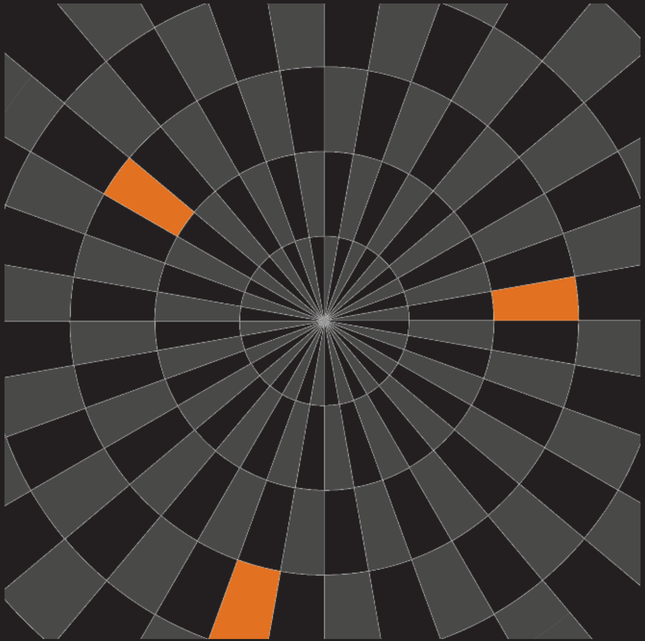
# GSM Hacking

## Wireless Mobile Phone Communication

30th January 2014

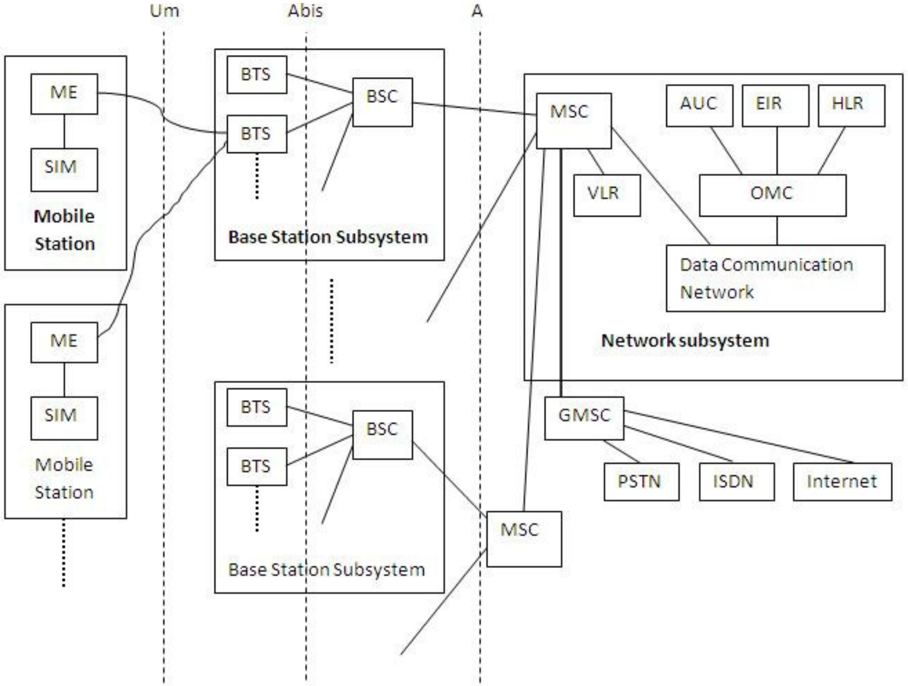


# Introduction to GSM

- June 2008 – **2.9 BILLION** subscribers use GSM.
- Replaced Analogue “Total Access Communication System” in the UK. (TACS)
- GSM is a European Wide Standard started in 1982 by Groupe Spécial Mobile.
- Digital standard with new Security attempting to address losses due to Fraud.
- How vulnerable are GSM communications today?

# GSM Architecture – An Overview

- Mobile Station is your phone.
- BSS provides the air interface between network & phone.
- Network Switching Subsystem (NSS) provides authentication, identity, billing and more.
- The architecture here is a typical GSM environment.



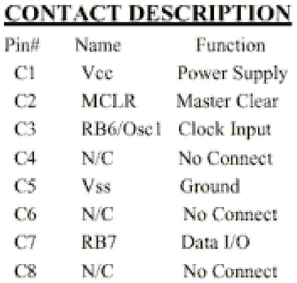
GSM Network Architecture

## What’s in a phone? Mobile Station (MS).

- International mobile station equipment identity (IMEI)
- Contains MS manufacturer & date made.
- SIM card contains subscriber information.
- International mobile subscriber identity (IMSI).
- Mobile Country Code – MCC - 3 digits.
- Mobile Network Code – MNC – 2 digits.
- Mobile Subscriber Identification Number – MSIN – (max 10).
- SIM card also holds encryption keys.
- Your phone contains a baseband processor and RTOS used by GSM.

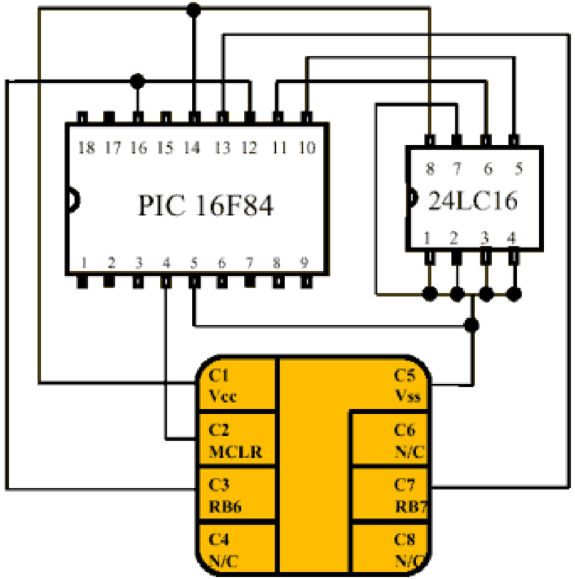
# What is a SIM card?

- Described in GSM 11.14.
- Subscriber Identity Module.
- Stores the IMSI and Ki key.



**CONTACT DESCRIPTION**

| Pin# | Name | Function |
|---|---|---|
| C1 | Vcc | Power Supply |
| C2 | MCLR | Master Clear |
| C3 | RB6/Osc1 | Clock Input |
| C4 | N/C | No Connect |
| C5 | Vss | Ground |
| C6 | N/C | No Connect |
| C7 | RB7 | Data I/O |
| C8 | N/C | No Connect |



- Ki key is needed for network authentication & Air encryption.
- Programmable card can be used which has a writeable Ki key.
- GSM test cards with a writeable Ki key can be bought online.

# ISO7816, SIM Toolkit & weaknesses?

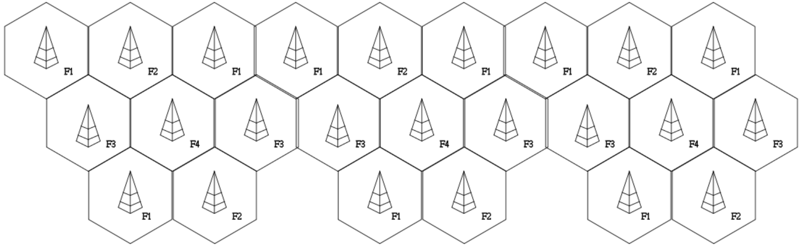
- ISO7816 defines a physical smart card standard.
- SIM Application Toolkit (STK) is implemented by GSM smart cards.
- COMP128v1 is an encryption algorithm found to be flawed.
- A “stop” condition was found that allows Ki to be brute forced.
- COMP128v1 attack takes 12-24 hours and requires physical card.
- COMP128v3 is used more widely today and COMP128v1 is rare.
- Chinese vendors sell cheap COMP128v1 multi-SIM cards & cloner.
- GSM application provides authentication APDU's.
- For more information on SIM attacks THC have a SIM Toolkit Research Group project that contains a lot more information!

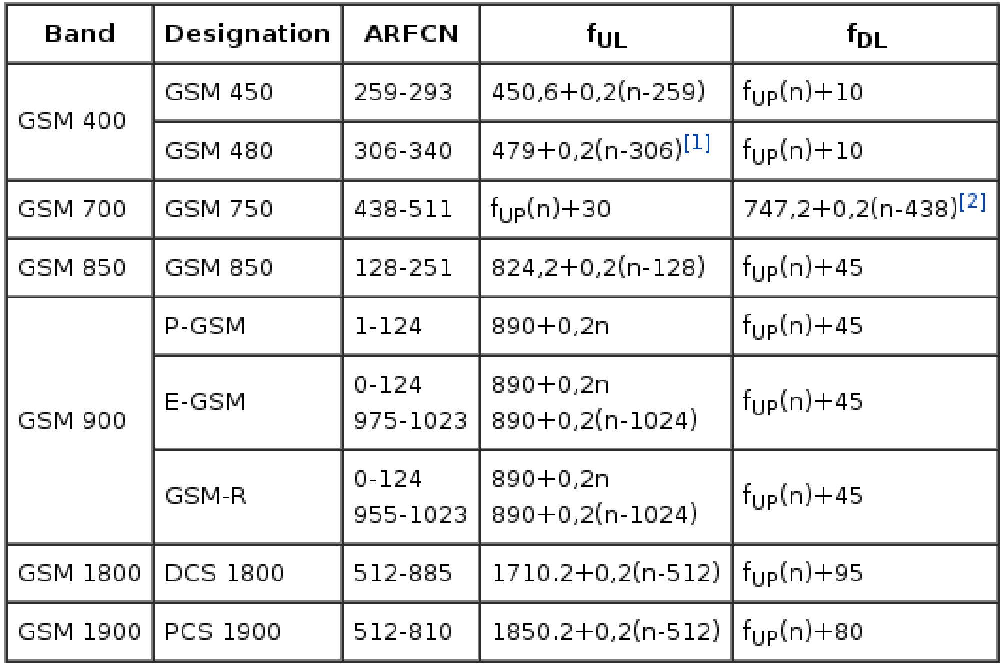
# What's a Base Transceiver System (BTS)?

- Transmitter and receiver equipment, such as antennas and amplifiers.
- Has components for doing digital signal processing (DSP)
- Contains functions for Radio Resource management.
- Provides the air (UM) interface to a MS.
- This is part of a typical "cell tower" that is used by GSM.
- BTS provides the radio signalling between a network and phone.
- Base Station Subsystem (BSS) has additional component Base Station Controller that provides logic & intelligence.

# Radio & Cellular?

- The spectrum is divided into “channels” with uplink and downlink frequencies.
- GSM uses Absolute Radio Frequency Channel Number (ARFCN).
- Cellular Network means channels can be re-used within different spatial areas.
- This is how a small number of frequencies can provide a national network!

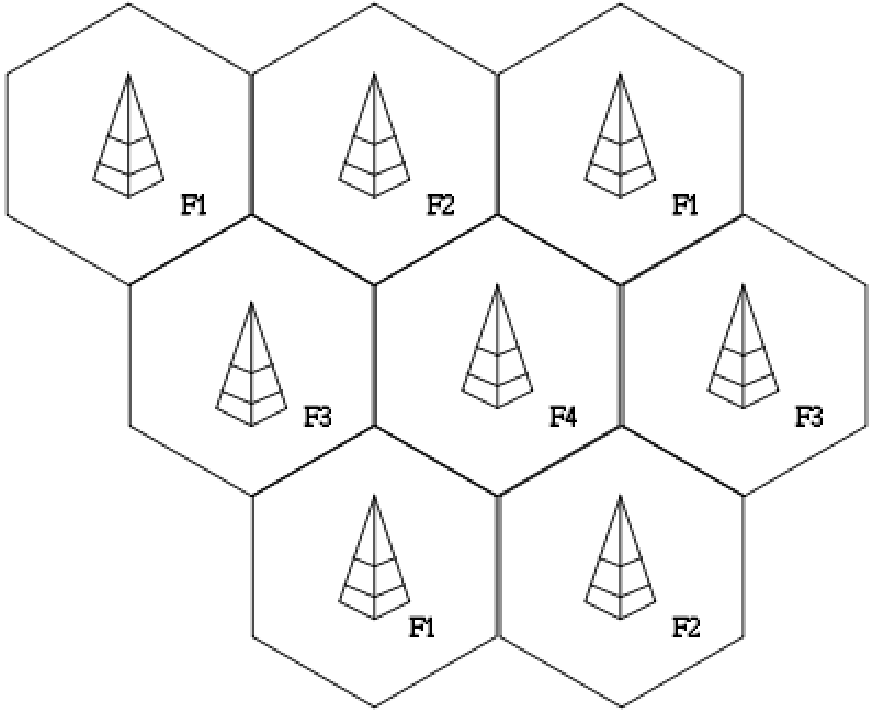




| Band | Designation | ARFCN | $f_{UL}$ | $f_{DL}$ |
|---|---|---|---|---|
| GSM 400 | GSM 450 | 259-293 | 450,6+0,2(n-259) | $f_{UP}$(n)+10 |
| | GSM 480 | 306-340 | 479+0,2(n-306)[1] | $f_{UP}$(n)+10 |
| GSM 700 | GSM 750 | 438-511 | $f_{UP}$(n)+30 | 747,2+0,2(n-438)[2] |
| GSM 850 | GSM 850 | 128-251 | 824,2+0,2(n-128) | $f_{UP}$(n)+45 |
| GSM 900 | P-GSM | 1-124 | 890+0,2n | $f_{UP}$(n)+45 |
| | E-GSM | 0-124<br>975-1023 | 890+0,2n<br>890+0,2(n-1024) | $f_{UP}$(n)+45 |
| | GSM-R | 0-124<br>955-1023 | 890+0,2n<br>890+0,2(n-1024) | $f_{UP}$(n)+45 |
| GSM 1800 | DCS 1800 | 512-885 | 1710.2+0,2(n-512) | $f_{UP}$(n)+95 |
| GSM 1900 | PCS 1900 | 512-810 | 1850.2+0,2(n-512) | $f_{UP}$(n)+80 |

# Radio & Cellular?

- GSM communicates using Time Division Multiple Access / Frequency Division Multiple Access (TDMA/FDMA) principles.
- Space Division Multiple Access gives the cellular concept.
- Traffic is transmitted as “bursts”.
- Radio modulation is using Gaussian Minimum Shift Keying (GMSK).



# Network Switching Subsystem?

- The GSM core network components often not visible to attacker.
- Mobile Switching Centre (MSC).
- Home Locality Registrar (HLR).
- Visitor Locality Registrar (VLR).
- Equipment Identity Registrar (EIR).
- These are components or databases that handle subscribers information, IMSI/encryption keys and perform processes like billing.
- Also where the call switching and routing takes place and connecting to other networks e.g. PSTN.

# GSM Logical Channels

- GSM implements logical channels to allow for signalling between handset and network.
- There is a defined Traffic Channel (TCH) – Full-rate and Half-rate channels are available as TCH/F (Bm), TCH/H (Lm).
- There are Signalling channels (Dm).
- Many exploitable weaknesses in GSM are due to “inband” signalling.
- This same weakness is what allows phreaker “blue boxes” to function and the same classification created “format string attacks.”
- History repeats itself.

# Broadcast Control Channel - BCH

- The BCH is used by a MS to synchronize it’s oscillator and frequency with the BTS.
- The BCH consists of sub-channels that assist with this process.
- Broadcast Control - BCCH
- Frequency Correction - FCCH
- Synchronization - SCH
- The channels are used during the preliminary stages of a MS being powered on and are integral part of “getting a signal”.

# Common Control Channel - CCCH

- The CCCH is used by MS and BTS for communicating requests for resources with network and handset.
- Also has a number of sub-channels responsible for tasks such as indicating that a subscriber is attempting to make a call.
- Random Access Channel - RACH
- Access Grant Channel - AGCH
- Paging Channel - PCH
- Notification Channel - NCH
- Temporary Mobile Subscriber Identity (TMSI) is used to help prevent tracking of a GSM user and can be frequently changed.
- A TMSI access table exists on a BTS with a configurable lifetime.

# Dedicated Control Channels - DCCH

- The DCCH and it’s associated sub-channels perform authentication requests, cipher selection & signalling of call completion.
- Standalone dedicated control - SDCCH
- Slow associated control - SACCH
- Fast associated control – FACCH

- Summary of the three control channels and purpose of each.
- Attacker could exploit GSM signalling weaknesses to access your data. We will look at this in more detail.

# What about Over-the-Air Encryption?

- A number of over-the-air encryption algorithms exist. These are used to encrypt *some* of the GSM logical channels data (such as TCH).
- A5/1 – publicly broken, rainbow tables exist.
- A5/2 – offers no real security.
- A5/3 – KASUMI Cipher, although some man-in-the-middle attacks are known – it has not yet been publicly broken in GSM.
- A3/A8 - used during the authentication process.
- Attacker can attempt to “passively” analyse traffic looking for weak encryption or man-in-the-middle attacks to access data.

## That was a lot of Theory!

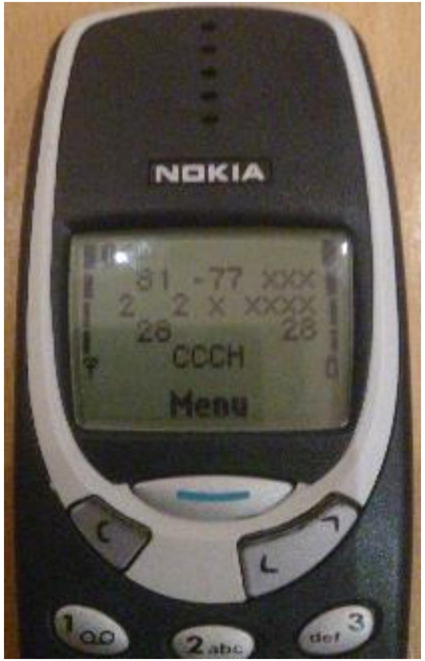
- The GSM standards are thousands of documents.
- There are dozens of great books that can help in your learning.
- Let’s take a look at some of the more practical and interesting parts of GSM.
- If you were an attacker – how do you start attacking?

# Cell Site Diagnostics!

- Nokia Netmonitor
- Dedicated Hardware
- Osmocom-BB
- Make your own!

# Nokia Netmonitor

- Nokia shipped diagnostic tool in early phones.
- Can be enabled on phone such as 3310 using cable.
- Provides a cellular diagnostic tool!
- ARFCN identification!
- Signalling channel display!
- Traffic capture!
- Very cool “feature” of Nokia ;)

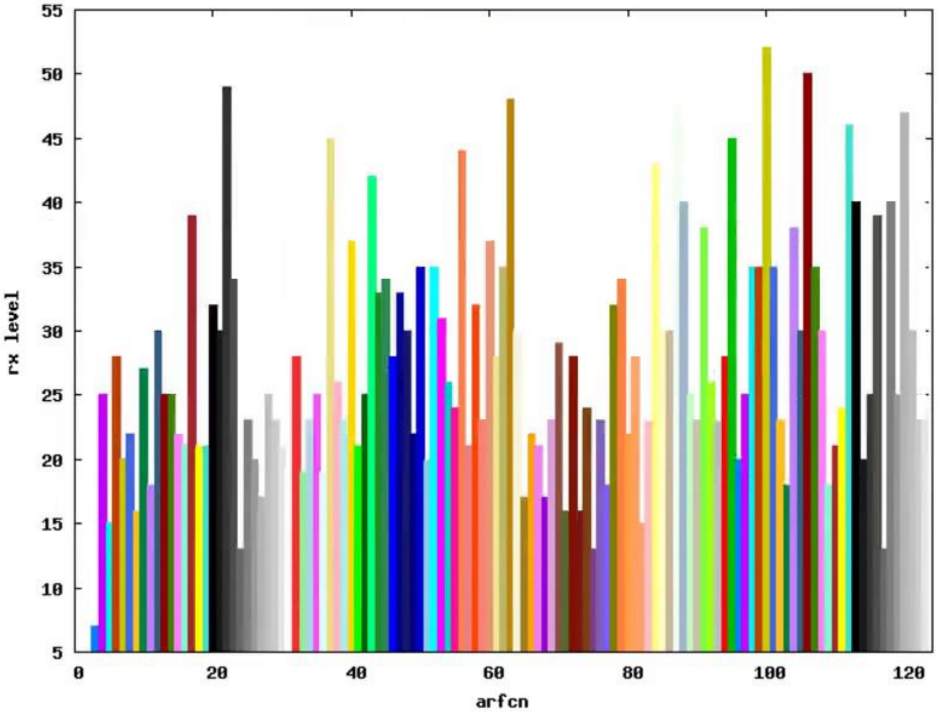


## Dedicated Test Hardware

- eBay is your friend.
- GSM testing hardware prices vary wildly.
- Open-source tools are now more flexible.
- GSM testing hardware is often not very featured.
- The price of dedicated hardware can be very high.

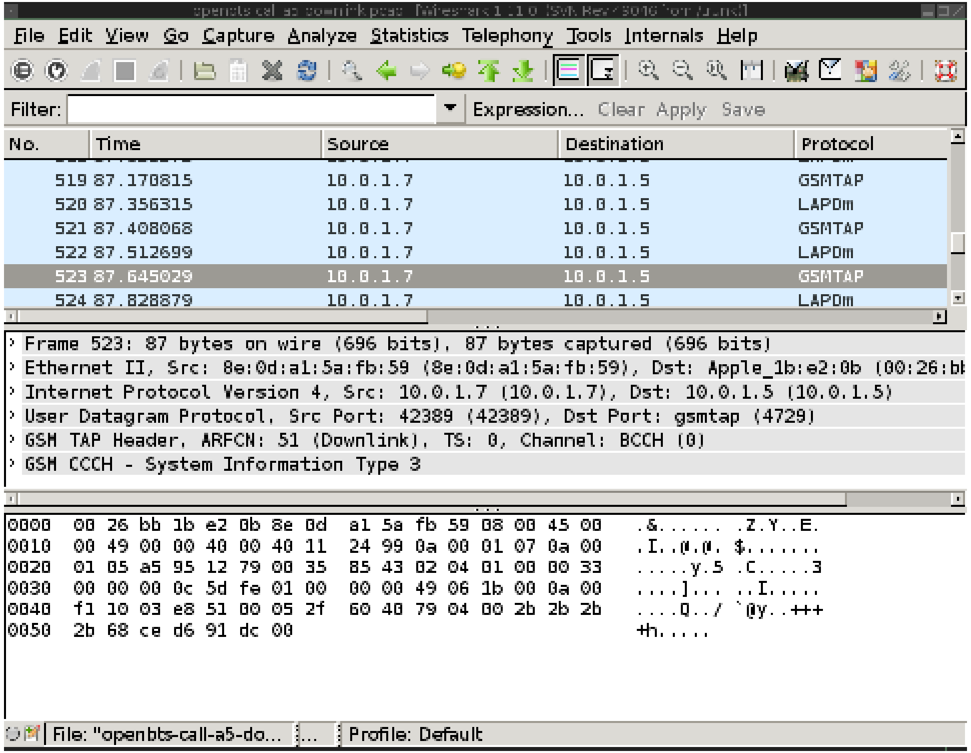
# Osmocom-bb & GNU-Plot – make your own tools!

- Osmocom-bb allows you to write tools for MS baseband.
- Lots of useful diagnostics already available in the public repository.
- You can extend the code to visually represent the GSM spectrum or perform more detailed analysis of a GSM cell tower.
- Requires a <£30 phone to use.



# GSMTAP

- Useful to debug the radio interface.
- GSMTAP encapsulates RF information and transmits it in a UDP encapsulated packet.
- This allows us to “see” the air interface traffic from a BTS or MS.
- Extremely useful capability when analysing GSM.


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

```
No.     Time          Source        Destination   Protocol
  519 87.170815       10.0.1.7      10.0.1.5      GSMTAP
  520 87.356315       10.0.1.7      10.0.1.5      LAPDm
  521 87.408068       10.0.1.7      10.0.1.5      GSMTAP
  522 87.512699       10.0.1.7      10.0.1.5      LAPDm
  523 87.645029       10.0.1.7      10.0.1.5      GSMTAP
  524 87.828879       10.0.1.7      10.0.1.5      LAPDm
```

```
> Frame 523: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
> Ethernet II, Src: 8e:0d:a1:5a:fb:59 (8e:0d:a1:5a:fb:59), Dst: Apple_1b:e2:0b (00:26:bb
> Internet Protocol Version 4, Src: 10.0.1.7 (10.0.1.7), Dst: 10.0.1.5 (10.0.1.5)
> User Datagram Protocol, Src Port: 42389 (42389), Dst Port: gsmtap (4729)
> GSM TAP Header, ARFCN: 51 (Downlink), TS: 0, Channel: BCCH (0)
> GSM CCCH - System Information Type 3
```

```
0000  00 26 bb 1b e2 0b 8e 0d  a1 5a fb 59 08 00 45 00   .&...... .Z.Y..E.
0010  00 49 00 00 40 00 40 11  24 99 0a 00 01 07 0a 00   .I..@.@. $.......
0020  01 05 a5 95 12 79 00 35  85 43 02 04 01 00 00 33   .....y.5 .C.....3
0030  00 00 00 0c 5d fe 01 00  00 00 49 06 1b 00 0a 00   ....]... ..I.....
0040  f1 10 03 e8 51 00 05 2f  60 40 79 04 00 2b 2b 2b   ....Q../ `@y..+++
0050  2b 68 ce d6 91 dc 00                               +h.....
```

File: "openbts-call-a5-do... | ... | Profile: Default

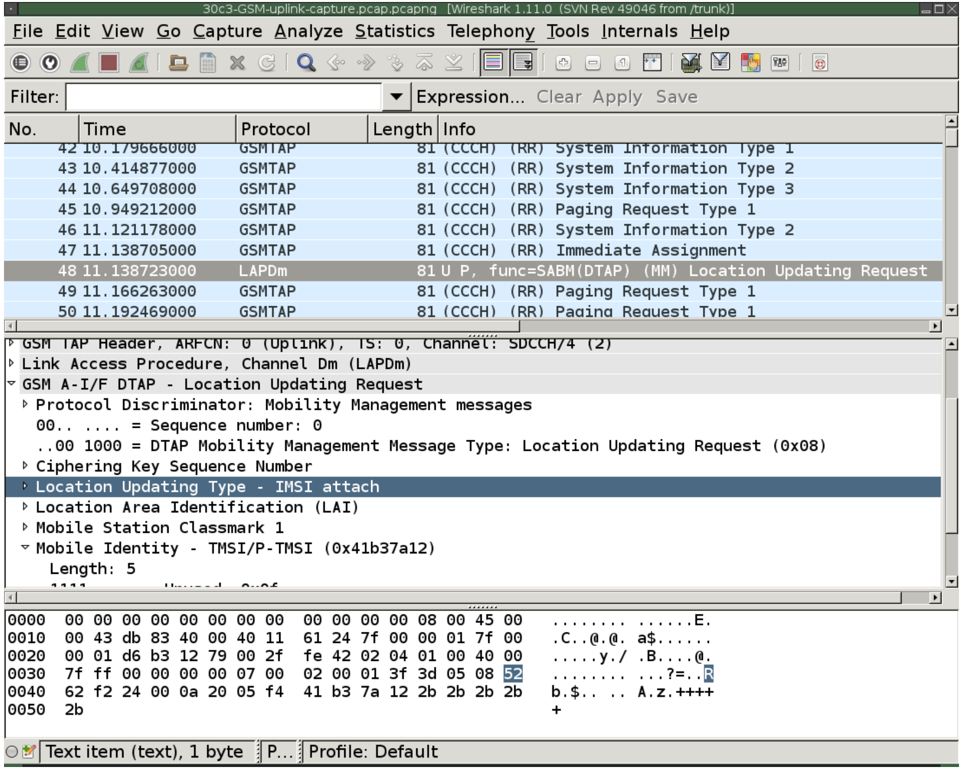
# Mobile Phone – Power-On Process

- MS starts a search for BCCH carriers performing RSSI measurements.
- After identifying the BCCH, the phone probes for presence of FCCH.
- The phone “syncs” and obtains information about the BTS it has identified.
- The phone now knows to monitor “neighbour cells” it has decoded from the transmission.
- This process is what is exploited by IMSI capture devices and fake BTS attack tools.

# IMSI Capture & Detection

- During a Public Land Network Mobile (PLNM) Search(PLNMS) this is trivial. Only performed during MS Power-on & if no service can be found.
- MS has path loss criterion C1 and reselection criterion C2. These are dynamic variables used by the phone to determine if a “neighbour cell” has better radio conditions. These variables are taken dynamically and frequently.
- Manipulating C1 and C2 can force an MS to join our BTS without requiring the phone to perform a PLMNS.
- The network can also request an IMEI during this update location request.

# IMSI Capture – Packet Analysis

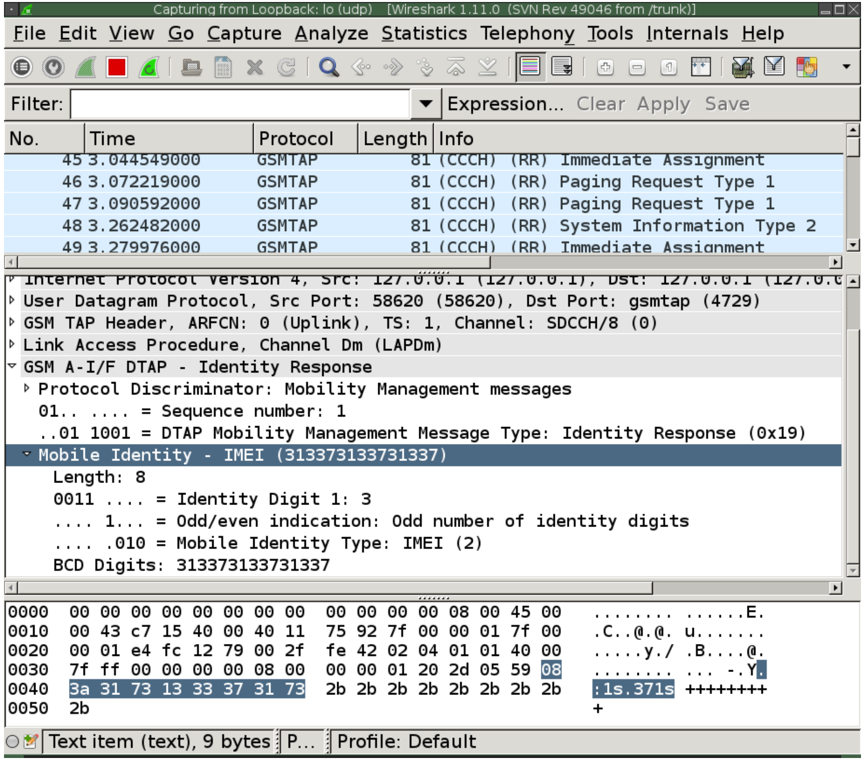

30c3-GSM-uplink-capture.pcap.pcapng [Wireshark 1.11.0 (SVN Rev 49046 from /trunk)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time           Protocol   Length Info
  42 10.179666000    GSMTAP         81 (CCCH) (RR) System Information Type 1
  43 10.414877000    GSMTAP         81 (CCCH) (RR) System Information Type 2
  44 10.649708000    GSMTAP         81 (CCCH) (RR) System Information Type 3
  45 10.949212000    GSMTAP         81 (CCCH) (RR) Paging Request Type 1
  46 11.121178000    GSMTAP         81 (CCCH) (RR) System Information Type 2
  47 11.138705000    GSMTAP         81 (CCCH) (RR) Immediate Assignment
  48 11.138723000    LAPDm          81 U P, func=SABM(DTAP) (MM) Location Updating Request
  49 11.166263000    GSMTAP         81 (CCCH) (RR) Paging Request Type 1
  50 11.192469000    GSMTAP         81 (CCCH) (RR) Paging Request Type 1
```

```
▹ GSM TAP Header, ARFCN: 0 (Uplink), TS: 0, Channel: SDCCH/4 (2)
▹ Link Access Procedure, Channel Dm (LAPDm)
▿ GSM A-I/F DTAP - Location Updating Request
  ▹ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..00 1000 = DTAP Mobility Management Message Type: Location Updating Request (0x08)
  ▹ Ciphering Key Sequence Number
  ▹ Location Updating Type - IMSI attach
  ▹ Location Area Identification (LAI)
  ▹ Mobile Station Classmark 1
  ▿ Mobile Identity - TMSI/P-TMSI (0x41b37a12)
      Length: 5
      1111 .... = Unused: 0x0f
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  00 43 db 83 40 00 40 11  61 24 7f 00 00 01 7f 00   .C..@.@. a$......
0020  00 01 d6 b3 12 79 00 2f  fe 42 02 04 01 00 40 00   .....y./ .B....@.
0030  7f ff 00 00 00 00 07 00  02 00 01 3f 3d 05 08 52   ........ ...?=..R
0040  62 f2 24 00 0a 20 05 f4  41 b3 7a 12 2b 2b 2b 2b   b.$.. .. A.z.++++
0050  2b                                                 +
```

```
Text item (text), 1 byte | P... | Profile: Default
```


Capturing from Loopback: lo (udp) [Wireshark 1.11.0 (SVN Rev 49046 from /trunk)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

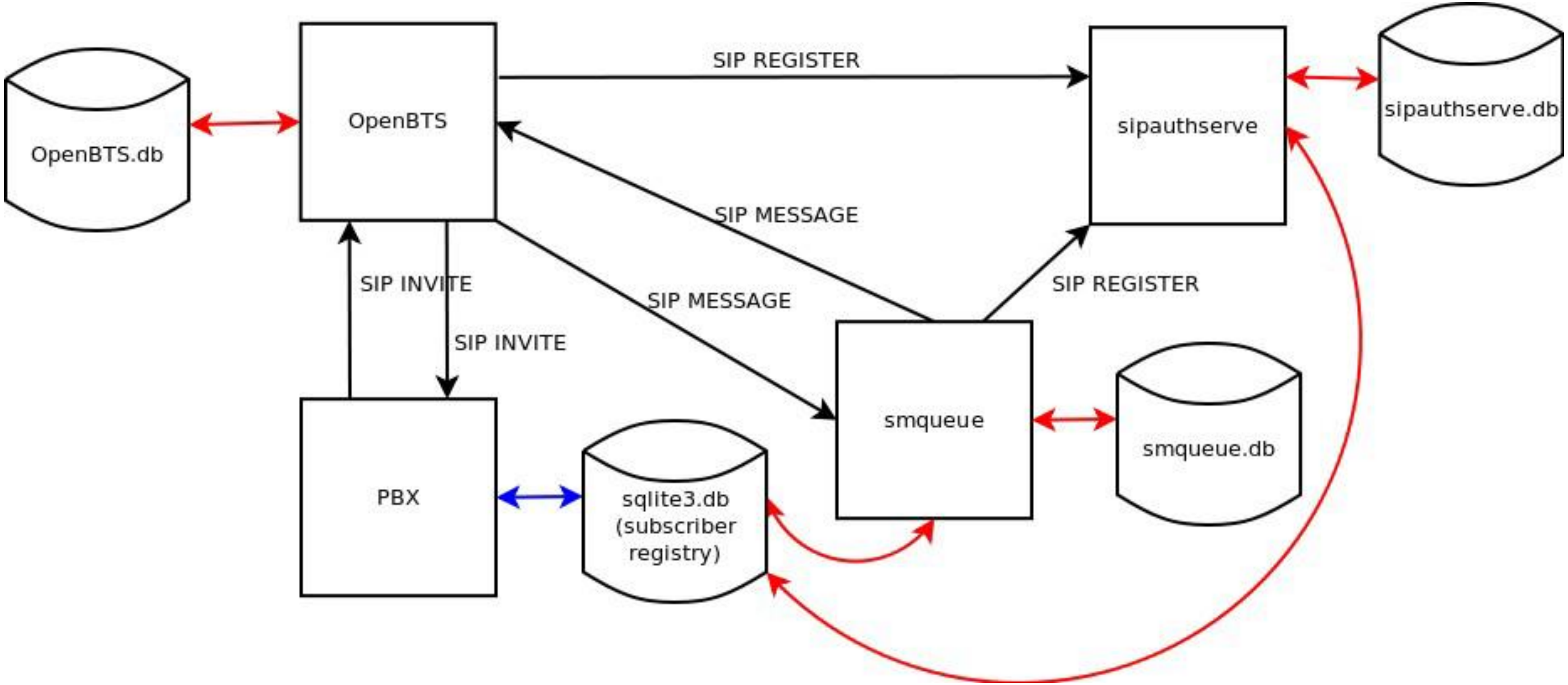
```
No.   Time          Protocol   Length Info
  45 3.044549000    GSMTAP         81 (CCCH) (RR) Immediate Assignment
  46 3.072219000    GSMTAP         81 (CCCH) (RR) Paging Request Type 1
  47 3.090592000    GSMTAP         81 (CCCH) (RR) Paging Request Type 1
  48 3.262482000    GSMTAP         81 (CCCH) (RR) System Information Type 2
  49 3.279976000    GSMTAP         81 (CCCH) (RR) Immediate Assignment
```

```
▹ Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0
▹ User Datagram Protocol, Src Port: 58620 (58620), Dst Port: gsmtap (4729)
▹ GSM TAP Header, ARFCN: 0 (Uplink), TS: 1, Channel: SDCCH/8 (0)
▹ Link Access Procedure, Channel Dm (LAPDm)
▿ GSM A-I/F DTAP - Identity Response
  ▹ Protocol Discriminator: Mobility Management messages
    01.. .... = Sequence number: 1
    ..01 1001 = DTAP Mobility Management Message Type: Identity Response (0x19)
  ▿ Mobile Identity - IMEI (313373133731337)
      Length: 8
      0011 .... = Identity Digit 1: 3
      .... 1... = Odd/even indication: Odd number of identity digits
      .... .010 = Mobile Identity Type: IMEI (2)
      BCD Digits: 313373133731337
```

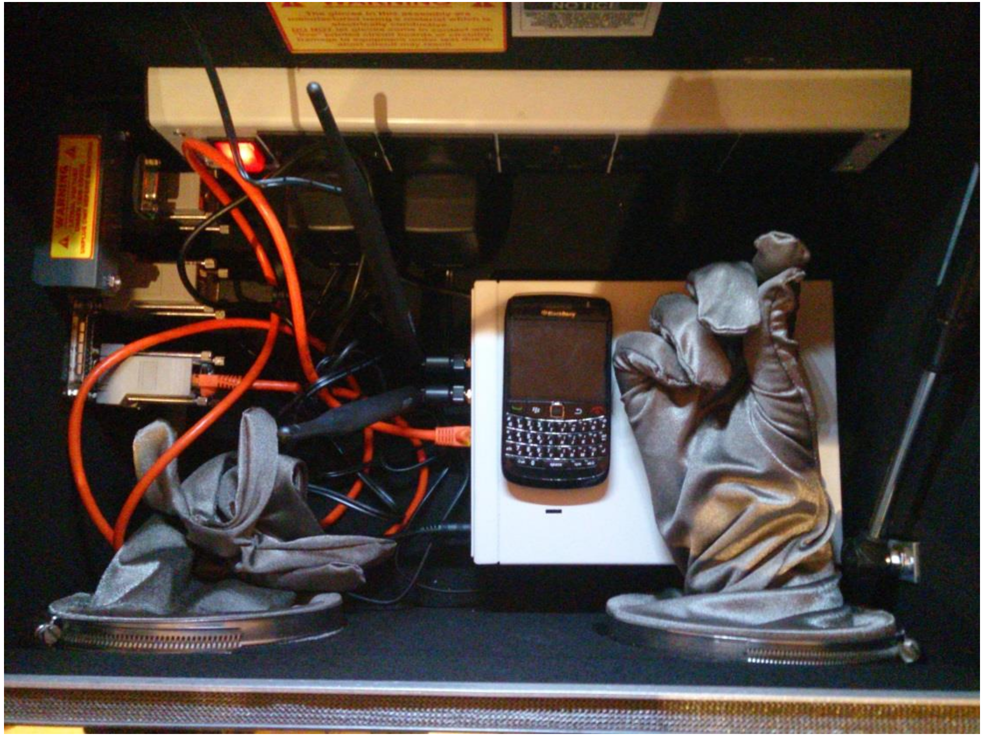
```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  00 43 c7 15 40 00 40 11  75 92 7f 00 00 01 7f 00   .C..@.@. u.......
0020  00 01 e4 fc 12 79 00 2f  fe 42 02 04 01 01 40 00   .....y./ .B....@.
0030  7f ff 00 00 00 00 08 00  00 00 01 20 2d 05 59 08   ........ ... -.Y.
0040  3a 31 73 13 33 37 31 73  2b 2b 2b 2b 2b 2b 2b 2b   :1s.371s ++++++++
0050  2b                                                 +
```

```
Text item (text), 9 bytes | P... | Profile: Default
```

# OpenBTS - Architecture

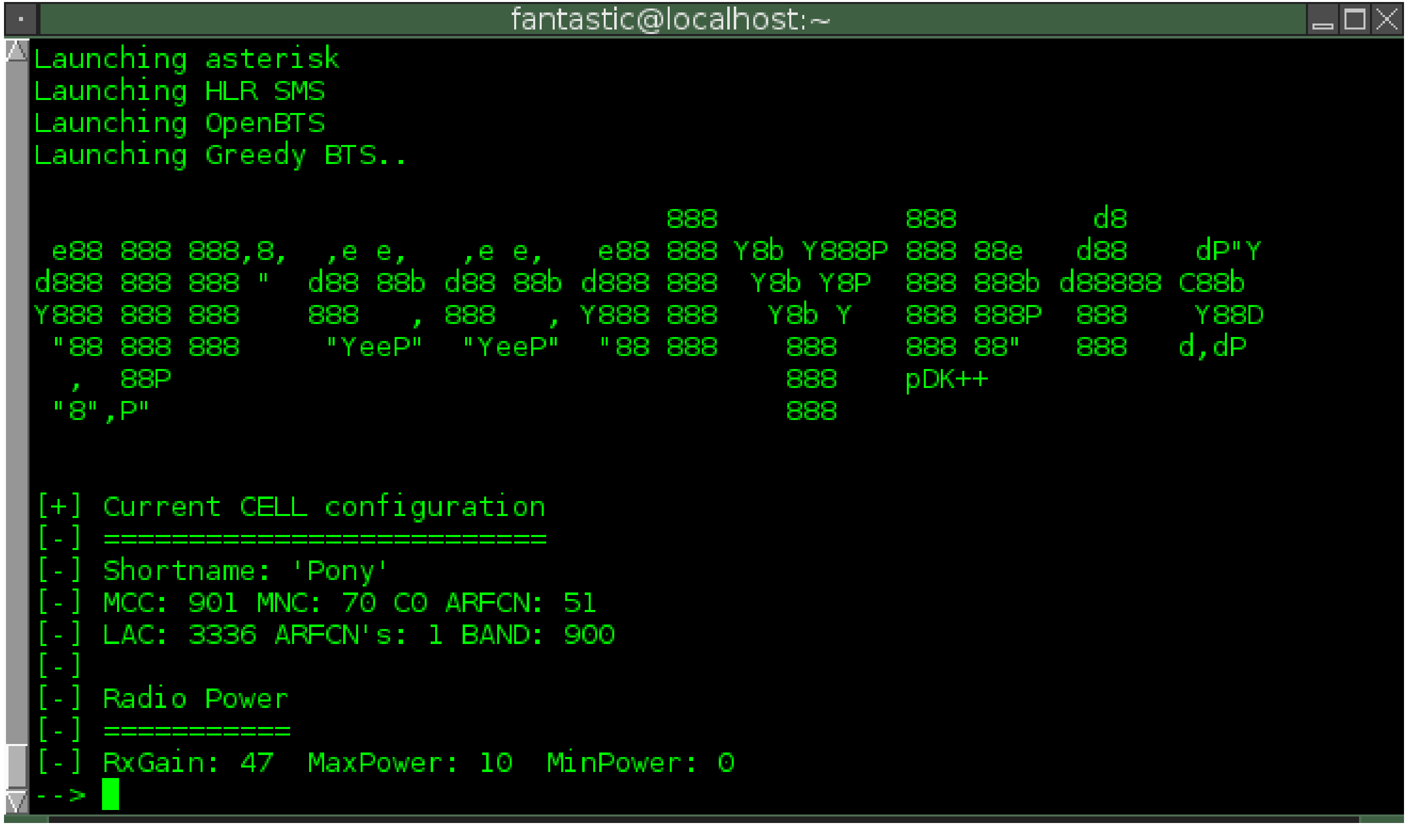


# RF shielding - (R&D at MWR)



# GreedyBTSv3.img - USRP E100 firmware image.

- OpenBTS w/Real-Time Asterisk configured to run on a USRP E100.
- I modified and built several packages from source to improve support for the E100 platform.
- Minor patches to OpenBTS to remove unwanted features such as message alerting.
- A console interface script is provided to simplify the process of attacking an MS from a BTS by watching syslog and creating SQLite entries.
- Any captured phone call & SMS are “autorecorded” to E100.
- If internet is available to the E100, GPRS and data is auto configured. Packet analysis tools (libpcap/tcpdump) and netfilter support are also compiled into the image.
- Fully embedded solution requires only an E100 and network connection.



```
Launching asterisk
Launching HLR SMS
Launching OpenBTS
Launching Greedy BTS..

                                     888           888        d8
 e88 888 888,8,  ,e e,   ,e e,   e88 888 Y8b Y888P 888 88e   d88    dP"Y
d888 888 888 "  d88 88b d88 88b d888 888  Y8b Y8P  888 888b d88888 C88b
Y888 888 888    888   , 888   , Y888 888   Y8b Y   888 888P  888    Y88D
 "88 888 888     "YeeP"  "YeeP"  "88 888    888    888 88"   888   d,dP
  ,  88P                                    888    pDK++
 "8",P"                                     888


[+] Current CELL configuration
[-] ==========================
[-] Shortname: 'Pony'
[-] MCC: 901 MNC: 70 C0 ARFCN: 51
[-] LAC: 3336 ARFCN's: 1 BAND: 900
[-]
[-] Radio Power
[-] ===========
[-] RxGain: 47  MaxPower: 10  MinPower: 0
-->
```

# Greedy BTS – Live Demo.

# MS -> BTS Active Attacks

- Osmocom-bb allows for full control of the baseband!
- Attacker can attempt MS -> BTS injection attacks.
- Osmocom-bb provides a full-featured console mobile phone app!
- You can perform uplink sniffing as well as injection of traffic.
- A very flexible tool that can be repurposed for attack and analysis.

# RACH & TMSI Paging Attacks

- Random Access requests have a finite resource.
- Attacker can continually request resources via RACH preventing users being able to place new calls once all available resources are consumed.
- TMSI is vulnerable to a race condition when the BTS is paging, attacker can answer all pages preventing legitimate communication.
- An attacker responds to pages made by the BTS to identify a particular phone causing the original request to be unanswered.
- Both attacks can be implemented in osmocom-bb.
- Both attacks could be used to perform a “DoS” of a BTS.

# Passive & Sniffing Attacks

- GNU/Radio is used to capture the RF of a GSM ARFCN.
- GSM receiver and toolkit exists for doing capture of GSM bursts & decoding of the data.
- Software Defined Radio is drastically reducing in price point.
- £20< RTLSDR dongles can be used to capture GSM traffic.
- Purely passive analysis allows for identification of call requests. TCH channel uses encryption.
- Kraken tool can decrypt A5/1, requires 1.6TB rainbow tables.
- A5/2 is very weak encryption & rarely enabled.

# Conclusion

- Information sent over your mobile phone may not be as secure as you think.
- Detection of GSM attacks is still in it's infancy, some tools are beginning to surface which detect greedy-BTS but they will require "active" use.
- If you are transmitting sensitive information such as usernames or passwords consider using a non-wireless technology.
- 2G GSM technology has a number of weaknesses that means the technology cannot be trusted for sensitive data.

# Questions

Thank you for all the hard work done by members of the open-source and security research communities in making GSM more accessible for analysis.