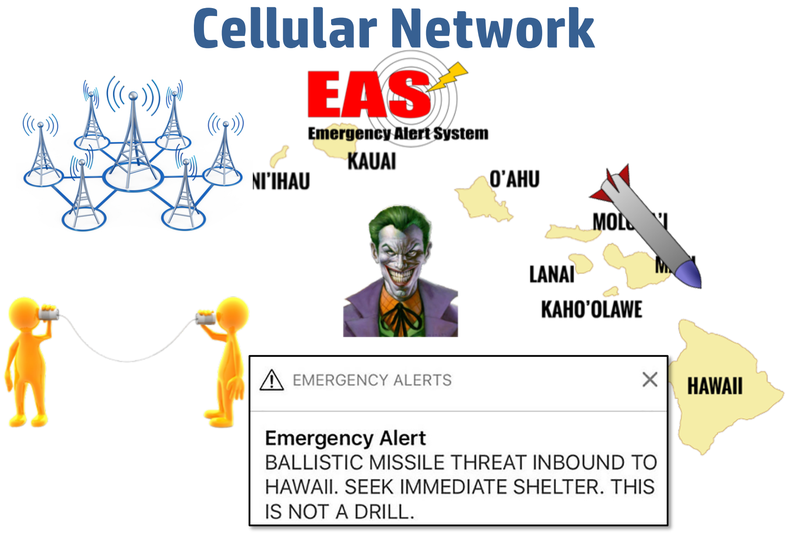
CERIAS

The Center for Education and Research in Information Assurance and Security

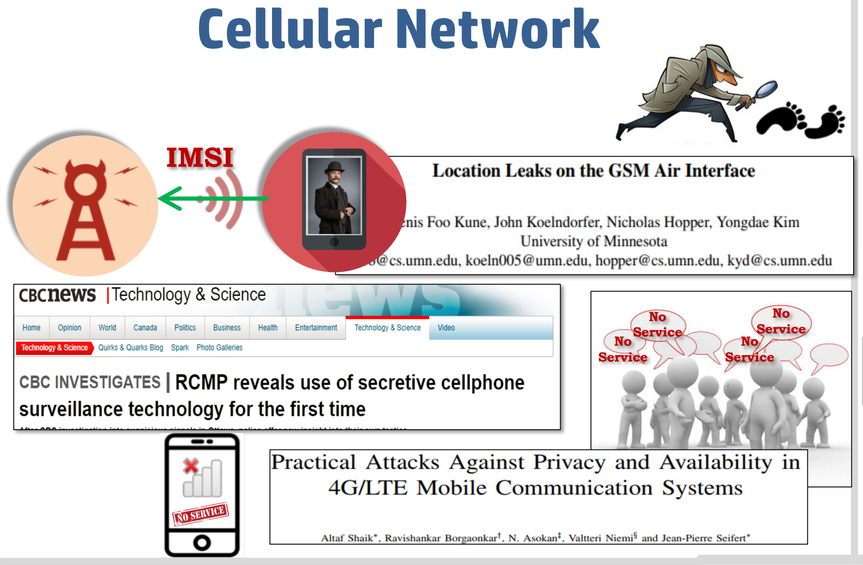
LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE

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

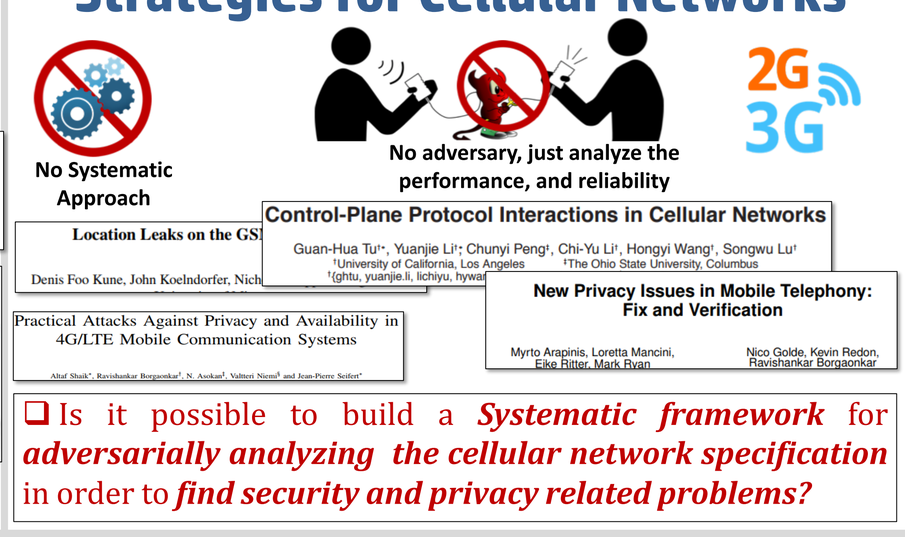
Critical Infrastructure using Cellular Network



Security and Privacy Threats on Cellular Network

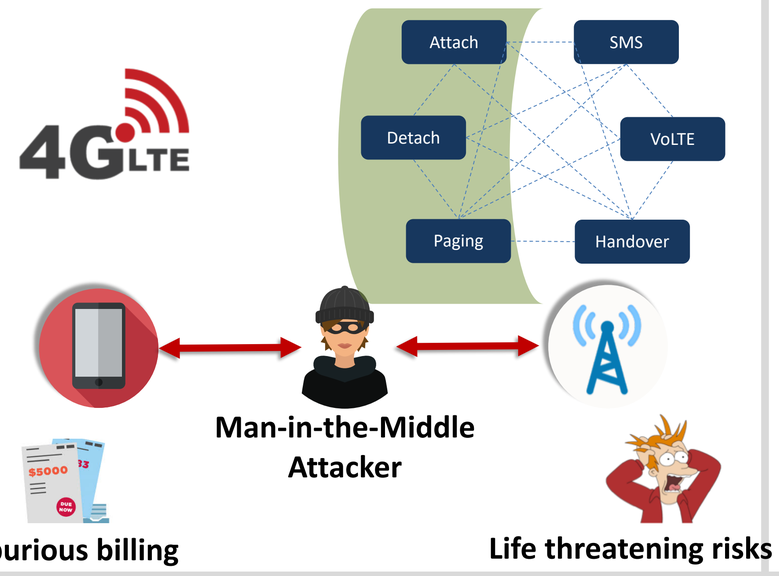


Limitations of Existing Attack Finding Strategies for Cellular Networks



❑ 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 of our work



Insight

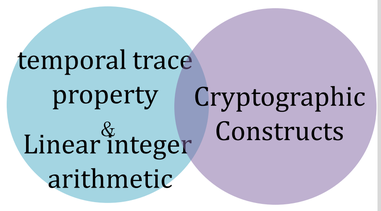
❑ **Property characteristics**

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

❑ **Intuition**:

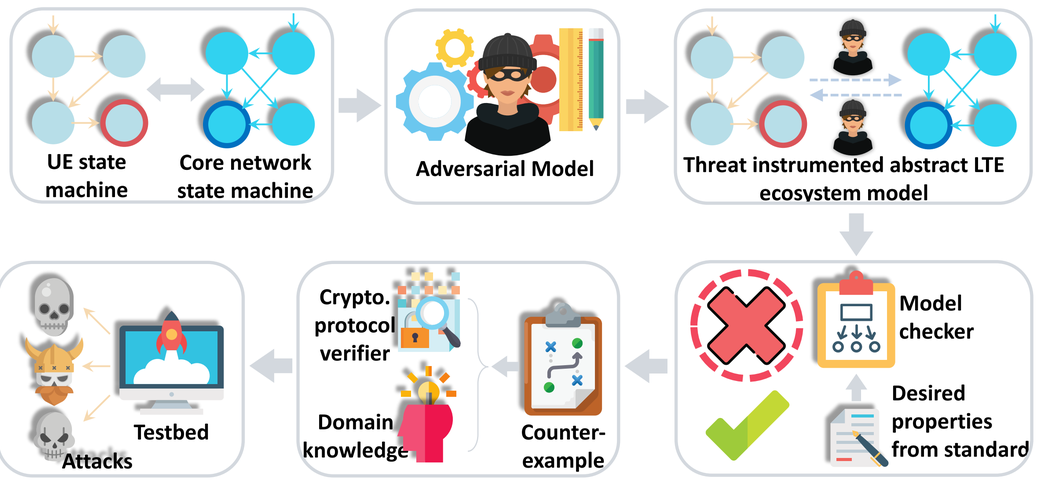
✓ Model checker

✓ Cryptographic protocol verifier



How can we leverage reasoning power of these two?

LTEInspector

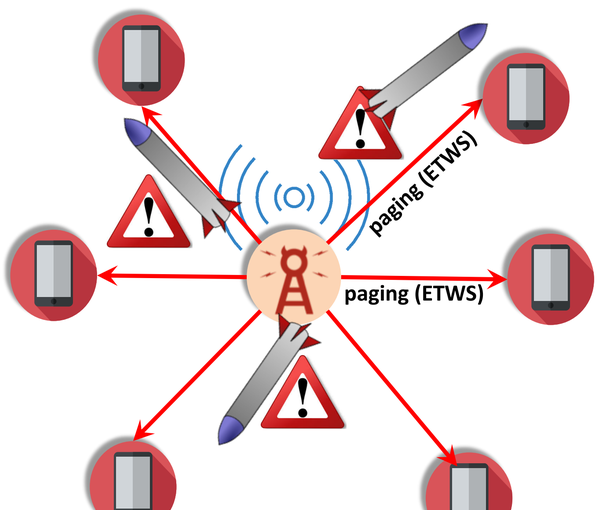


Abstract LTE Model

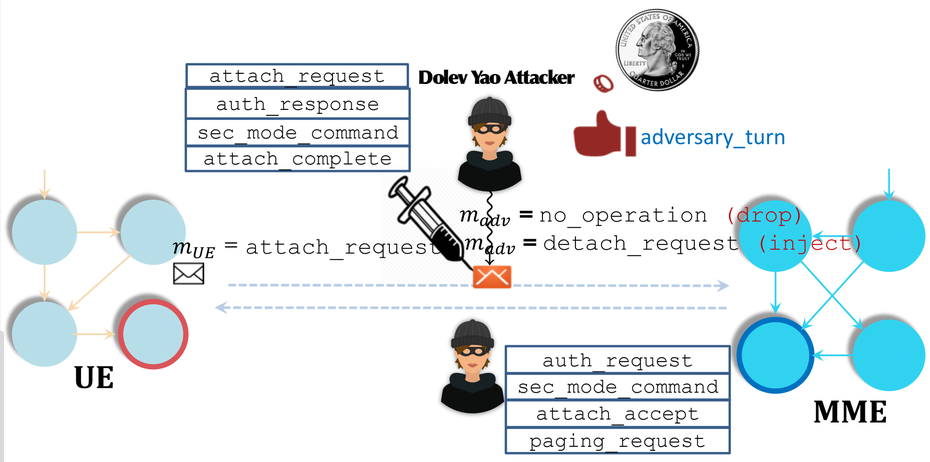
❑ Specification Model for NAS layer (UE-MME) interactions

- Propositional logic level
- Model message types only, not message data
- Abstract away cryptographic constructs
- Two unidirectional channels

Panic Attack



Adversarial Model Instrumentor



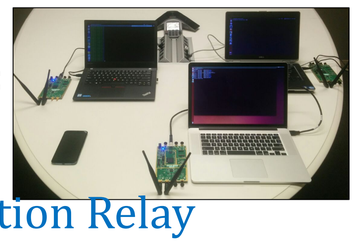
LTEInspector Findings

❑ Uncovered 10 new attacks

❑Detected 9 prior attacks

❑Notable attack: Authentication Relay

- *poison the location of the victim device.*
- *allow setting up a false alibi or planting fake evidence during a criminal investigation*



Model Checker

❑ Temporal trace properties

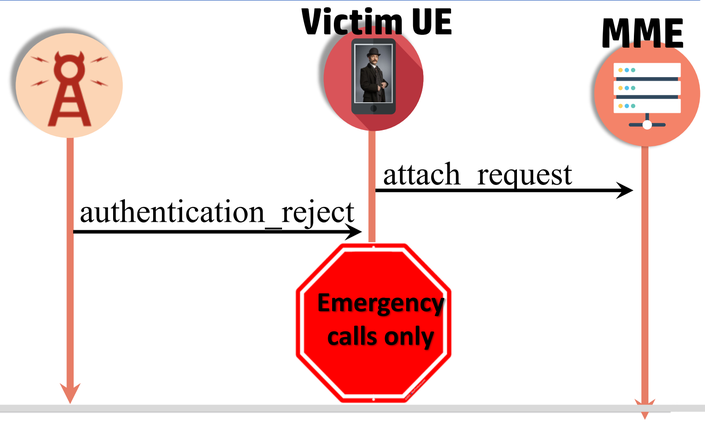
- Liveness–*something good eventually happens*
- Safety–*nothing bad happens*

❑ NuSMV

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

❑ Injective-correspondence

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



CERIAS

PURDUE UNIVERSITY