LTE Security Disabled
Misconfiguration in Commercial Networks

Merlin Chlostaa, David Rupprecht, Thorsten Holz
RUHR UNIVERSITY BOCHUM

Christina Pöpper
NEW YORK UNIVERSITY ABU DHABI

May 16, 2019
Motivation – Complex Infrastructure

User

Base Stations

Core Network
Motivation – Complex Infrastructure

User → Base Stations → Core Network

- User
- Base Stations
- Core Network

**LTE Security Disabled: Misconfiguration in Commercial Networks | Merlin Chlosta | May 16, 2019**
Recent work focuses on specification, implementation
Configuration has potential to disable security measures
Security Capabilities
Security Capabilities

Integrity  Encryption

- NULL: X
- Snow3G: 
- AES: 
- ZUC: ?

<table>
<thead>
<tr>
<th>NULL</th>
<th>Snow3G</th>
<th>AES</th>
<th>ZUC</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>✔</td>
<td>✔</td>
<td>?</td>
</tr>
</tbody>
</table>

Mandatory

Optional
Security Capabilities

Emergency call without SIM

Integrity Encryption

NULL ❌❓

Snow3G ✔️
AES ✔️
ZUC ❓❓

Mandatory
Optional

Legislative requirement
Algorithm Negotiation

- Attach Request (Security Capabilities)
- Authentication and Key Agreement
- Security Mode Command (AES)
- Security Mode Command (AES)
Tools for Network Testing

Our paper: provide standard test — security algorithm support
Contribution: SIM cards and encryption for srsLTE

Commercial network support, tested at operator’s lab
SECURITY MODES

WHAT DO REAL NETWORKS SAY?
Test Procedure

Security Capabilities — Example Test Case

Attach (Security Capabilities)

Attach Accept (Cipher)

or

Attach Reject
Test Procedure

Security Capabilities — Example Test Case

<table>
<thead>
<tr>
<th>Integrity</th>
<th>Encryption</th>
<th>NULL</th>
<th>Snow3G</th>
<th>AES</th>
<th>ZUC</th>
<th>Plaintext</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Attach (Security Capabilities)

Attach Accept (Cipher)

or

Attach Reject
Drive Tests

- 12 operators in 5 countries
- Reception in hotels, mobility
- Car-mounted setup
RESULTS

WHAT COULD GO WRONG?
### Full Results

<table>
<thead>
<tr>
<th>AT-1</th>
<th>AT-2</th>
<th>CZ-1</th>
<th>CZ-2</th>
<th>CZ-3</th>
<th>DE-1</th>
<th>DE-2</th>
<th>DE-3</th>
<th>ES-1</th>
<th>ES-2</th>
<th>ES-3</th>
<th>FR-1</th>
</tr>
</thead>
</table>

**Null-Encryption & Null-Integrity**
Key Findings – Null-Integrity & Null-Encryption

NULL ok? — Sure

- Completely undermines LTE security goals
  - Unauthenticated users, network and traffic
- Enables impersonation attack in 3 out of 12 networks
  - Free data, anonymous Internet access.
Impersonation Attack

Attach Request → Attach Request (NULL) → Security Mode Command (NULL) → Authentication and Key Agreement

Man in the Middle
Impersonation Attack

Attach Request

Authentication and Key Agreement

Attach Reject

Attach Request (NULL)

Security Mode Command (NULL)

Attach Accept (IP)

Man in the Middle
Impersonation Attack

Attach Request -> Attach Request (NULL)

Authentication and Key Agreement

Attach Reject <- Security Mode Command (NULL)

Attach Accept (IP)

LTE SECURITY DISABLED: MISCONFIGURATION IN COMMERCIAL NETWORKS | MERLIN CHLOSTA | MAY 16, 2019
Worldwide Impact

Forward authentication via Internet
### Full Results

<table>
<thead>
<tr>
<th>Null-Encryption</th>
<th>AT-1</th>
<th>AT-2</th>
<th>CZ-1</th>
<th>CZ-2</th>
<th>CZ-3</th>
<th>DE-1</th>
<th>DE-2</th>
<th>DE-3</th>
<th>ES-1</th>
<th>ES-2</th>
<th>ES-3</th>
<th>FR-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null-Integrity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Null-Encryption & Null-Integrity**

**Insecure Fallback**
Key Findings – Insecure Fallback

NULL ok? — No. Go away.

ZUC ok? — No, but let’s talk NULL.
Key Findings – Insecure Fallback

Occurs in two cases

- Empty security capabilities (not even NULL signalled)
- Base station and core network disagree

NULL ok? — No. Go away.

ZUC ok? — No, but let’s talk NULL.
### Full Results

<table>
<thead>
<tr>
<th></th>
<th>AT-1</th>
<th>AT-2</th>
<th>CZ-1</th>
<th>CZ-2</th>
<th>CZ-3</th>
<th>DE-1</th>
<th>DE-2</th>
<th>DE-3</th>
<th>ES-1</th>
<th>ES-2</th>
<th>ES-3</th>
<th>FR-1</th>
</tr>
</thead>
</table>

**Null-Encryption & Null-Integrity**

**Insecure Fallback**

**Illegal Encoding**
Key Findings – Illegal Encoding

- Base station signals *undefined* “EIA7” integrity
- In practice: EIA7 == EIA0 == Null-Integrity
• GSMA Coordinated Disclosure CVD-2018-13
  – Contact with vendors, operators, standardisation
• Changes integrated to 4G, 5G standards
• Immediate mitigation by affected operators
• Null-integrity & null-encryption is reality
• Insecure Fallback
• Encoding Issues
• Impersonation Attack in Commercial Networks

Download at
https://github.com/mrlnc/eia0