



GreedyBTS – Hacking Adventures in GSM



- Who am I?
- Technical overview of 2.5G environments
- Cellular environment diagnostics and tools
- Security vulnerabilities in GSM
- Creating an open-source 2.5G simulation environment for analysis.
- Implementations of GSM attacks
- Demo

# 2.5G Technical Overview

## Introduction to GSM



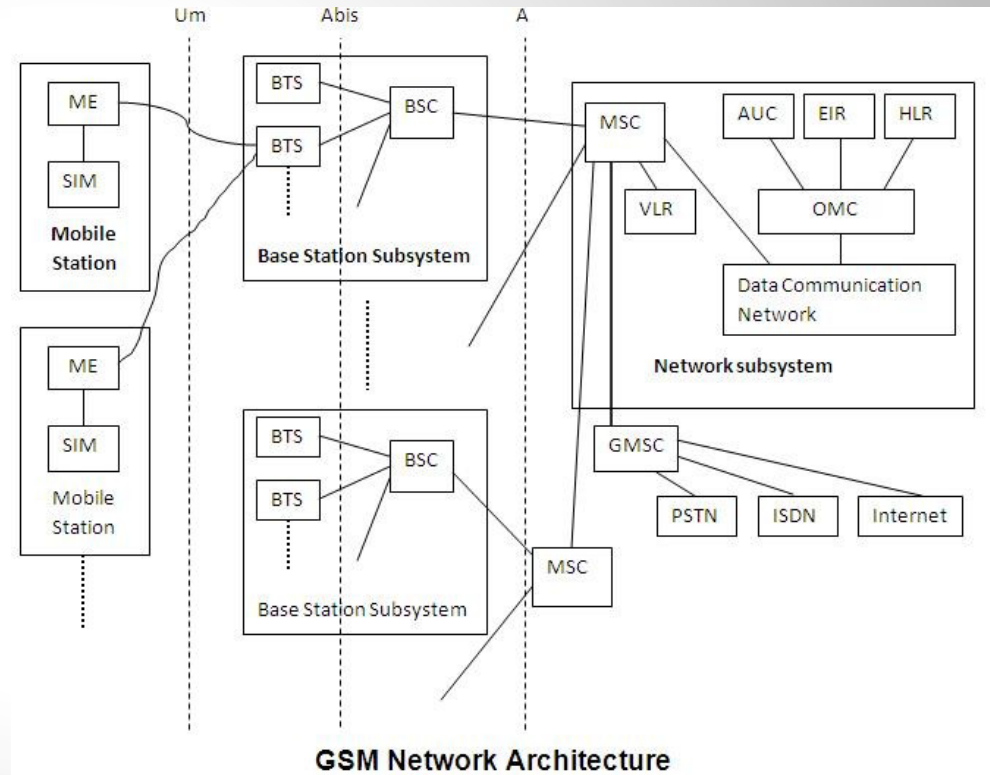
- June 2008 – **2.9 BILLION** subscribers use GSM.
- Replaced Analogue “Total Access Communication System” in the UK. (TACS)
- GSM is a European Wide Standard started in 1982 by Groupe Spécial Mobile.
- Digital standard with new Security attempting to address losses due to Fraud.
- GPRS created to work with GSM and address data needs, 2.5G.
- UMTS and LTE, 3<sup>rd</sup> and 4<sup>th</sup> generation networks have arrived – 2.5G still here.
- How vulnerable are 2.5G networks & GSM communications today?

# 2.5G Technical Overview

## GSM Architecture



- Mobile Station is your phone.
- BSS provides the air interface between network & phone.
- Network Switching subsystem provides authentication, identity, billing and more.
- The architecture shown is a typical 2G GSM environment.



# 2.5G Technical Overview

## Mobile Station (MS).



- International mobile station equipment identity (IMEI)
- Contains uniquely identifiable information on device.
  
- 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.

# 2.5G Technical Overview

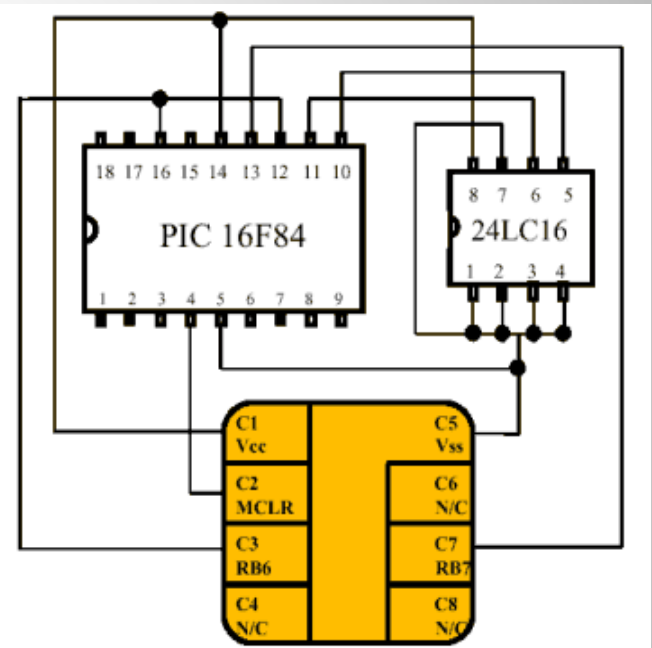
## What is a SIM card?



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

### 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



# 2.5G Technical Overview

## ISO7816 & SIM Toolkit



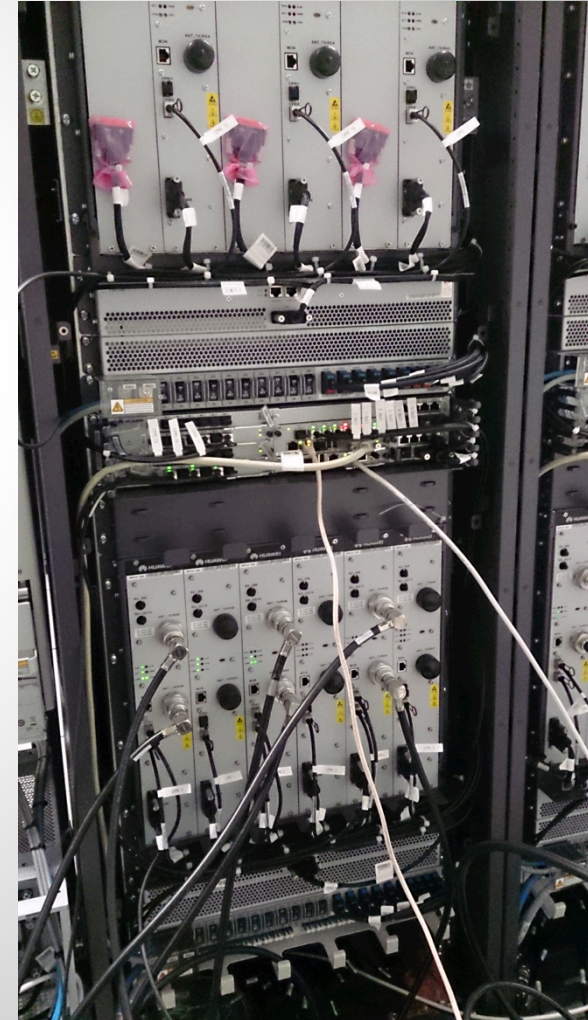
- ISO7816 defines a physical smart card standard.
- SIM Application Toolkit (STK) is implemented by GSM smart cards.
- GSM application provides authentication APDU's.
  
- COMP128v1 is an encryption algorithm that was found to be flawed.
- A “stop” condition was found that allows Ki to be brute forced.
- 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.
  
- SIM Trace <http://bb.osmocom.org/trac/wiki/SIMtrace>
- For more information on SIM attacks THC have a SIM Toolkit Research Group project that contains a lot more information!

# 2.5G Technical Overview

## 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.



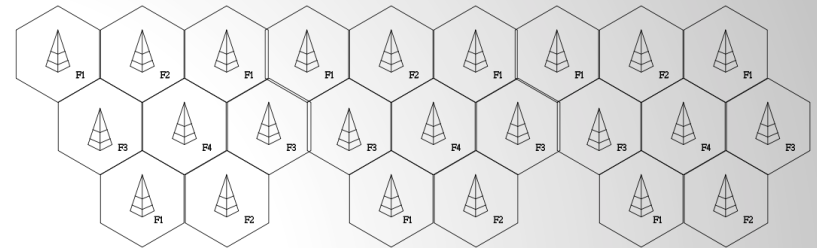


# 2.5G Technical Overview

## Radio & Cellular?



- The spectrum is divided into uplink/downlink “channels”.
- 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!



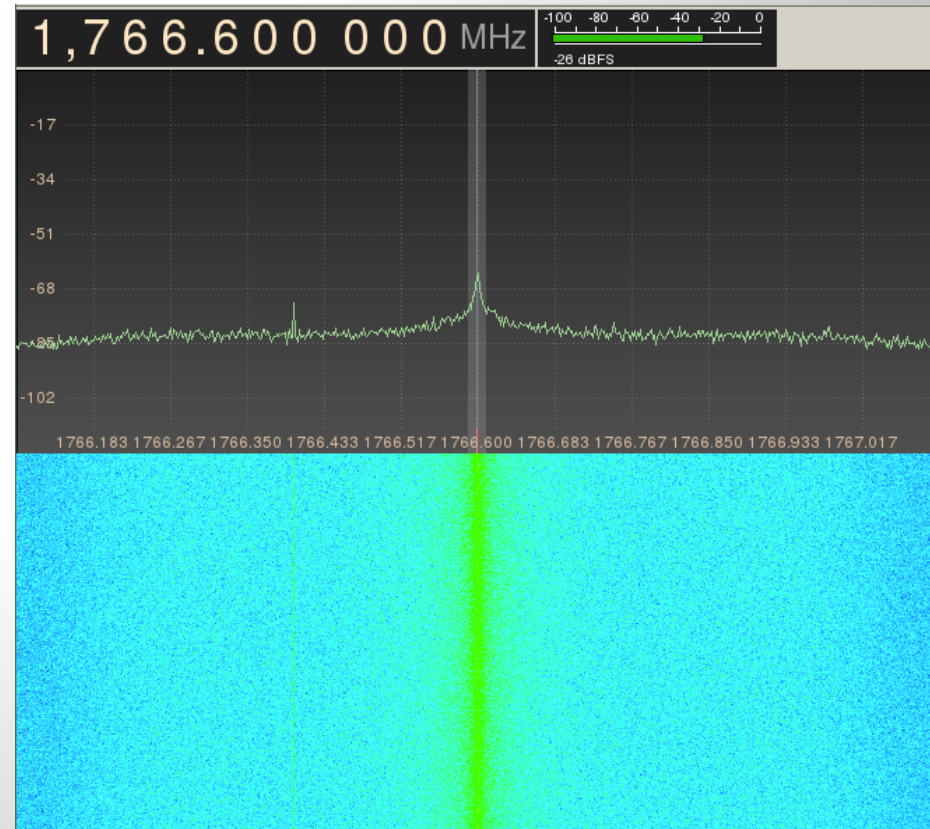
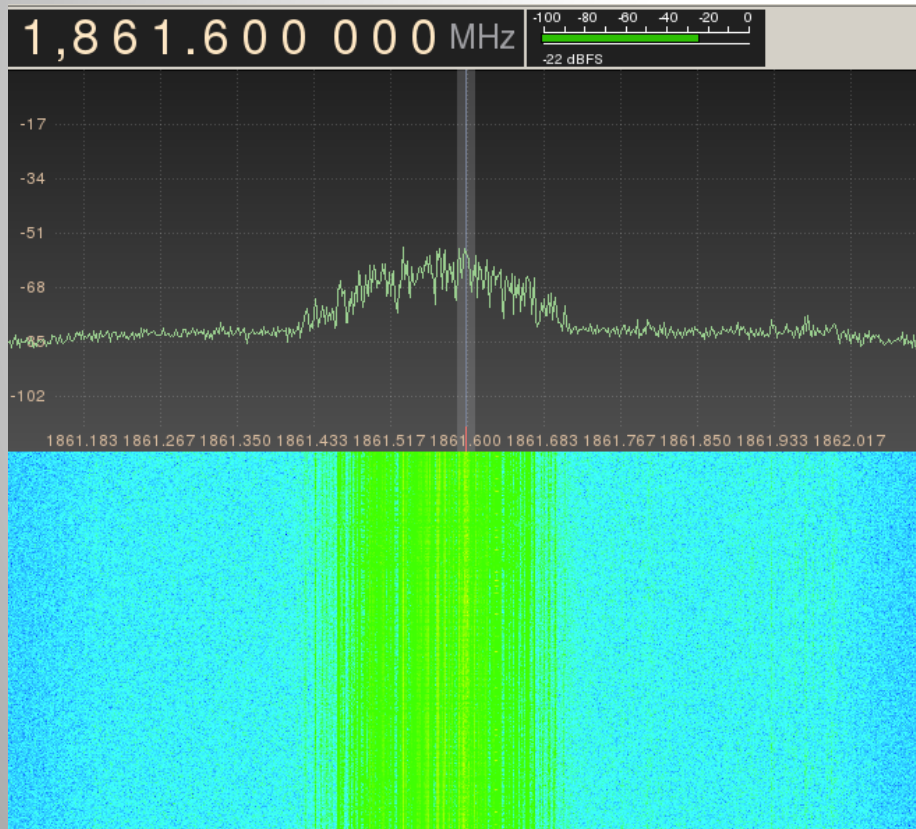
Band	Designation	ARFCN	$f_{UL}$	$f_{DL}$
GSM 400	GSM 450	259-293	$450,6+0,2(n-259)$	$f_{UP}(n)+10$
	GSM 480	306-340	$479+0,2(n-306)$ <sup>[1]</sup>	$f_{UP}(n)+10$
GSM 700	GSM 750	438-511	$f_{UP}(n)+30$	$747,2+0,2(n-438)$ <sup>[2]</sup>
GSM 850	GSM 850	128-251	$824,2+0,2(n-128)$	$f_{UP}(n)+45$
GSM 900	P-GSM	1-124	$890+0,2n$	$f_{UP}(n)+45$
	E-GSM	0-124	$890+0,2n$	$f_{UP}(n)+45$
		975-1023	$890+0,2(n-1024)$	
GSM-R	0-124 955-1023	$890+0,2n$ $890+0,2(n-1024)$	$f_{UP}(n)+45$	
GSM 1800	DCS 1800	512-885	$1710,2+0,2(n-512)$	$f_{UP}(n)+95$
GSM 1900	PCS 1900	512-810	$1850,2+0,2(n-512)$	$f_{UP}(n)+80$

# 2.5G Technical Overview

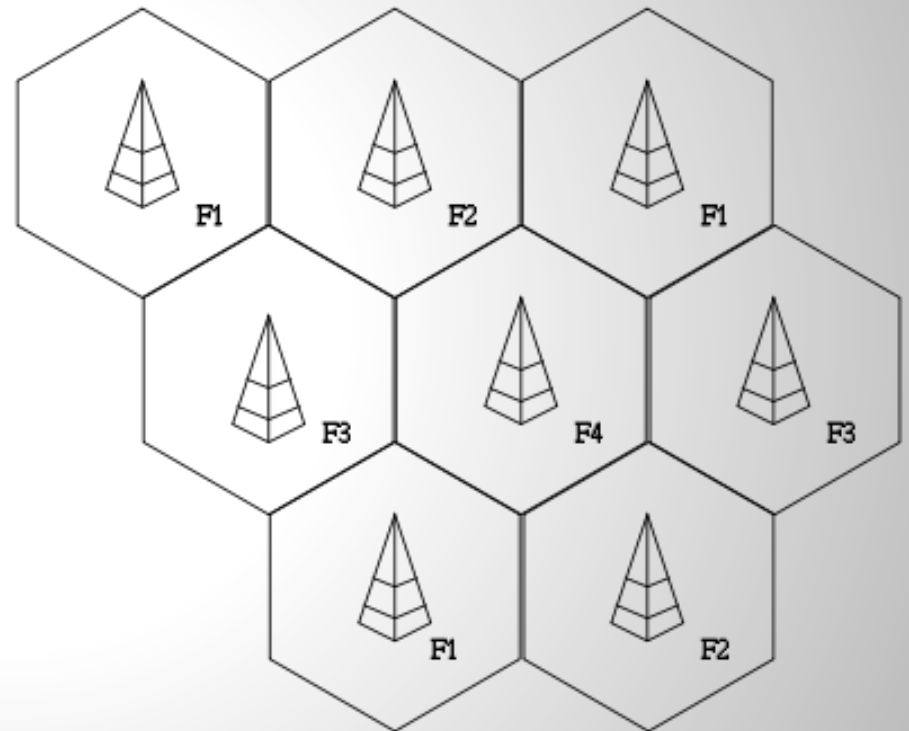
## Physical Interface



- Waterfall views of GSM ARFCN downlink (left) and uplink (right).
- ARFCN is 200kHz channel and this is divided into TDMA slots.
- Five different types of “bursts” are modulated within.



- GSM communicates using Time Division Multiple Access / Frequency Division Multiple Access (TDMA/FDMA) principles.
- Space Division Multiple Access gives the cellular concept.
- Traffic transmitted as “bursts”.
- Radio modulation is using Gaussian Minimum Shift Keying (GMSK).
- GMSK is variant of frequency shift keying (FSK) designed to reduce bandwidth, minimum shift keying (MSK) with further Gaussian bandpass (GMSK).



# 2.5G Technical Overview

## Network Switching Subsystem



- The GSM core network components usually 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.

# 2.5G Technical Overview

## 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 “in-band” signalling.
- This same class of vulnerability is what allows phreaker “blue boxes” to function and responsible for “format string attacks.” – where management capability is accessible it has potential for subverting.

# 2.5G Technical Overview

## Broadcast 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”.

# 2.5G Technical Overview

## Common Control Channel - CCCH



- The CCCH is used by MS and BTS for communicating requests for resources with network and handset such as when a call attempt is placed.
- 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, can be frequently changed and has a lifetime limit.

# 2.5G Technical Overview

## Dedicated Control Channels - DCCH



- The DCCH and its 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 subscriber mobile usage. We will look at this in more detail.



## 2.5G Technical Overview

### What about Over-the-Air Encryption?



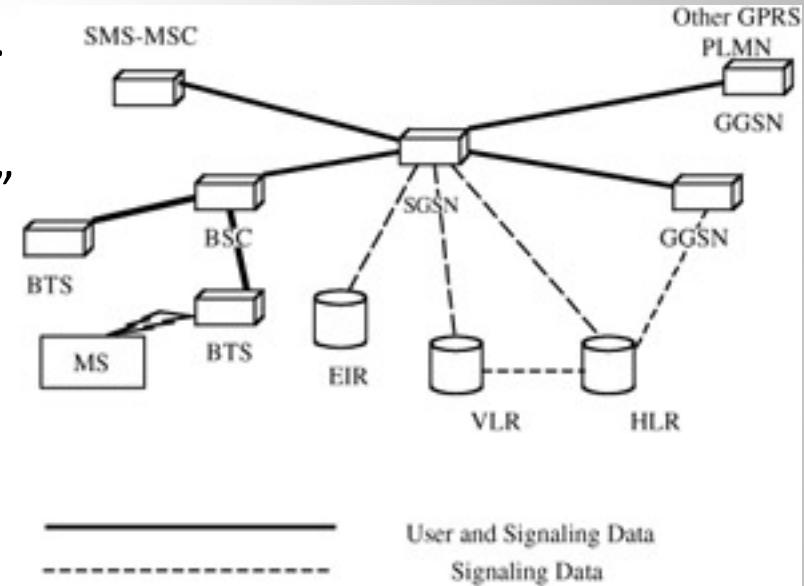
- Several over-the-air (OTA) encryption algorithms exist. These are used to encrypt \*some\* of the GSM logical channels data (such as TCH).
- A5/1 – publicly broken, rainbow tables exist.
- A5/2 – offers no real security.
- A5/3 – KASUMI Cipher, although some man-in-the-middle attacks are known – it 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 perform man-in-the-middle attacks against subscriber MS and BTS.

# 2.5G Technical Overview

## General Packet Radio Service



- Uses existing GSM concepts, e.g. timeslots.
- Introduces “Subscriber GPRS Service Node” (SGSN) and “Gateway GPRS Service Node” (GGSN).
- Adds Packet Control Unit to BSS.
- Data is sent in PCU frames.
- Introduces a new Radio Resource (RR) protocol.
- Radio Link Control (RLC) / Media Access Control (MAC)

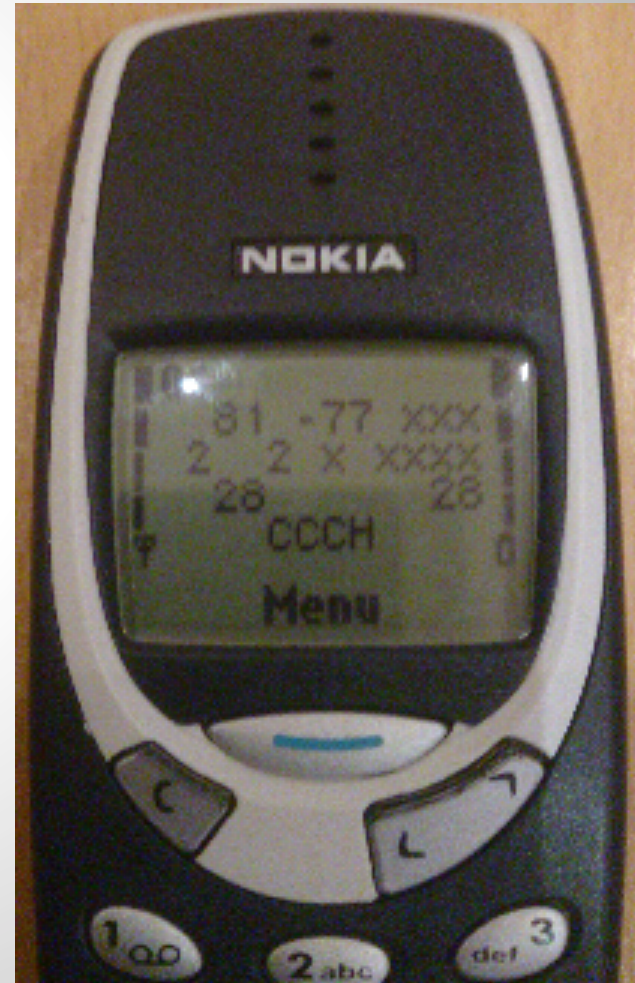


# Cell Diagnostics & Tools

## 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!
- Uplink Traffic capture!
- Very cool “feature” of Nokia ;)



# Cell Diagnostics & Tools

## 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.
- Vendors often not forthcoming with help.

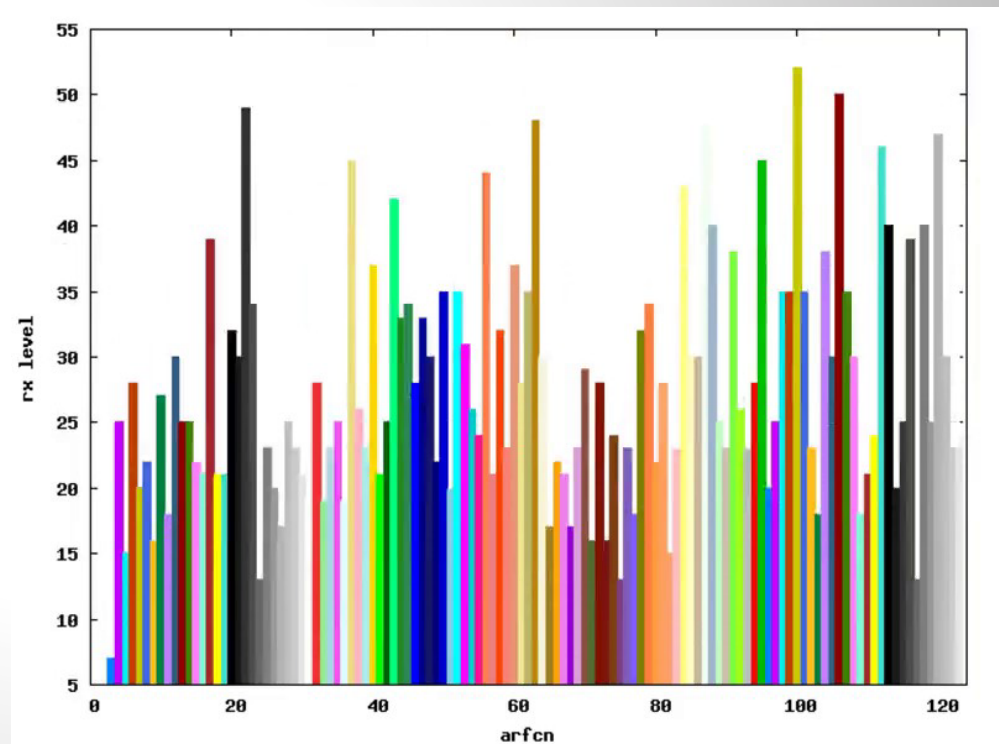


# Cell Diagnostics & Tools

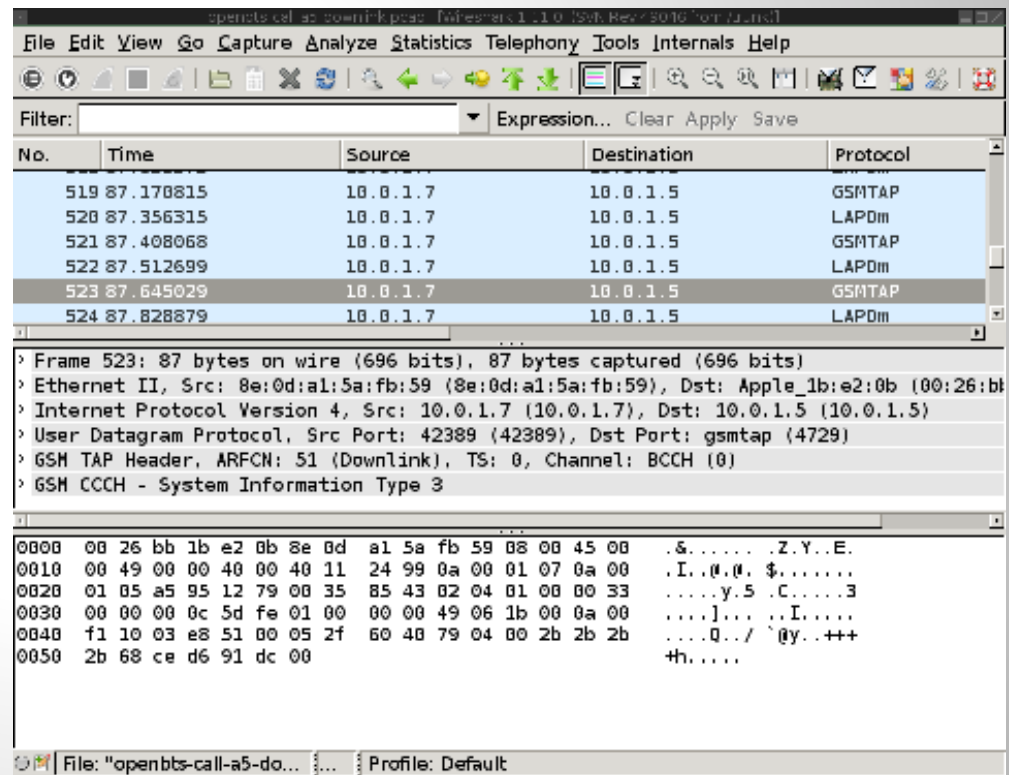
## Osmocom-bb & GNU/Plot



- 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.



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



The image shows a Wireshark network traffic capture window. The main pane displays a list of captured packets with the following columns: No., Time, Source, Destination, and Protocol. The packets are as follows:

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

The packet details pane for frame 523 shows the following structure:

- 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:bd:00:00:00)
- 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

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
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..0.0.$.....
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                               th.....
```

# Cell Diagnostics & Tools

## AirProbe & Sniffing



- 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.
- £20< RTLSDR dongles can be used to capture GSM traffic.
- Purely passive analysis allows for identification of call requests. TCH channel should use encryption.
- Kraken tool can decrypt A5/1 on TCH, requires 1.6TB rainbow tables.
- Wireshark can parse the GSMTAP output and sniff the air interface.

- 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.



- 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.

	AA	BB	BB	BB	CC	CC	CC	D or EE
IMEI	TAC			TAC (FAC)	Serial			(Luhn Checksum)
IMEI	013035			00	561434			0

- IMEI contains Type Allocation Code (TAC), serial number and checksum.
- TAC starts with two digit Reporting Body Identifier (RBI), determines country.
- Remaining six digits of TAC identify vendor who produced the device.
- RBI: 01 Org: PTCRB Country: United States
- TAC: 01303500 Manufacturer: Apple Model: iPhone 4S model MD239B/A

# GSM Security

## Location Update Request



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  
 ....

```

0000 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 (127.0.0.1)  
 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 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

- Attacker needs to simulate condition to entice MS to fake BTS.
- Locates the MCC / MNC of target phone provider or roaming agreement.
- Identifies the Neighbor ARFCN for target MS by performing PLMN locally.
- Creates a BTS using the MCC, MNC, ARFCN, LAC and any other parameters to match a weak signal ARFCN BTS to reduce interference.
- This will create an environment where target in close physical proximity to the BTS will trigger cell re-selection as MS sees a better RF environment.
- Cell diagnostics tools need to be used to obtain this data for attacker to use.

- Osmocom-BB is very versatile, GNU/Radio or gsm-receiver tool could also be used. Osmocom-BB mobile includes “monitor” command that provides RSSI monitoring of current and Neighbor ARFCN.

```
fantastic@localhost:~  
% MON: f=112 lev=-63 snr= 0 ber= 11 LAI=234 10 472b ID=8cb6  
% MON: f=112 lev=-63 snr= 0 ber= 7 LAI=234 10 472b ID=8cb6  
% MON: f=112 lev=-61 snr= 0 ber= 6 LAI=234 10 472b ID=8cb6  
% MON: cell ARFCN LAC C1 C2 CRH RLA_C bargraph  
% MON: serving 112 0x472b 43 43 -62 =====  
% MON: nb 1 105 0x472b 34 34 0 -71 =====  
% MON: nb 2 121 0x472b 18 18 0 -87 =====  
% MON: nb 3 1000 -92 =====  
% MON: nb 4 120 0x472b 11 11 0 -94 =====  
% MON: nb 5 106 -95 =====  
% MON: nb 6 114 0x472b 10 10 0 -95 =====  
% MON: f=112 lev=-61 snr= 0 ber= 7 LAI=234 10 472b ID=8cb6  
% MON: f=112 lev=-61 snr= 0 ber= 3 LAI=234 10 472b ID=8cb6  
% MON: f=112 lev=-61 snr= 0 ber= 10 LAI=234 10 472b ID=8cb6  
% MON: cell ARFCN LAC C1 C2 CRH RLA_C bargraph  
% MON: serving 112 0x472b 45 45 -60 =====  
% MON: nb 1 105 0x472b 34 34 0 -71 =====  
% MON: nb 2 121 0x472b 17 17 0 -88 =====  
% MON: nb 3 1000 -93 =====  
% MON: nb 4 120 0x472b 12 12 0 -93 =====  
% MON: nb 5 106 -95 =====  
% MON: nb 6 114 0x472b 10 10 0 -95 =====  
% MON: f=112 lev=-62 snr= 0 ber= 6 LAI=234 10 472b ID=8cb6
```

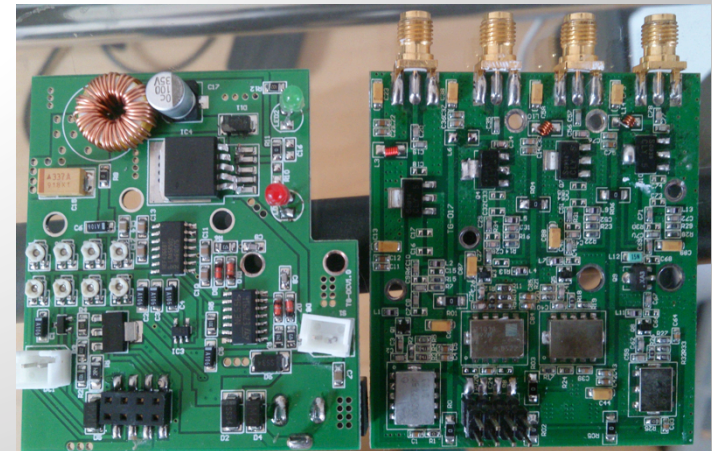
- Random Access requests have a finite resource.
- Attacker can continually request resources via RACH preventing users being able to place new calls once all available resources are consumed.
- TMSI is vulnerable to a race condition when the BTS is paging, attacker can answer all pages preventing legitimate 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.

# GSM Security

## Downgrade & Jamming

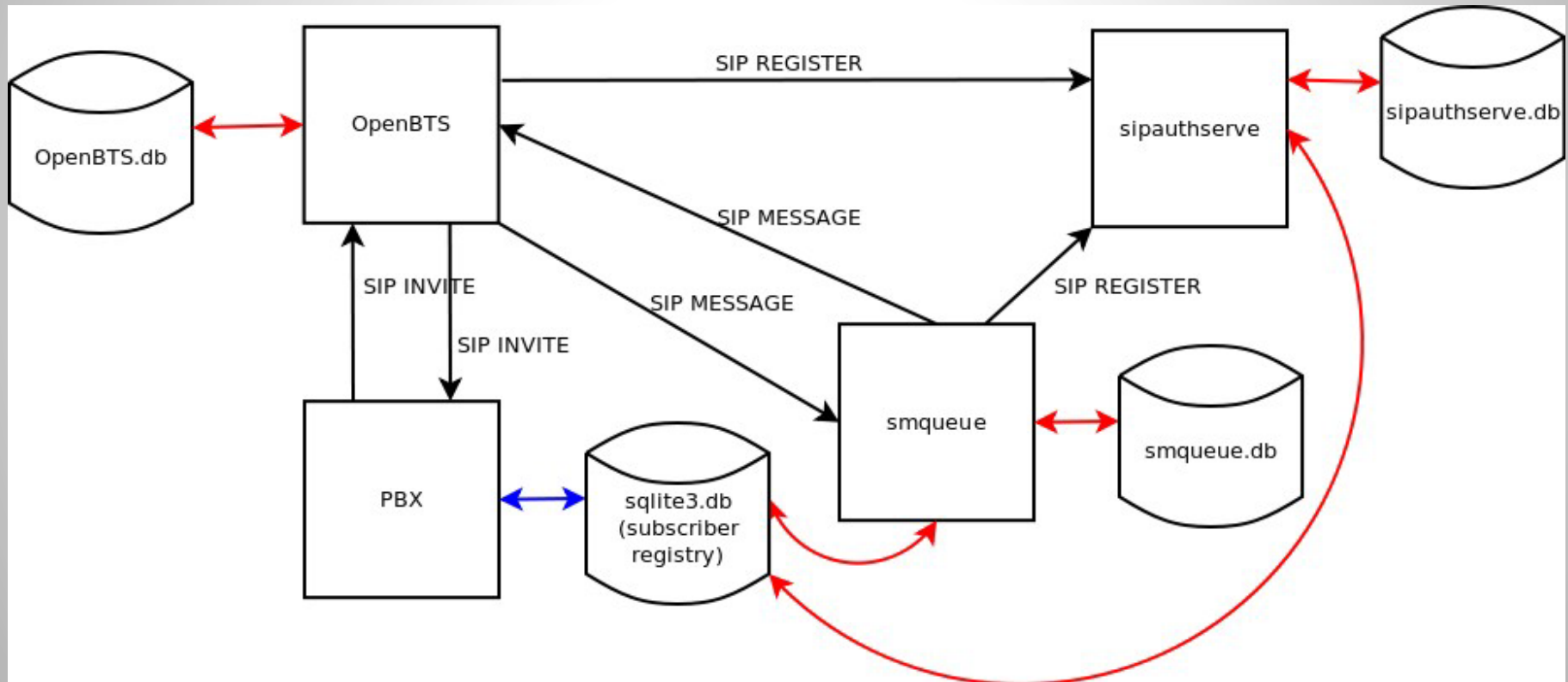


- LTE, UMTS and GSM can be “jammed” to downgrade/force connections.
- Overpower the analogue components of a radio with a stronger signal.
- Asian devices are often multi-band 1-10Watt radios and go against EMC.
- Protocols attempt to address “noise” or “sawtooth” jamming.
- None suitable for researchers or testing.
- Effect can be simulated by disabling 4G/3G.
- Wireless & Telegraphy Act in UK forbids use.



# 2.5G Simulation

## OpenBTS - Architecture





# Implementation

## GreedyBTS – USRP E100



- Gumstix Overo (computer-on-module)
- TI OMAP-3 SoC ARM Cortex-A8
- C64 DSP
- Xilinx Spartan 3A-DSP 1800 FPGA
- SBX (400Mhz – 4.4Ghz) 100 mW
- GPSDO Kit –or- Clock Tamer
- Ettus provide Angstrom Linux Image (e1xx-003) with GNU/Radio 3.6.4.1



# 2.5G Simulation EMC & Shielding



TX 50  $\Omega$  (ohm) load & RX 900Mhz omnidirectional antenna.  
Spectrum Analyser inside and outside enclosure (use a second SDR!)

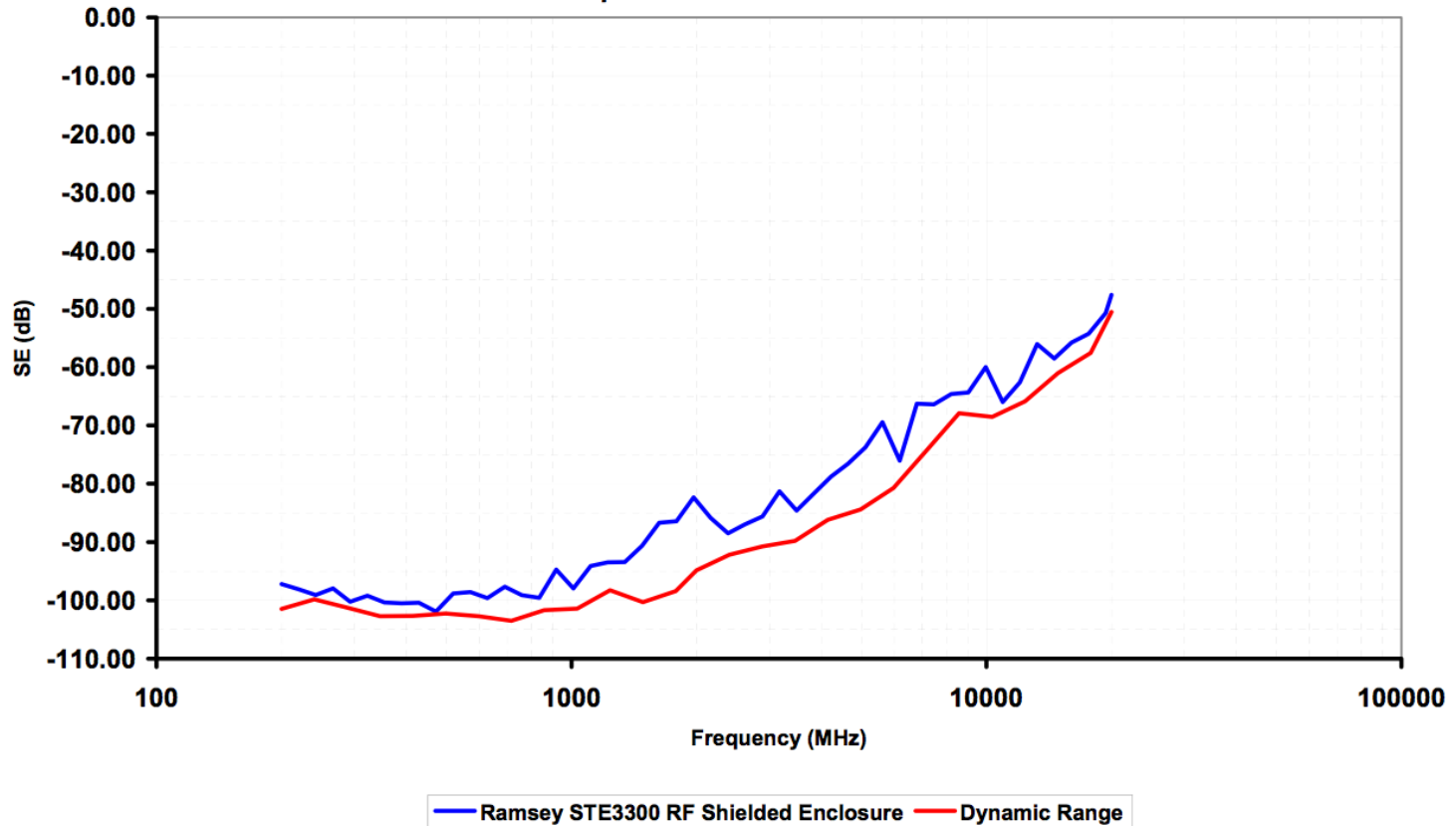


# 2.5G Simulation

## EMC & Shielding



**Shielding Effectiveness**  
**Ramsey STE3300 RF Shielded Test Enclosure**  
**Ramsey STE2000, STE3000 & STE4000 Series Have Same Construction as STE3300**  
**per EN61000-4-21**



- Spent a lot of time trying to build Angstrom for USRP E-1xx from scratch with limited success.
- Used Ettus E1xx\_3 firmware, cross-compiled new Kernel (no netfilter support or IP forwarding) and built packages from source with additional options such as ODBC and SQLite support.
- OpenBTS 5.0 and OpenBTS 2.8 (with mini-SGSN GPRS support) both installed.
- OpenBTS transceiver application has been broken for E1xx, modified for 5.0.
- I made minor patches to OpenBTS for more stealth operation (i.e. no welcome messages), increased logging in L3 Mobility Management events and disable SGSN firewalling for GPRS attacks.
- Asterisk configured with real-time SQLite support and automatic logging via monitor().
- Console interface script for interacting with components and BTS.
- Integrated DB for IMEI fingerprinting (50000+ devices) & MCC/MNC search.

# Implementation

## GreedyBTS – E100 firmware



```
fantastic@localhost:~
      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

22854: old priority 0, new priority 10
[+] Current CELL configuration
[-] =====
[-] Shortname: 'Test'
[-] MCC: 1 MNC: 1 C0 ARFCN: 51
[-] LAC: 1234 ARFCN's: 1 BAND: 900
[-]
[-] Radio Power
[-] =====
[-] RxGain: 0 MaxPower: 10 MinPower: 0
[-] Waiting 60 seconds before configuring GPRS...
net.ipv4.conf.all.forwarding = 1
SIOCADDRT: File exists
[-] GPRS OK!
--> []
```

- Useful events are sent to “greedyBTS.log” for logging and use by console app.
- Can dynamically provision a phone based on regex of IMSI or IMEI.
- User’s real-time configuration, can be left to run “headless” in target area.
- Useful utilities (airprobe, osmo-arfcn, tshark, tcpdump, libpcap) built.
- CDR records keep detail of subscriber communication attempts.
- Call content is automatically recorded to “call-recordings” directory.
- Can use Asterisk for connecting users to PSTN or amusement.
- GPRS is auto-configured, if the BTS has an internet connection so does phone.
- Example background exploit iPwn attacks MS over GPRS.
- Designed to be used against a specific target (1 or 2 users) in a small geographical area.
- Clone the BTS environment of CEO office, enter RegEx of CEO IMEI and wait ;-)
- It’s Linux! You can roll your own attacks / backdoors on-top.

```
fantastic@localhost:~  
[+] HELP SCREEN  
[-] dumpimei - lists all identified IMEI  
[-] dumpassoc - lists all IMEI+IMSI associations  
[-] dumpimsi - lists all identified IMSI  
[-] startservice - provide immediate service to IMSI  
[-] showservice - show all provisioned IMSI  
[-] stopservice - stop providing service to IMSI  
[-] seenservice - shows all seen IMSI and service status  
[-] watchservice - provide service to IMSI via regex  
[-] watchshow - show all IMSI provision regex  
[-] watchstop - stop providing service to IMSI regex  
[-] imeiservice - provide service to IMEI via regex  
[-] imeishow - show all provisioned IMEI  
[-] imeistop - stop providing service to IMEI regex  
[-] fingerprint - show fingerprints of seen IMEI  
[-] showipwn - show output of background iPwn attack  
[-] cellconfig - configure cell parameters for spoofing  
[-] cellinfo - dump information on current cell config  
[-] cellfind - find MCC/MNC, Operator, Status, Country  
[-] verbose - toggle real-time tracing  
[-] restart - restart OpenBTS (load new config)  
[-] exit - leave without shutdown to shell  
[-] shutdown - terminate all processes!  
--> 
```

- GPRS can be very slow to launch an exploit or extract data!

```
fantastic@localhost:~  
PING 192.168.99.2 (192.168.99.2): 56 data bytes  
64 bytes from 192.168.99.2: icmp_seq=0 ttl=63 time=2768.433 ms  
--- 192.168.99.2 ping statistics ---  
1 packets transmitted, 1 packets received, 0% packet loss  
round-trip min/avg/max/stddev = 2768.433/2768.433/2768.433/0.000 ms  
host is alive  
wiping old SSH keys  
ssh login test against 192.168.99.2  
connected  
SSH session started  
IOS accepts default password.  
login success  
Warning: Permanently added '192.168.99.2' (RSA) to the list of known hosts.  
Darwin Matthews-iPhone 14.0.0 Darwin Kernel Version 14.0.0: Thu May 15 23:10:44  
PDT 2014; root:xnu-2423.10.71~1/RELEASE_ARM_S5L8940X iPhone4,1 arm N94AP Darwin  
added SSH key to known hosts, grabbing SMS  
downloaded SMS, grabbing contacts  
downloaded AddressBook  
done  
  
real    5m47.059s  
user    0m0.344s  
sys     0m0.094s  
root@usrp-elxx:~/gsmhax/ipwn#
```



- You will need an 8GB MicroSD card to install in E100.
- Change default root password on login and change SSH keys.
- [https://mega.co.nz/#!hAU2iJyB!  
GK54dtAxUVXavcZUGPJPDI7X3\\_OjpnPqs\\_qSZfc9iwE](https://mega.co.nz/#!hAU2iJyB!GK54dtAxUVXavcZUGPJPDI7X3_OjpnPqs_qSZfc9iwE)
- 726f9d810aca42ed5ba3034efe6b6a2a greedyBTS-44CON-v1.img.enc
- openssl aes-256-cbc -d -in greedyBTS-44CON-v1.img.enc -out greedyBTS-44CON-v1.img (**Contact me for password.**)
- 4667f83fdc4a30245fdcc49946833e5d greedyBTS-44CON-v1.img
- dd if=./greedyBTS-44CON-v1.img of=/dev/sdc bs=1024
- Discussed in Feb on OpenBTS / USRP mailing lists, 7:1 GSM researchers mailed in favor of image sharing in a controlled way.

# Implementation

## Example traffic



- Interested in GSM?
- Here is a PCAP trace of 2.5G environment showing uplink/downlink, two MS devices, SIM APDU information!
- Recommend reading a good book and review in wireshark!
- <https://github.com/HackerFantastic/Public/blob/master/misc/44CON-gsm-uplink-downlink-sim-example.pcap>
- BeagleBone Black and NanoBTS/USRP B200/BladeRF could be used in future for cheaper alternative!

# Implementation Demo





- 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 greedyBTS but they will require “active” use and aimed at power users.
- If you are transmitting sensitive information such as usernames or passwords consider using a non-wireless technology.
- An attacker can launch attacks against your mobile device without you being aware using 2.5G, we need baseband security enhancements and access to cell data.

E-mail: [hackerfantastic@riseup.net](mailto:hackerfantastic@riseup.net)

Twitter: @HackerFantastic

<https://github.com/hackerfantastic/public>

Questions?



Thank you for all the hard work done by members of the open-source and security research communities in making 2.5G networks more accessible for analysis.

Twitter: @MDSecLabs

Blog: <http://blog.mdsec.co.uk>

