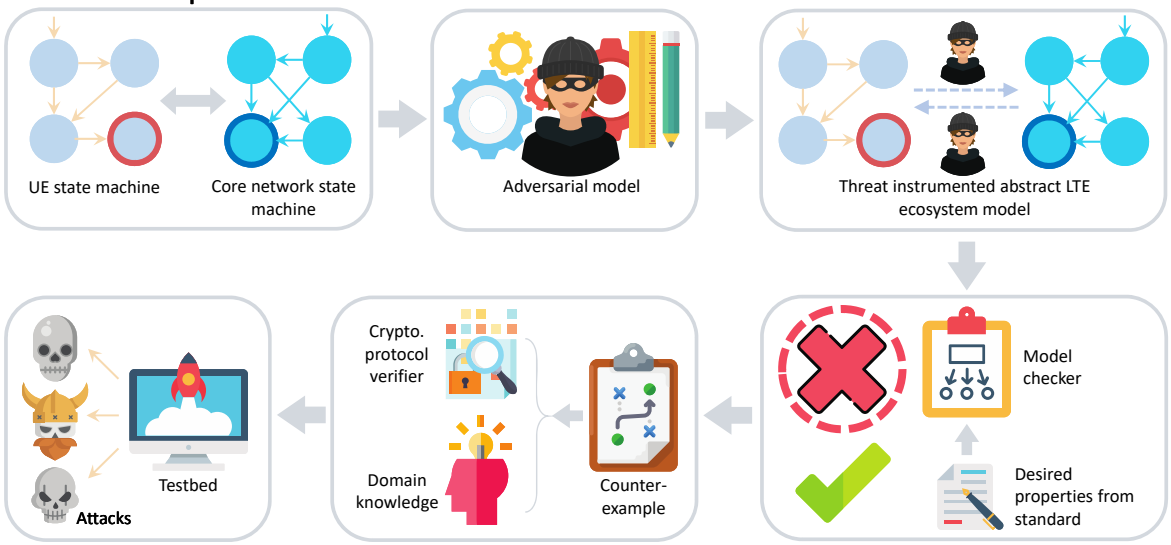
- Intuition:
  - ✓ Model checker
  - ✓ Cryptographic protocol verifier



How can we leverage reasoning power of these two?

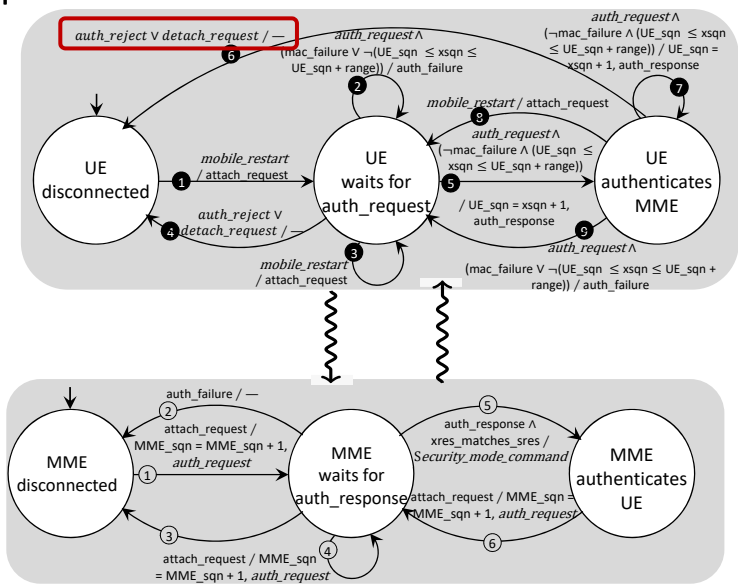
14

LTEInspector

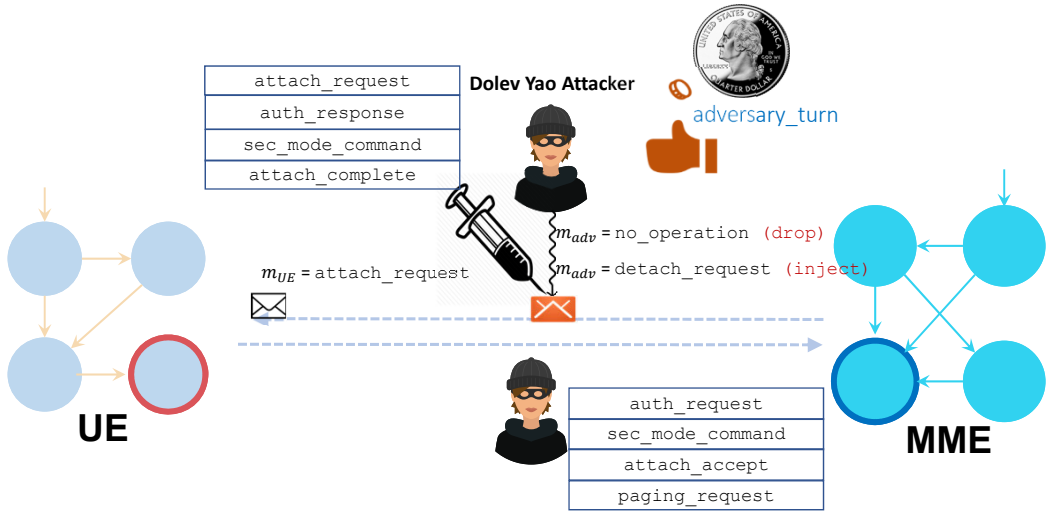


Abstract LTE Model

- 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

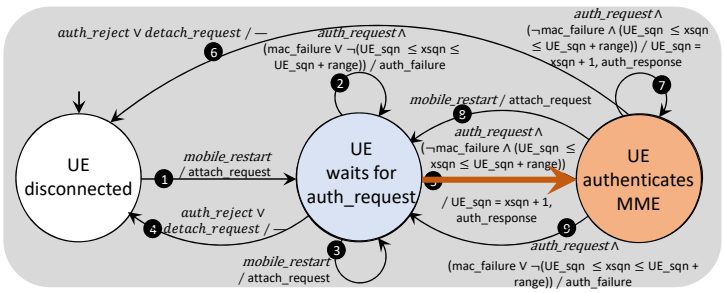


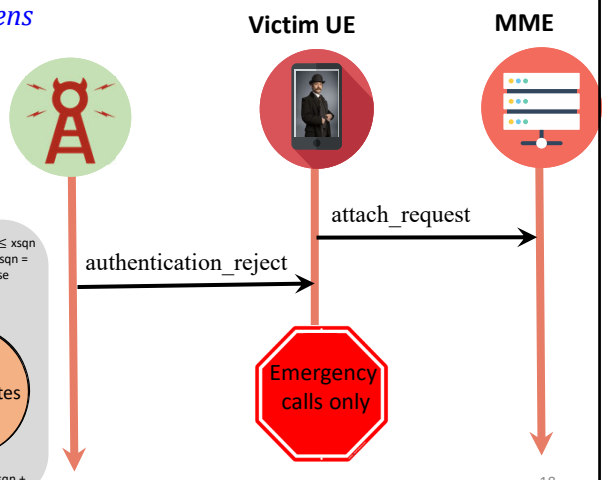
17

Model Checker

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

φ_1: It is always the case that whenever UE is in the *wait for auth request*, it will eventually *authenticates MME*.

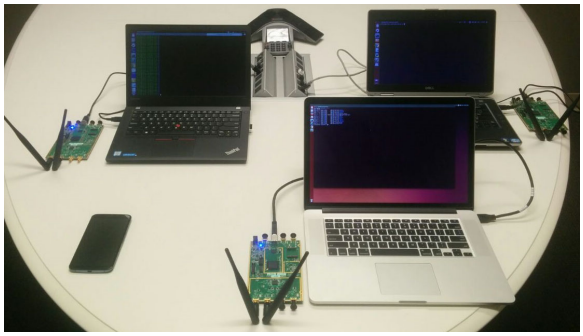




18

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



19

20

Findings

❑ Uncovered **10** new attacks

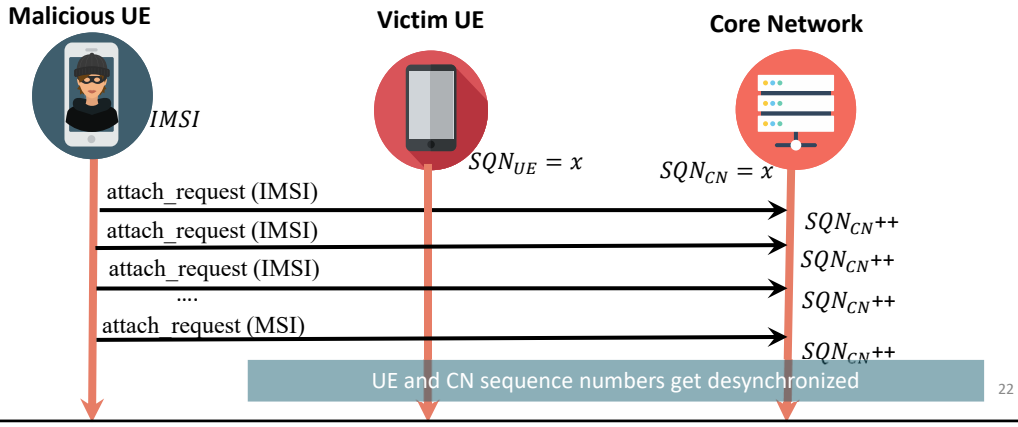
Attack	Procedures	Responsible	Notable Impacts
Auth Sync. Failure	Attach	3GPP	DoS
Traceability	Attach	carriers	Coarse-grained location tracking
Numb using auth_reject	Attach	3GPP, smartphones	DoS
Authentication relay	Attach	3GPP	Location spoofing
Paging Channel Hijacking	Paging	3GPP	DoS
Stealthy Kicking-off	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

❑ Uncovered **9** prior attacks: IMSI-catching, DoS, Linkability, MitM in 3G and 2G, etc. 21

Authentication Synchronization Failure Attack

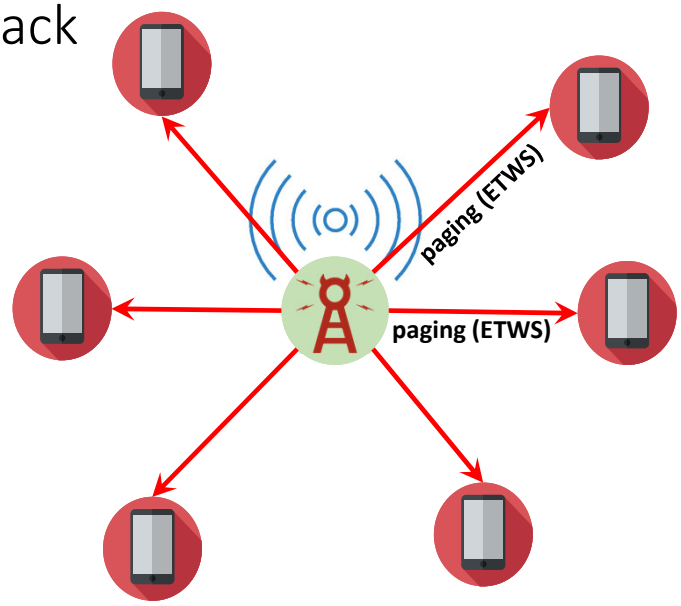
❑Assumption:

- ➢ Victim UE's IMSI
- ➢ Malicious UE setup



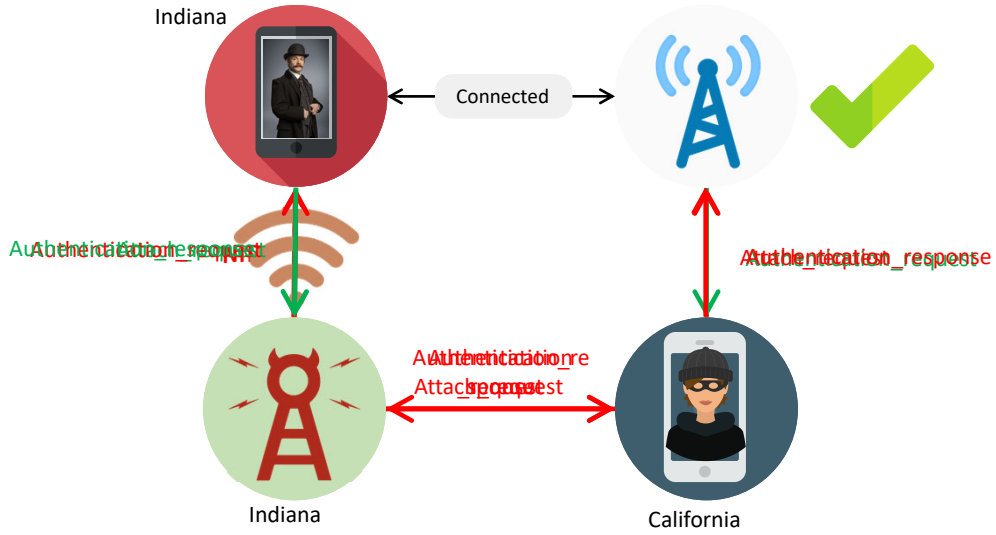
22

Panic Attack

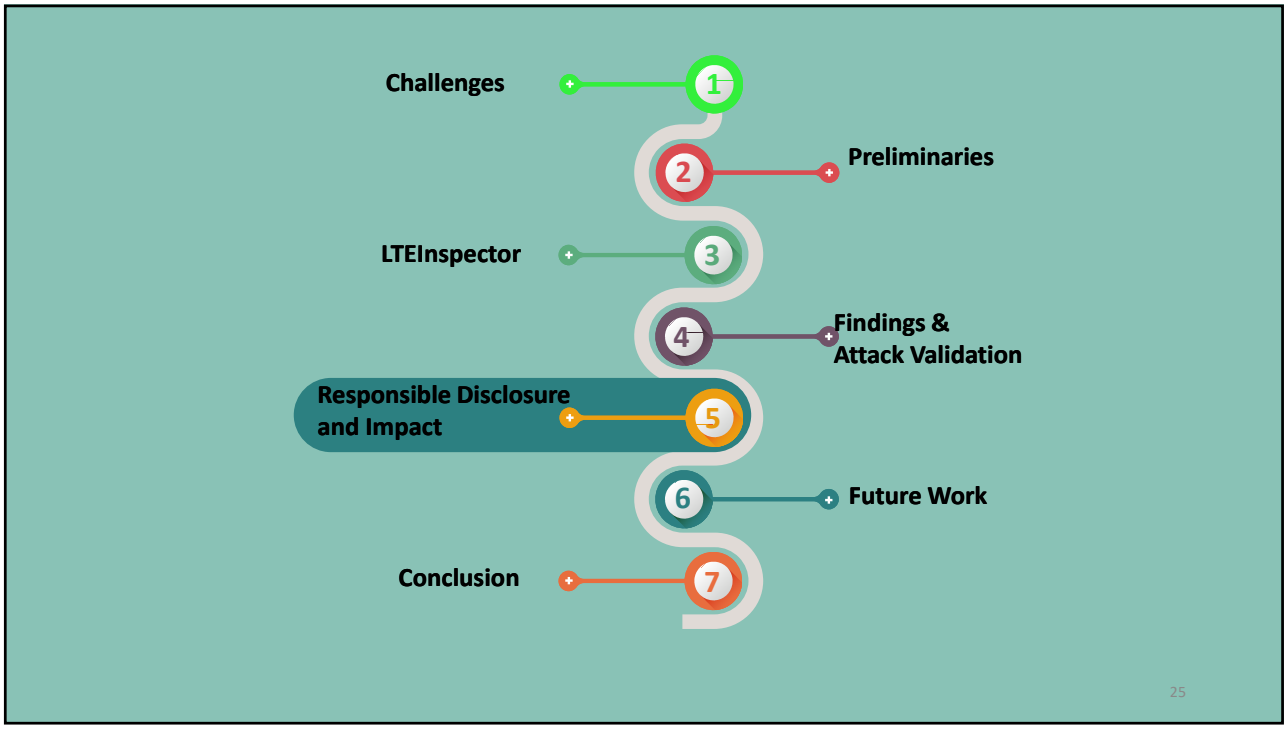


23

Attack Chaining (Authentication Relay or Mafia Attack)



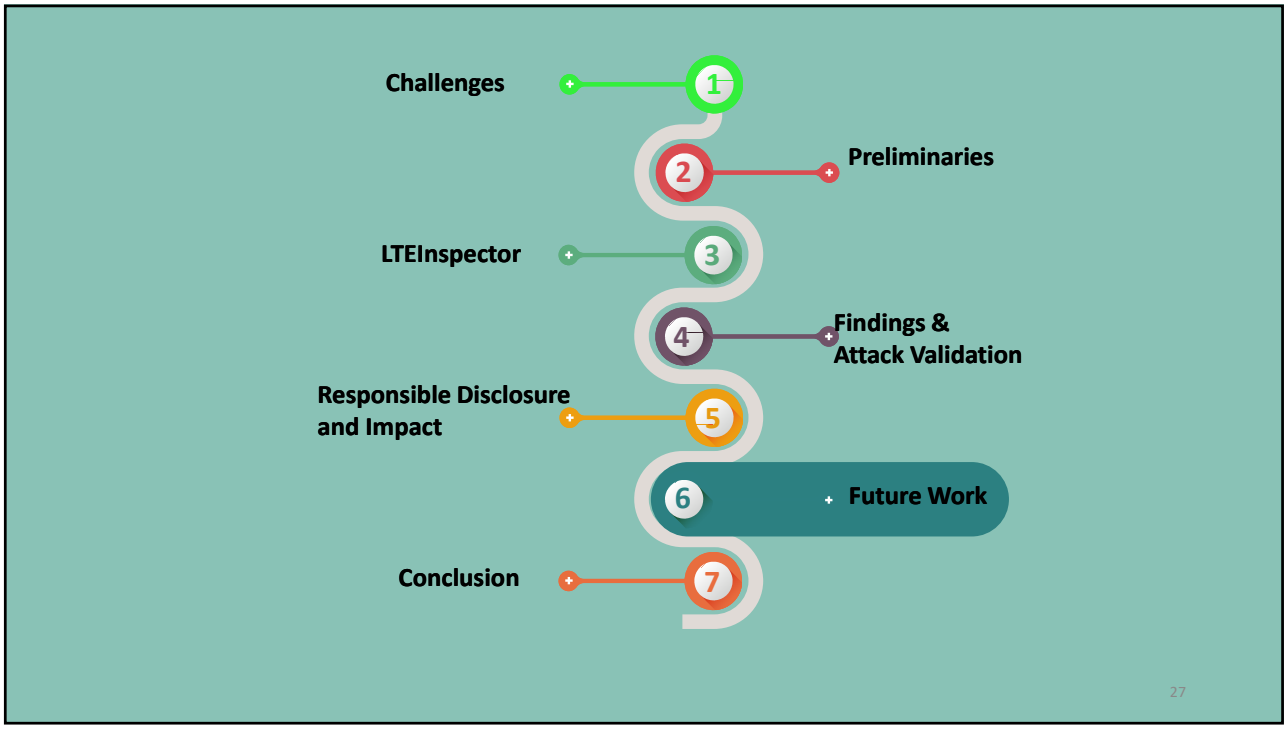
24



Responsible Disclosure and Impacts

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

26



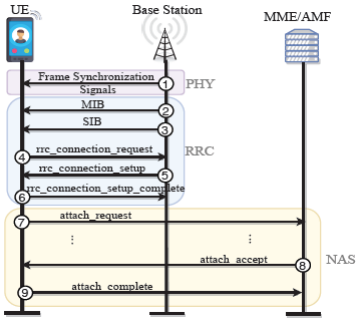
Future Work

- Use of LTEInspector to analyze implementations of 4G
- Analysis of 5G

28

Defenses – Initial Work

- UE's Cell Selection and bootstrapping
  - ❑ MIB – broadcast every 40ms
  - ❑ SIB – broadcast every 80ms
  - ❑ These messages are not digitally signed
- Possible approaches
  - ❑ Broadcast symmetric key authentication (3GPP suggests Tesla)
  - ❑ Asymmetric key authentication
- Requirements
  - ❑ *Minimize signature size* – critical to save bandwidth
  - ❑ *Minimize signature generation time* – critical because of MIB and SIB broadcast frequency
  - ❑ Minimize signature verification time – critical to reduce energy cost at the UE
- Elements of our solutions
  - ❑ PKI-level optimization: *design of a lightweight certificate*
  - ❑ Protocol-level optimization: *authentication only for SIB (and only for SIB1 and SIB2)*; *signature aggregation for SIB1 and SIB2*
  - ❑ Cryptographic scheme-level optimization: *use of BGLS + Structure-free and Compact Real Time Authentication (SCRA-BLGS)*



29

30

Conclusion


Proposed a systematic approach for analyzing the specification


Uncovered 10 new attacks and 9 prior attacks


Validated most of the attacks in a testbed


https://github.com/relentless-warrior/LTEInspector

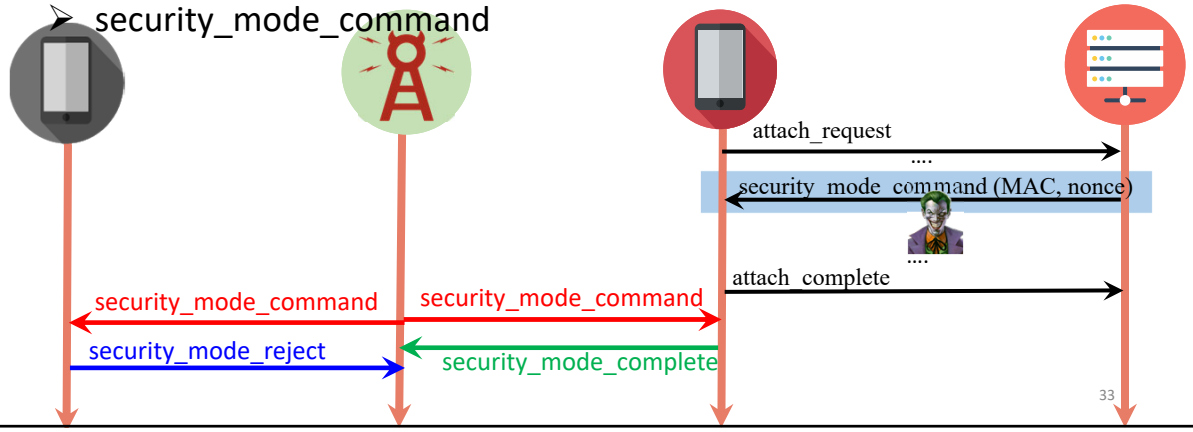
31

Questions

32

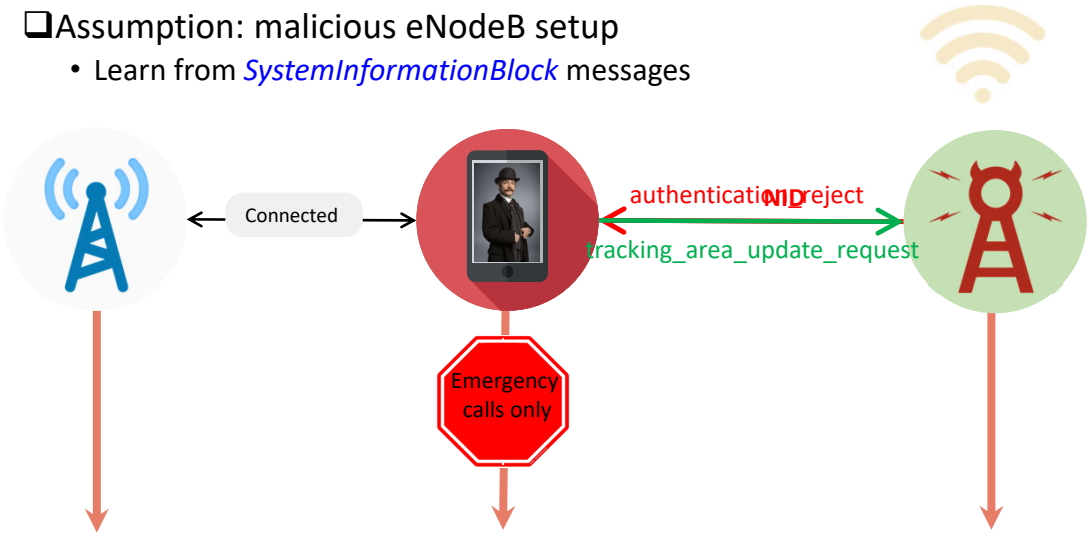
Traceability attack

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

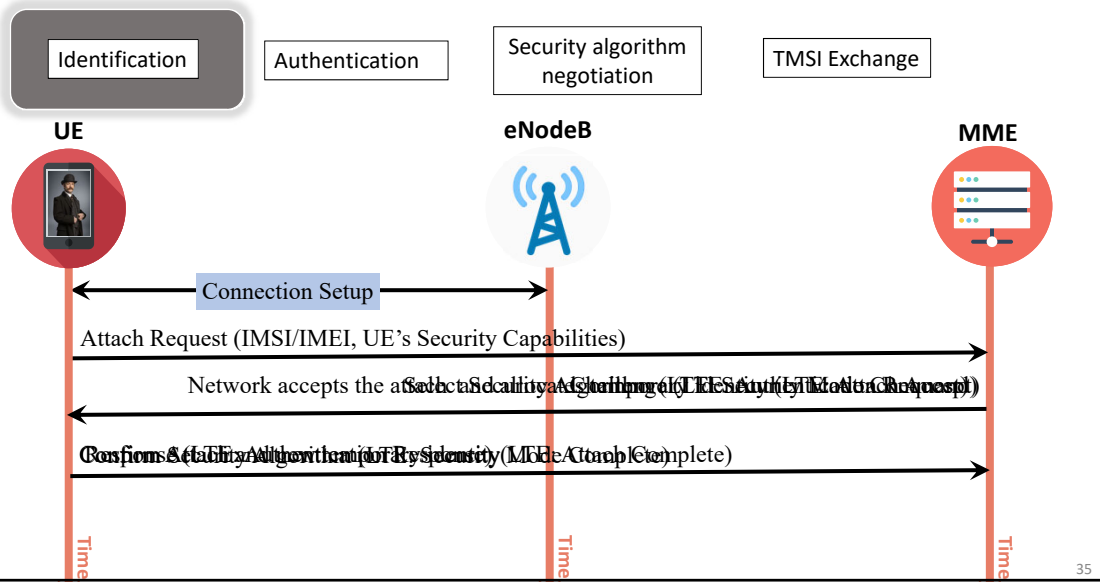


Numb Attack

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



Background (Attach)



35