Advanced interconnect attacks

*Chasing GRX and SS7 vulns*

Karsten Nohl <nohl@srlabs.de>
Luca Melette <luca@srlabs.de>
Agenda

- IMSI catcher catching
- GRX attack potential
- GRX exposure
- Research outlook
Thank you so much for growing GSMmap!

Submissions to GSMmap.org

Countries covered on GSMmap.org
SnoopSnitch catches cell detection analyzes a cell’s config and behavior

SnoopSnitch combines three types of IMSI catcher heuristics

A. Suspicious cell configuration
- No proper neighbors
- Out-of-place location area
- High cell reselect offset, low registration timer
- Large number of paging groups

B. Suspicious cell behavior
- IMSI+IMEI requests during location update
- Immediate reject after identity request
- Paging without transaction
- Orphaned traffic channel

C. Lack of proper encryption
- No encryption -or-
- Downgrade to crackable A5/1 or A5/2
- Delayed Cipher Mode Complete (due to A5/1 cracking time)

SnoopSnitch assigns a score to each heuristic\(^1\) and sums scores to form catcher events

1 Metric details: opensource.srlabs.de/projects/snoopsnitch/wiki/IMSI_Catcher_Score
Majority of IMSI catcher sightings has medium score

Some chance of false positives. Certainty threshold revised upwards multiple times as we learned about false positive causes (discussed next)

Near-certain catcher sightings. Several heuristics triggered (3%)
Many heuristics trigger regularly

<table>
<thead>
<tr>
<th>Description</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption downgrade [C1]</td>
<td>454</td>
</tr>
<tr>
<td>Silent call [T4]</td>
<td>12</td>
</tr>
<tr>
<td>Paging w/o transaction [T3]</td>
<td>13</td>
</tr>
<tr>
<td>ID requests during LU [C4]</td>
<td>77</td>
</tr>
<tr>
<td>Inconsistent neighbors [R1]</td>
<td>60</td>
</tr>
<tr>
<td>Low registration timer [T1]</td>
<td>21</td>
</tr>
<tr>
<td>High reselect offset [K2]</td>
<td>19</td>
</tr>
<tr>
<td>No neighbors [K1]</td>
<td>2</td>
</tr>
<tr>
<td>Lonesome LAC [A5]</td>
<td>356</td>
</tr>
<tr>
<td>Inconsistent LAC [A2]</td>
<td>9</td>
</tr>
</tbody>
</table>
IMSI catcher detection pitfalls (1/3)

- False positive causes
  - Suspicious cell configuration
    - No proper neighbors
    - Lonesome location area
    - Out-of-place location area

1. Networks often change abruptly; e.g. when entering the subway
2. SnoopSnitch cannot directly read the radio channel (ARFCN) from the baseband. In the few cases its heuristic guesses wrong, an IMSI catcher event is reported
### B IMSI catcher detection pitfalls (2/3)

#### False positive causes

- Femto cells behave very similar to IMSI catchers:
  - a. Query IMSI + IMEI (for whitelisting)
  - b. Reject all but their owner’s phones
  - c. Implement radio protocols somewhat incomplete
  - d. Use hardware similar to small IMSI catchers

#### Suspicious cell behaviour

- IMSI + IMEI requests during location update
- Immediate reject
**IMSI catcher detection pitfalls (3/3)**

1. Some networks alternate between ciphers! For example, E-Plus Germany:
   
   \[
   \begin{array}{cccccc}
   \text{A5/3} & /3 & /1 & /3 & /3 & /1 & /3 \\
   \end{array}
   \]

2. Can IMSI catchers really not use A5/3 and other strong crypto? We are about to find out!
Spot the difference: Not all catcher events are being uploaded

<table>
<thead>
<tr>
<th>SnoopSnitch</th>
<th>App ID: 83ead3d4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 IMSI Catcher</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Last 24 hours**

- 06:55
- 07:00
- 07:05
- 07:10
- 07:15
- 07:20
- 07:25
- 07:30
- 07:35
- 07:40
- 07:45
- 07:50

**Score:** 3,00

**Time:** 21 avr. 2015 07:54:13

**Location:** 45.7350672 | 4.8233948

**Cell ID:** 208/10/49539/0

**Posted to Twitter but not uploaded for further analysis**
Agenda

- IMSI catcher catching
- GRX attack potential
- GRX exposure
- Research outlook
The GRX network connects nodes along the Internet access path of mobile phones.

- Phone configures an APN
- The APN’s DNS entry determines which GGSN is used
- GGSN typically stays the same even when roaming

**PDP Context** – Collection of identifiers needed for data flow, including: TEID←, TEID→
Can attackers abuse GRX for data intercept?

Research question: What can attackers do on GRX?

Attacker needs –
1. GRX connectivity? Not always! (discussed herein)
2. IP of current SGSN. Query through:
   a. SRI-GPRS over SS7
   b. SRI-GPRS over GRX
   c. Send SGSN-ContextRequest to all possible SGSNs; one will respond
3. Subscriber IMSI. Several methods exist for IMSI extraction
   a. Various SS7 / HLR queries
   b. IMSI catching
   c. Passive sniffing
   d. Guessing from IMSI range (non-targeted)

Prerequisites:
SGSN reachability and IMSI

SGSN  GRX  GGSN

DoS      ✓  → P1Sec @ HITB
Fraud    ✓
MITM
Local intercept
Hijacking

Focus of this talk

SECURITY RESEARCH LABS
Simple GRX attack ideas face challenges

**Attack idea 1 – Full MITM by spoofing SGSN and GGSN**

- **Catch** – Attack assumes knowledge of TEIDs from CreatePDP, which is only accessible if you are already MITM.

- **UpdatePDP(TEID<->)** sets new GGSN IP

- **UpdatePDP (TEID-> -or- IMSI)** pretends that the subscriber moved to a different SGSN
Attack variant encounters further roadblocks

**Attack idea 1’ – Full MITM by spoofing SGSN and GGSN**

**Catch 2 –**
Standard only specifies setting new IP when request is sent towards GGSN; fails on all SGSNs we tried

1. `SGSNContext-Req(IMSI)`
2. `UpdatePDP(TEID→)`

**Catch 1 –**
Still don’t know `TEID→`

Partial solution – Entropy bugs in some SGSNs:
- `TEID→ = 86093C47`
- `TEID← = 86498247`

**3. UpdatePDP(TEID←)** to set new GGSN IP

### Diagram:
- SGSN
- GGSN
- Attacker

1. `SGSNContext-Req(IMSI)`
2. `UpdatePDP(TEID→)`
3. `UpdatePDP(TEID←)`

TEID→, GGSN IP
Simple handover attempts fail (1/2)

**Attack idea 2 – Abuse handover (target-initiated)**

**Catch** – RNC may send data directly to GGSN but ignore the update. (RNC assumes the phone is idle anyway)

1. SGSNContextReq
2. Context Ack

16
Simple handover attempts fail (2/2)

**Attack idea 3 – Abuse handover (serving-initiated)**

**Catch** – The ‘radio msg’ specifies a channel on which the target phone is supposed to be waiting. But it isn’t
Forced connection establishment fails for current phones

**Attack idea 4 – Abuse network-initiated connection establishment**

**Catch** – The phone must be registered to the network but with no data connection established. Since newer phones always try to maintain a data connection, they seem to not support this mechanism, and reject

1. **PDUNotificationReq** (IMSI, APN, IP)
   This message is used when data is received for a non-connected phone. It establishes a new connection

2. **ActivatePDP**
3. **Accept**

**SGSN**

**GGSN**

**Attacker**
APN replacement is often prevented through whitelists

**Attack idea 5 – Rewrite APN over SS7**

1. InsertSubscriber-Data(Camel server) cancels data connection
2. Phone reconnects (immediately)
3. Sends APN to Camel server for verification
4. Looks up GGSN IP as apn.mcc.mnc.gprs
5. Connects to attacker GGSN

**Catch 2** – Many operators filter APNs:
- Use default APN for home users
- Maintain operator-to-APN whitelist

**Catch 3** – Requires Camel v3, which only minority of operators supports as of now

<table>
<thead>
<tr>
<th>SS7 STP</th>
<th>Camel server</th>
<th>GGSN</th>
<th>Attacker</th>
</tr>
</thead>
</table>

**Catch 1** – SGSN may ignore Camel-supplied APN and use higher priority default

**Solution** – Configure OI over SS7, which has highest priority
Attack 1: Fully-encrypting voice+data IMSI catcher

**Catch IMSI**
- NanoBTS or any other small cell

**Request auth/encryption keys over GRX or SS7**
- GRX: SGSNContextReq
- SS7: SendAuthInfo or SendIdentification
- Usually possible over GRX or SS7 connection
- Also possible over the Internet? (next chapter)

**Offer encrypted voice and data service**
- Passes mutual auth
- 2G Voice: A5/3
- 2G Data: GEA/3
- 3G: UEA/1 & UIA/1

GPRS Encryption Algorithm GEA/3 (3)
Agenda

- IMSI catcher catching
- GRX attack potential
- GRX exposure
- Research outlook
GTP is highly exposed on the Internet
A small but significant number of exposed GTP endpoints are SGSNs

- Brazil: 267
- Tim: 267
- China: 153
  - China Mobile: 76
  - Guangdong Mobile: 65
  - Shanghai Mobile: 12
- Korea: 58
  - SK Telecom: 54
  - Korea Telecom: 4
- Colombia: 47
  - Colombia Móvil: 47
- USA: 10
  - NewCore Wireless: 8
  - Union Cell: 1
  - Globecom: 1

+ Angola, Congo, Central African Republic, Ivory Coast, Cape Verde, Gambia, Guinea, Guam, India, Kuwait, Laos, Madagascar, Mexico, Malaysia, Romania, Rwanda, Sierra Leone, Chad, Tanzania, Vietnam

+ Many more SGSN/MME are reachable from an operator’s customer IP segment
Exposed SGSNs talk to anybody on the Internet

root@scan:~# ./sgsn_probe.sh 211.234.233.0/24 220.103.193.0/24

Target list: 508 host(s)
Starting GTP Echo scan on port 2123... done.
Starting GTP Echo scan on port 2152... done.
Got 190 responses
Sending SGSN probe payload... done.
Got 54 responses
Saving to sgsn_ok.iplist

root@scan:~# ./get_context.sh 450050417xxxxxx sgsn_ok.iplist

Starting tshark on eth1
Sending SGSN context request to 54 host(s)
Response filtering (gtp.cause == 128)
Verbose context dump:
  Ciphering key CK: baf49a6610370984f823a20d9xxxxxx
  Integrity key IK: 15d743e469e2e2ef64e63bf8d4xxxxxx
  PDP type: IPv4 (33)
  PDP address length: 4
  PDP address: 10.63.150.161 (10.63.150.161)
  GGSN address length: 4
  GGSN Address for control plane: 172.28.29.116 (172.28.29.116)
  GGSN 2 address length: 4
  GGSN 2 address: 172.28.29.116 (172.28.29.116)
  APN length: 37
  APN: web.sktelecom.com.mnc005.mcc450.gprs

SGSNs disclose current encryption key on the Internet!
Attack 2: Passive data intercept

Capture bursts
- NanoBTS or any other small cell

Layer 2 parsing
- GPRSdecode: srlabs.de/gprs

Layer 3 parsing
- Wireshark:

Capture bursts
- NanoBTS or any other small cell

Layer 2 parsing
- GPRSdecode: srlabs.de/gprs

Layer 3 parsing
- Wireshark:

Query current key
- GRX: SGSNContextReq
- Or even over the Internet!
Attack 3: Hijacking data connections

- Get subscriber context
  - GRX: SGSNContextReq

- Spoof SGSN handover
  - GRX: UpdatePDP

Misuse subscriber IP

**Main attack:** Gain access –
- Access Internet for free
- Also access private/corporate APNs (no repeat authentication)

**Gimmick:** Privacy intrusion –
- Original subscriber can still send packets out
- Attacker receives the responses
- Can enumerate apps/services by DNS response
Much more filtering is needed on GRX

<table>
<thead>
<tr>
<th>Attacker position</th>
<th>Necessary filter</th>
<th>Prevelance</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Internet</td>
<td><strong>Never</strong> expose GRX/SS7 on the Internet</td>
<td>Most networks have this filter, but not all</td>
</tr>
<tr>
<td>Over GRX or SS7</td>
<td><strong>Never</strong> talk to non-roaming partners</td>
<td>Some networks distinguish roaming partners, many don’t</td>
</tr>
<tr>
<td></td>
<td>Filter by GT (SS7) or IP (GRX)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Velocity checks: Can a subscriber possibly have moved into the new network?</td>
<td>Hardly anybody does these feasibility checks (yet)</td>
</tr>
</tbody>
</table>
Agenda

- IMSI catcher catching
- GRX attack potential
- GRX exposure

Research outlook
Released today: SnoopSnitch 1.0

Improvements since last beta

- Better IMSI catcher metric
- Lower battery impact
- Autonomous upload option
- Daily measurement option
- Wireshark export

Mobile intrusion detection system
Meant for you to keep a SnoopSnitch phone running at home to spot changes/anomalies
SnoopSnitch provides access to radio traces for further research.

Live export of 2G, 3G, 4G traces.
Immediate research challenge: Capture the Catcher

**Objective.** Find ways to exploit or crash an IMSI catcher

**Setup.** A GSM network “crash_me” is waiting for you to do that

**Tools.** OsmocomBB? rad1o?

**Results.** Please post here: camp.snoopsnitch.com

**Workshop.** Results to be discussed at
- SnoopSnitch data workshop
- Day 3, 17:00, Berlin village
## Takeaways

- Mobile security research involves plenty of trial and error
- Attacks often fail on implementation differences, not actual defenses
- GRX allows for data-enabled IMSI catchers, passive intercept, and connection hijacking; sometimes over the Internet

## Next Events

### Mobile Security

<table>
<thead>
<tr>
<th>Event</th>
<th>Date/Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnoopSnitch data workshop</td>
<td>Day 3, 17:00</td>
<td>Berlin village</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Date/Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture the catcher</td>
<td>All camp long</td>
<td>camp.snoopsnitch.com</td>
</tr>
</tbody>
</table>

### Other SRLabs

<table>
<thead>
<tr>
<th>Event</th>
<th>Date/Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuzzing with AFL</td>
<td>Day 2; 16:00</td>
<td>Hackcenter 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Date/Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometrics hacks</td>
<td>Day 3; 14:30</td>
<td>Hardware Hacking area</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Date/Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware hack playground</td>
<td>All camp long</td>
<td>SRLabs camper</td>
</tr>
</tbody>
</table>

## Questions?

- Karsten Nohl  <nohl@srlabs.de>
- Luca Melette   <luca@srlabs.de>