IMP4GT
IMPersonation Attacks in 4G NeTworks

David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper
25.02.2020 NDSS Symposium, San Diego, USA
Motivation: Internet Passes
LTE Security Aims

- Mutual Authentication
- Traffic Confidentiality
- Identity & Location Confidentiality
Security Features

Authentication and Key Agreement

Connection
## Missing Integrity Protection

<table>
<thead>
<tr>
<th></th>
<th>Control Plane</th>
<th>User Plane</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>stream cipher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity Protection</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

- **Encryption stream cipher**: Both Control and User Plane have encryption enabled.
- **Integrity Protection**: Only the Control Plane has integrity protection enabled, while the User Plane does not.
Malleable Encryption

Encryption $10 \rightarrow $100

Stream Cipher

\[
\begin{array}{cccc}
1 & 0 & 1 & 0 \\
\oplus & & & \\
0 & 1 & 0 & 1 \\
\hline \\
1 & 1 & 1 & 1
\end{array}
\]

Decryption
Already Known: Redirection

Can it be worse?

Yes, with IMP4GT /ɪmpækt/

Rupprecht, D., Kohls, K., Holz, T., & Pöpper, C. “Breaking LTE on Layer Two”. In 2019 IEEE Symposium on Security and Privacy (SP)
Impersonation in 4G Networks (IMP4GT)

Breaks mutual authentication in both directions.
The Basic Principle

Malleable Encryption

Encryption Oracle

Decryption Oracle

Impersonation

Reflection
Reflection: ICMP Ping

IP / ICMP (ping) / Data

IP / ICMP (ping) / Data
Uplink Encryption Oracle

Encrypted on the Radio Layer
Uplink Enc + Downlink Dec = Full Impersonation

- Uplink Encryption
- Downlink Decryption
- Uplink Encryption
- Downlink Decryption
Experiments

• **Commercial** network and phone
• **Uplink** impersonation
  • Visit a website only accessible by a **victim**: pass.telekom.de
  • **Upload** a 10KB file to a server
• **Downlink** impersonation
  • **TCP** connection towards the phone
• **No** interaction of the user
  • **connectivitycheck.android.com**
  • Checks if you have an Internet connection
Consequences

Providers
- Over Billing
- Authorization

Law Enforcement
- Lawful Interception
- Lawful Disclosure Process

User
- Privacy
- Firewall / NAT
- IoT
Conclusion: We need Integrity Protection!

- Fully specified and deployed
- Optional integrity protection
- Unlikely...
- Limited support in early implementations

We emphasize the need for mandatory integrity protection.

David Rupprecht  
Ruhr University Bochum  
david.rupprecht@rub.de  
https://imp4gt-attacks.net