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

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

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

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

Ahad Shahr*, Ravishankar Borgohain†, N. Asokan‡, Valtteri Niemi§ and Jean-Pierre Steffes*
Limitations of Existing Attack Finding Strategies for Cellular Networks

No Systematic Approach

No adversary, just analyze the performance, and reliability

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

Attach, Detach, Paging, Handover, VoLTE, SMS, etc.

Spurious billing

Life threatening risks
Challenges

Preliminaries

LTEInspector

Findings & Attack Validation

Responsible Disclosure and Impact

Future Work

Conclusion
Challenges

- Stateful procedures and multiple participants

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

- Closed system
  ✓ Proprietary

- Legal barrier
  ✓ Licensed spectrum
Challenges

Preliminaries

LTEInspector

Findings & Attack Validation

Responsible Disclosure and Impact

Future Work

Conclusion
Background: LTE Architecture
Background (Attach)

**Attachment:**

- **Identification**
- **Authentication**
- **Security algorithm negotiation**
- **TMSI Exchange**

**UE**

- **Connection Setup**
  - Attach Request (IMSI/IMEI, UE’s Security Capabilities)
  - Network accepts the attach and allocates temporary identity (LTE: Attach Accept)
  - Confirm Attach and new temporary identity (LTE: Attach Complete)

**eNodeB**

- **Select Security Algorithm** (LTE: Security Mode Command)
  - Confirm Security Algorithm (LTE: Security Mode Complete)

**Core Network**

- Challenge (LTE: Authentication Request)
  - Response (LTE: Authentication Response)
Background (Paging & Detach)

UE → eNodeB → MME

- Paging
- detach_request
- detach_accept
- paging_request
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

UE state machine
Core network state machine
Adversarial model
Threat instrumented abstract LTE ecosystem model

Crypto. protocol verifier
Domain knowledge
Counter-example

Testbed
Attacks
Model checker
Desired properties from standard
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

Dolev Yao Attacker

\[
m_{\text{UE}} = \text{attach\_request}
\]

\[
m_{\text{adv}} = \text{no\_operation} \quad (\text{drop})
\]

\[
m_{\text{adv}} = \text{detach\_request} \quad (\text{inject})
\]

\[
\text{UE} 
\]

\[
\text{MME}
\]

\[
\text{attach\_request}
\]

\[
\text{auth\_response}
\]

\[
\text{sec\_mode\_command}
\]

\[
\text{attach\_complete}
\]

\[
\text{auth\_request}
\]

\[
\text{sec\_mode\_command}
\]

\[
\text{attach\_accept}
\]

\[
\text{paging\_request}
\]

\[
\text{adversary\_turn}
\]
Model Checker

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

\[ \phi_1 : \text{It is always the case that whenever UE is in the wait for auth request, it will eventually authenticate MME.} \]
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
## Findings

- **Uncovered 10 new attacks**

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

- **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

Malicious UE

Victim UE

Core Network

- $\text{SQN}_{\downarrow \text{UE}} = x$
- $\text{SQN}_{\downarrow \text{CN}} = x$

UE and CN sequence numbers get desynchronized
Panic Attack
Attack Chaining (Authentication Relay or Mafia Attack)
Responsible Disclosure and Impacts

- Mobile network operators

- Resolved the issue of using **EEA0 (no encryption)**

- Other issues are in progress
Challenges

Preliminaries

LTEInspector

Findings & Attack Validation

Responsible Disclosure and Impact

Future Work

Conclusion
Future Work

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
Challenges

Preliminaries

LTEInspector

Findings & Attack Validation

Responsible Disclosure and Impact

Future Work

Conclusion
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
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
  - security_mode_command

Assumption:
- Victim UE’s IMSI
- Malicious UE setup
- security_mode_command
Numb Attack

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

Connected → Emergency calls only

NID rejection → tracking_area_update_request
Background (Attach)

Identification
Authentication
Security algorithm negotiation
TMSI Exchange

UE
MME
eNodeB

Connection Setup
Attach Request (IMSI/IMEI, UE’s Security Capabilities)
Network accepts the attach and allocates temporary identity (LTE: Attach Accept)
Confirm Attach and new temporary identity (LTE: Attach Complete)
Select Security Algorithm (LTE: Security Mode Command)
Confirm Security Algorithm (LTE: Security Mode Complete)