MDSec

GreedyBTS – Hacking Adventures in GSM

GreedyBTS – Hacking Adventures in GSM

Agenda

- 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

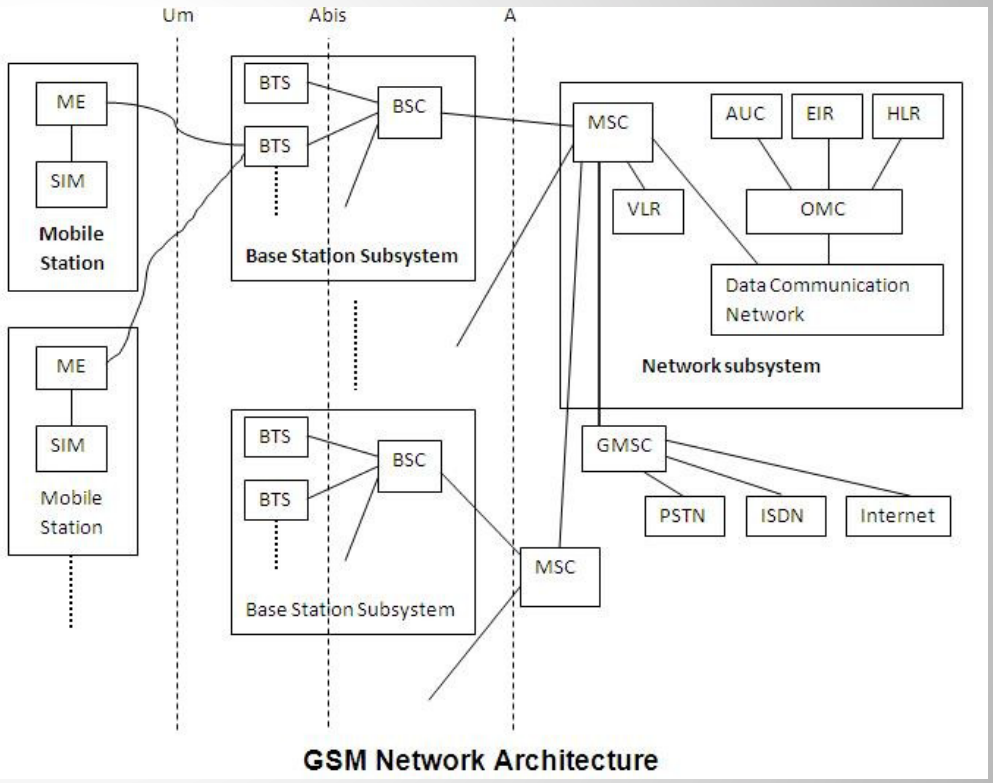
Introduction to GSM

- 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, 3rd and 4th 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.



GSM Network Architecture

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.

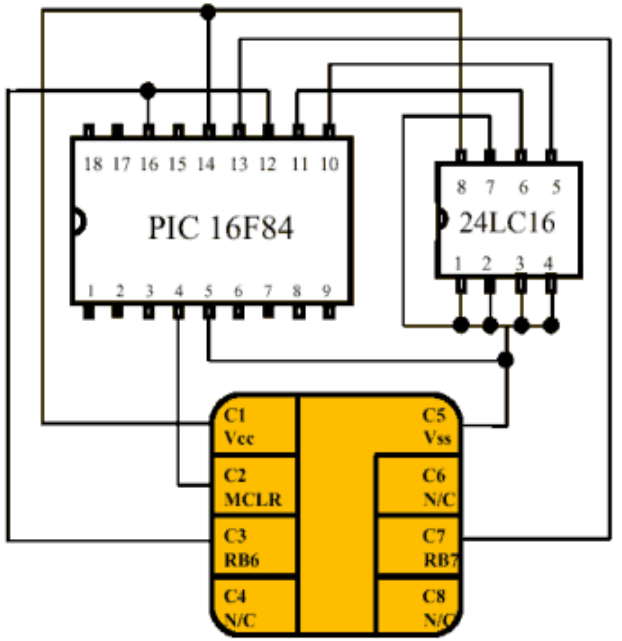
- Your phone contains a baseband processor and RTOS used by GSM.

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.

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



- Programmable card can be used which has a writeable Ki key.
- GSM test cards with a writeable Ki key can be bought online.

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.

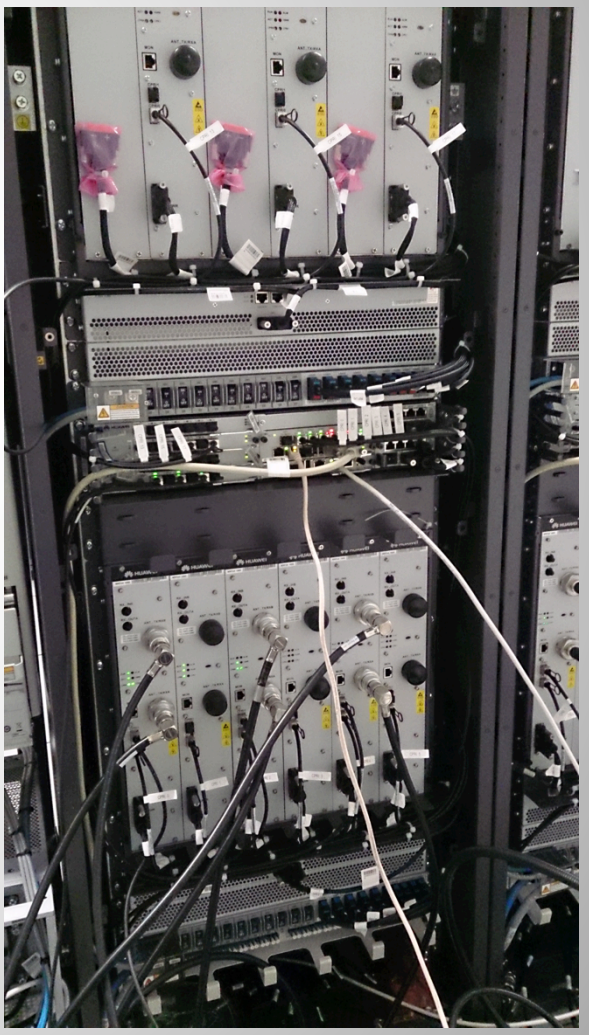
- COMP128v1 is an encryption algorithm that was found to be flawed.
- A “stop” condition was found that allows Ki to be brute forced.
- COMP128v1 attack takes 12-24 hours and requires physical card.
- COMP128v3 is used more widely today and COMP128v1 is rare.
- Chinese vendors sell cheap COMP128v1 multi-SIM 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)?

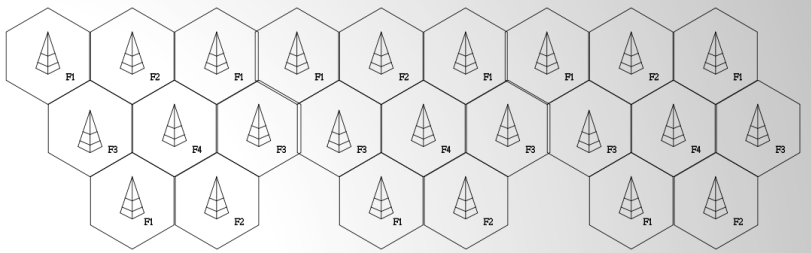
- Transmitter and receiver equipment, such as antennas and amplifiers.
- Has components for doing digital signal processing (DSP).
- Contains functions for Radio Resource management.
- Provides the air (UM) interface to a MS.
- This is part of a typical "cell tower" that is used by GSM.
- BTS provides 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!

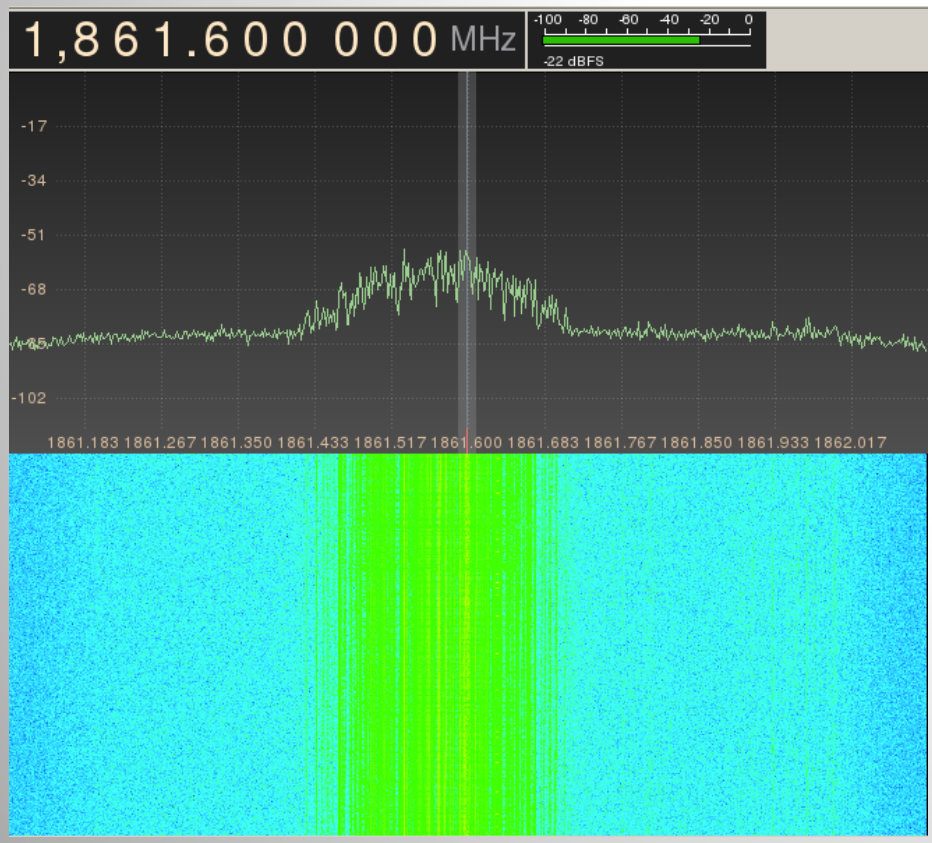


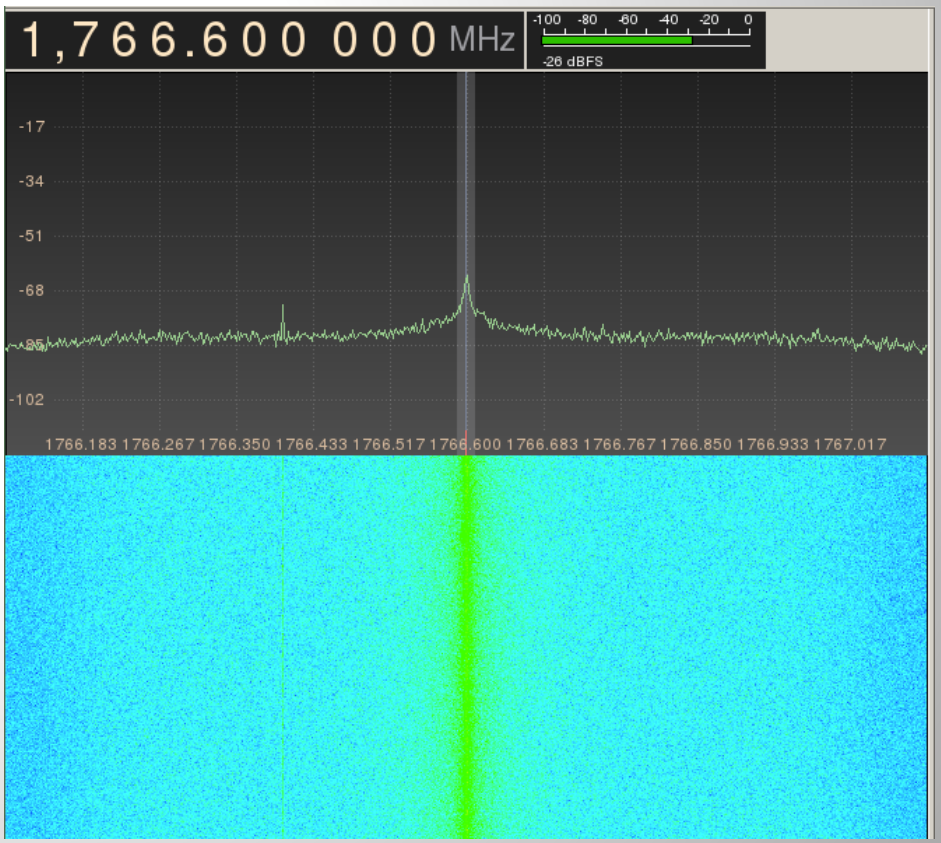
Band	Designation	ARFCN	f_{UL}	f_{DL}
GSM 400	GSM 450	259-293	450,6+0,2(n-259)	$f_{UP}(n)+10$
	GSM 480	306-340	479+0,2(n-306)[1]	$f_{UP}(n)+10$
GSM 700	GSM 750	438-511	$f_{UP}(n)+30$	747,2+0,2(n-438)[2]
GSM 850	GSM 850	128-251	824,2+0,2(n-128)	$f_{UP}(n)+45$
GSM 900	P-GSM	1-124	890+0,2n	$f_{UP}(n)+45$
	E-GSM	0-124 975-1023	890+0,2n 890+0,2(n-1024)	$f_{UP}(n)+45$
	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.

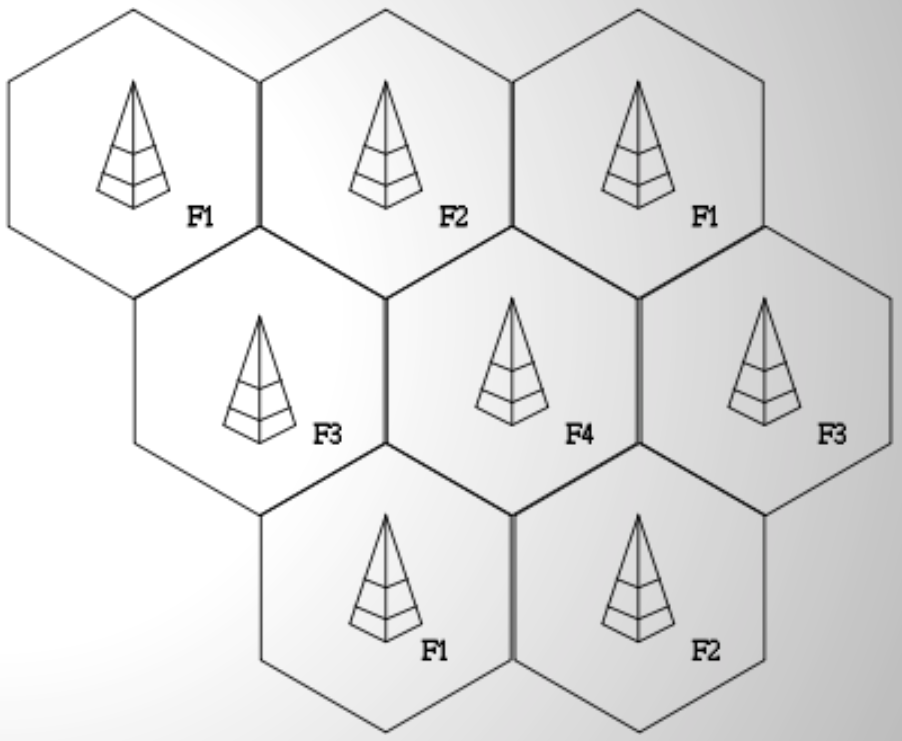




2.5G Technical Overview

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 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).



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.

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.

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 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 subscriber mobile usage. We will look at this in more detail.

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).

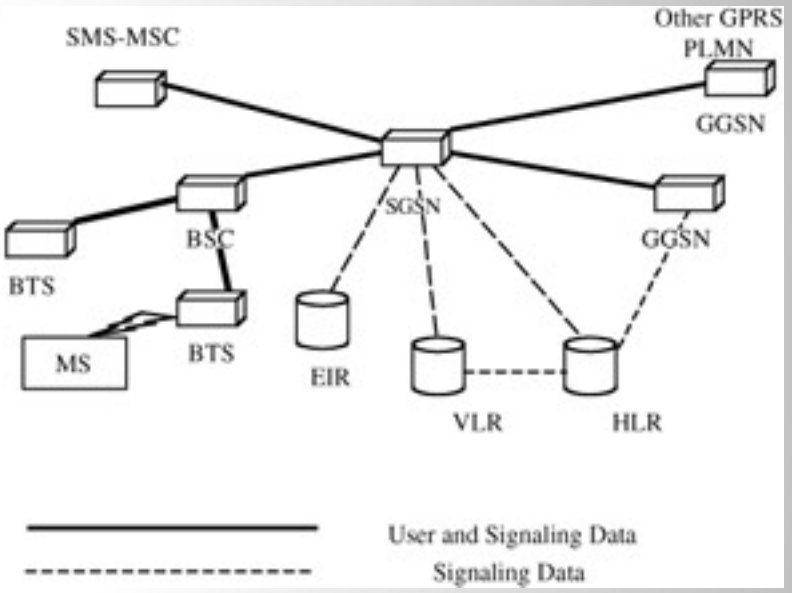
- A5/1 – publicly broken, rainbow tables exist.
- A5/2 – offers no real security.
- A5/3 – KASUMI Cipher, although some man-in-the-middle attacks are known – it has not yet been publicly broken in GSM.
- A3/A8 - used during the authentication process.

- 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

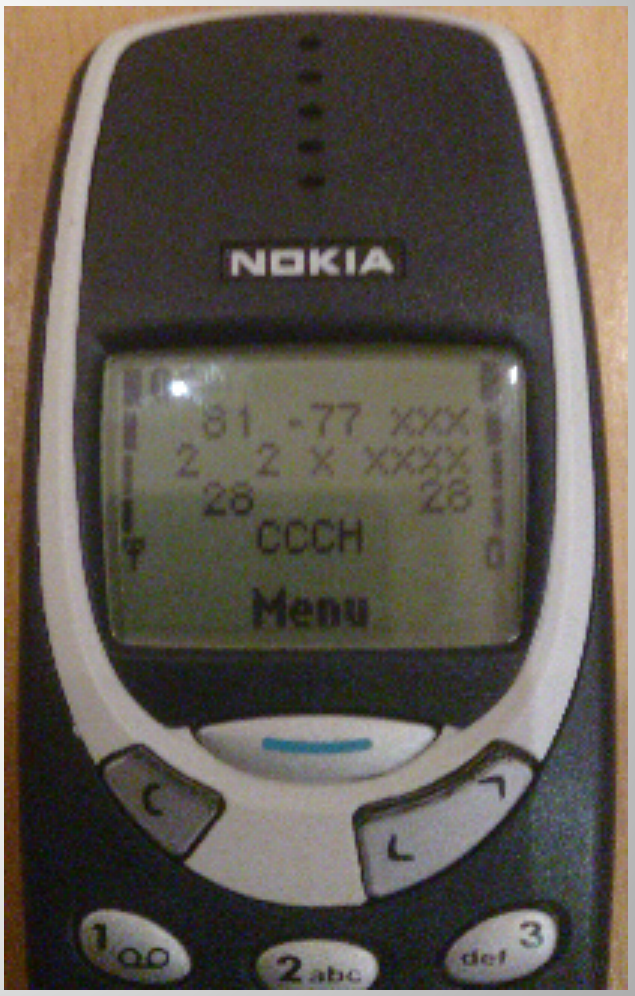
- Uses existing GSM concepts, e.g. timeslots.
- Introduces “Subscriber GPRS Service Node” (SGSN) and “Gateway GPRS Service Node” (GGSN).
- Adds Packet Control Unit to BSS.
- Data is sent in PCU frames.
- Introduces a new Radio Resource (RR) protocol.
- Radio Link Control (RLC) / Media Access Control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

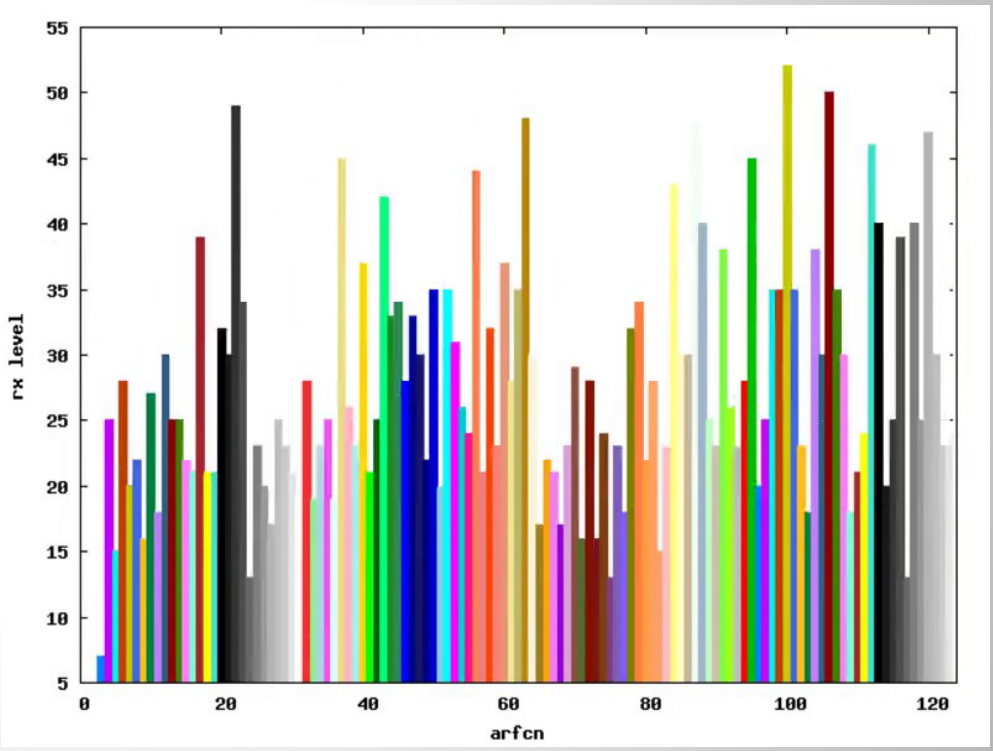
Dedicated Test Hardware

- 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

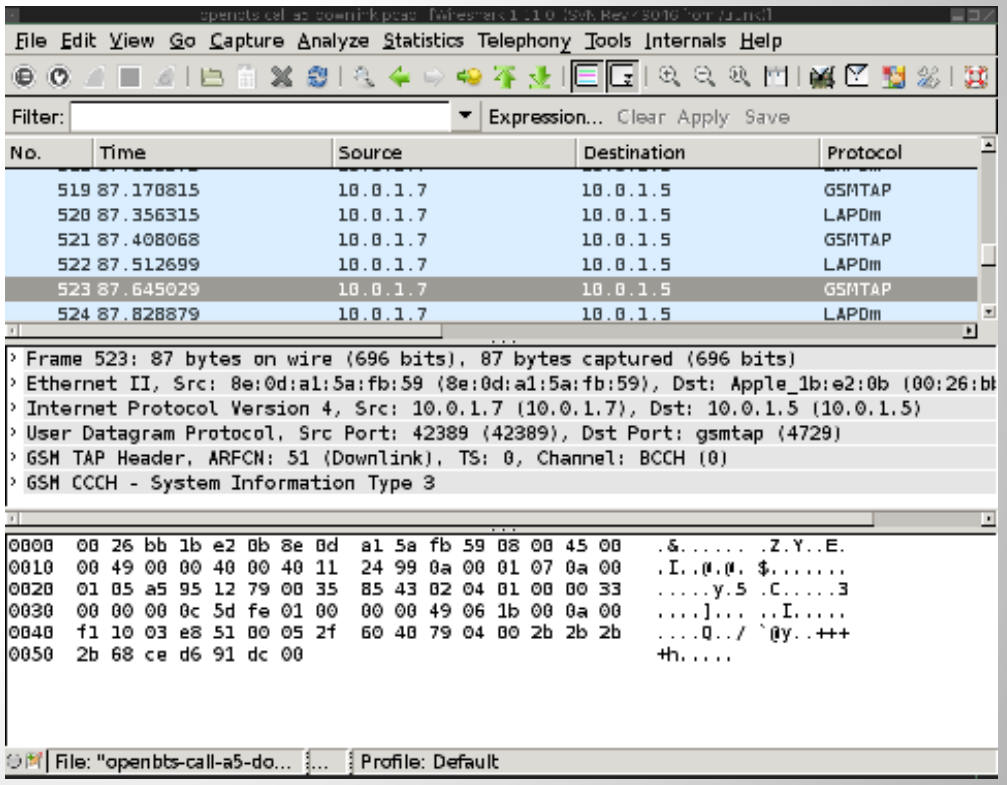
- Osmocom-bb allows you to write tools for MS baseband.
- Lots of useful diagnostics already available in the public repository.
- You can extend the code to visually represent the GSM spectrum or perform more detailed analysis of a GSM cell tower.
- Requires a <£30 phone to use.



Cell Diagnostics & Tools

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 Um interface traffic from a BTS or MS of downlink and uplink.
- Extremely useful capability when analysing GSM.



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 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.

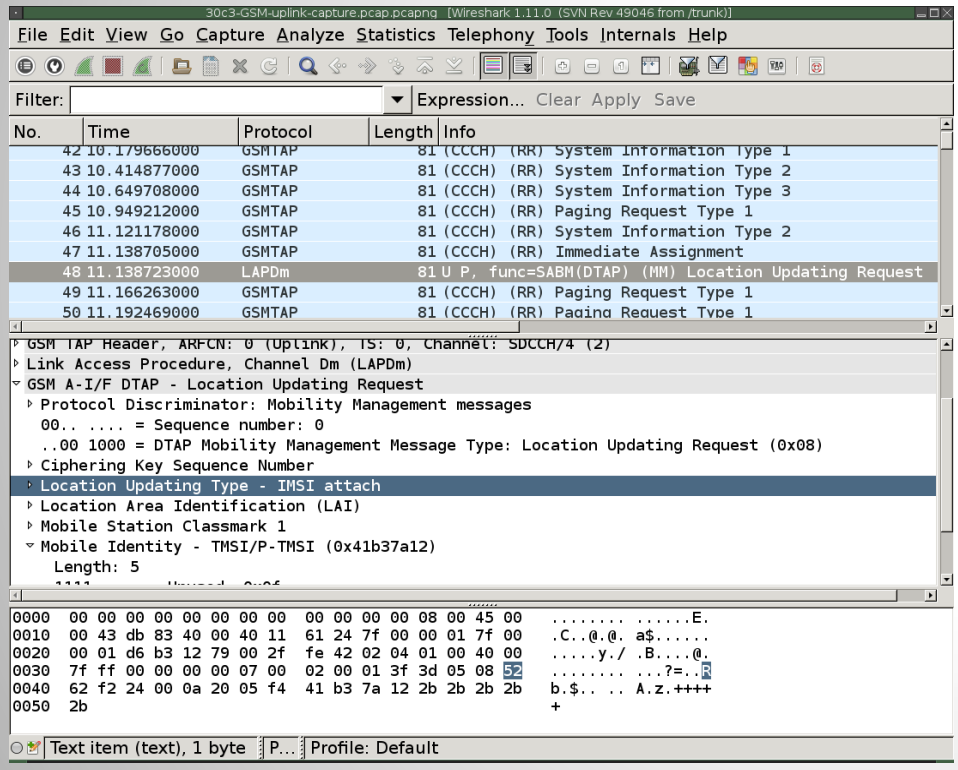
IMEI & Device Fingerprint

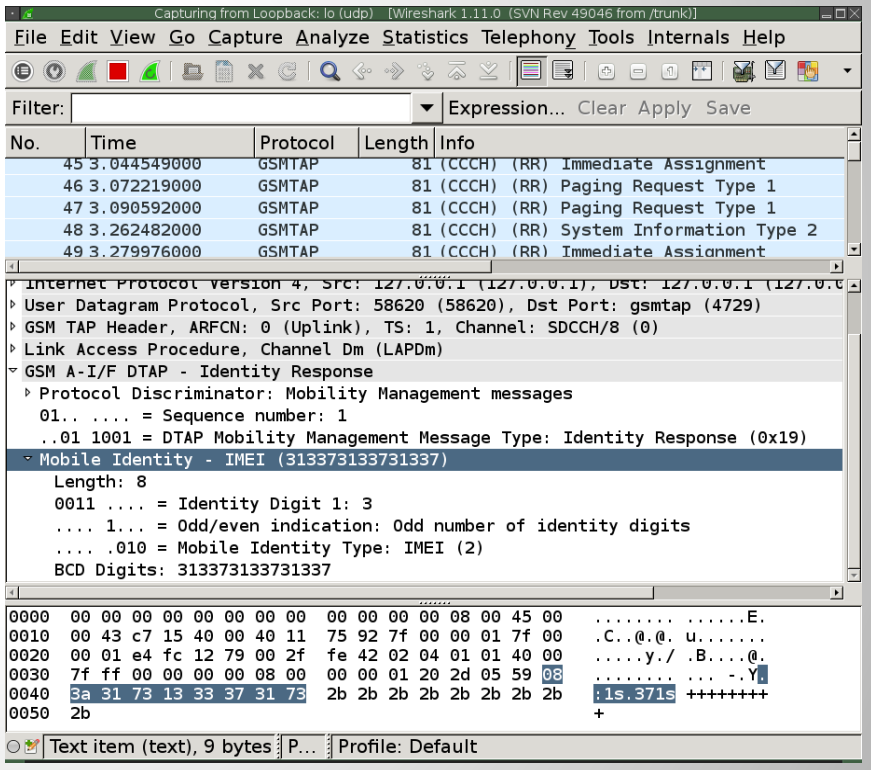
	AA	BB	BB	BB	CC	CC	CC	D or EE
IMEI	TAC			TAC (FAC)	Serial			(Luhn Checksum)
IMEI	013035			00	561434			0

- 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



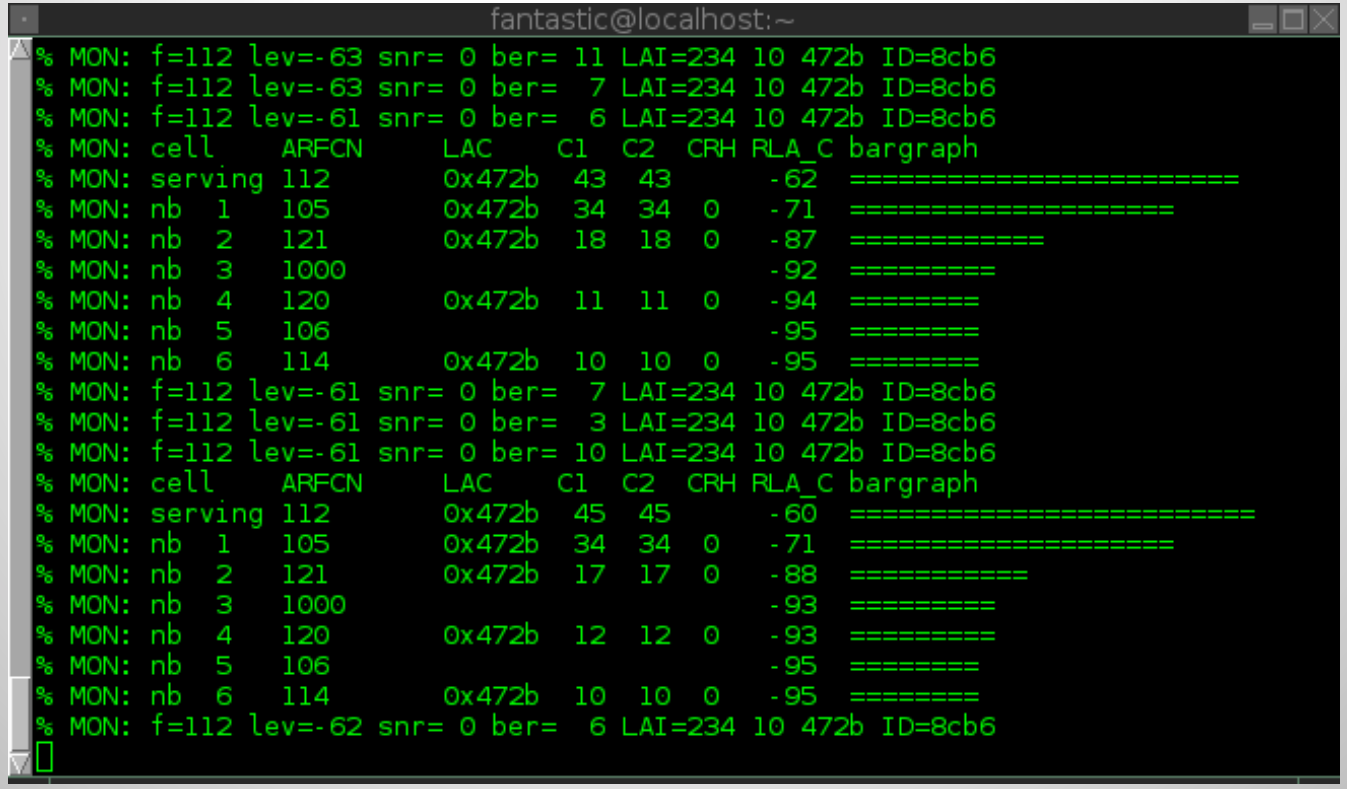


GSM Security
Clone a BTS

- 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.

Clone a BTS

- 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.

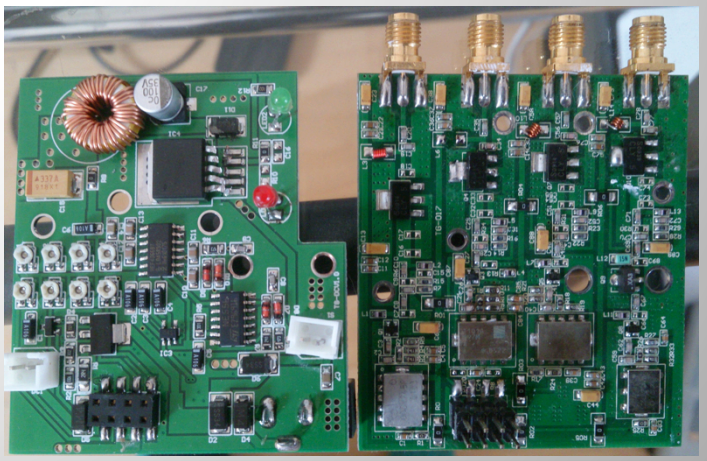


RACH & TMSI Paging Attacks

- 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.

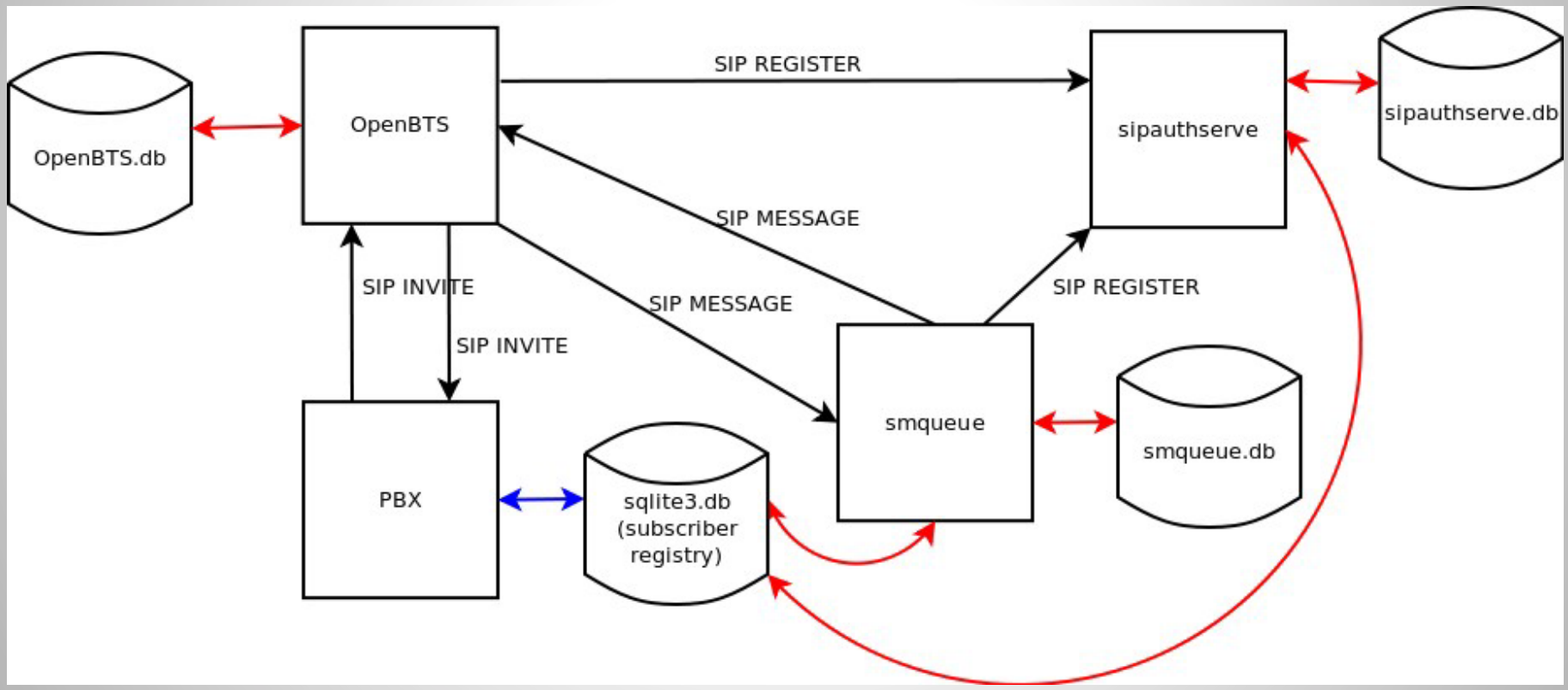
GSM Security
Downgrade & Jamming

- 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

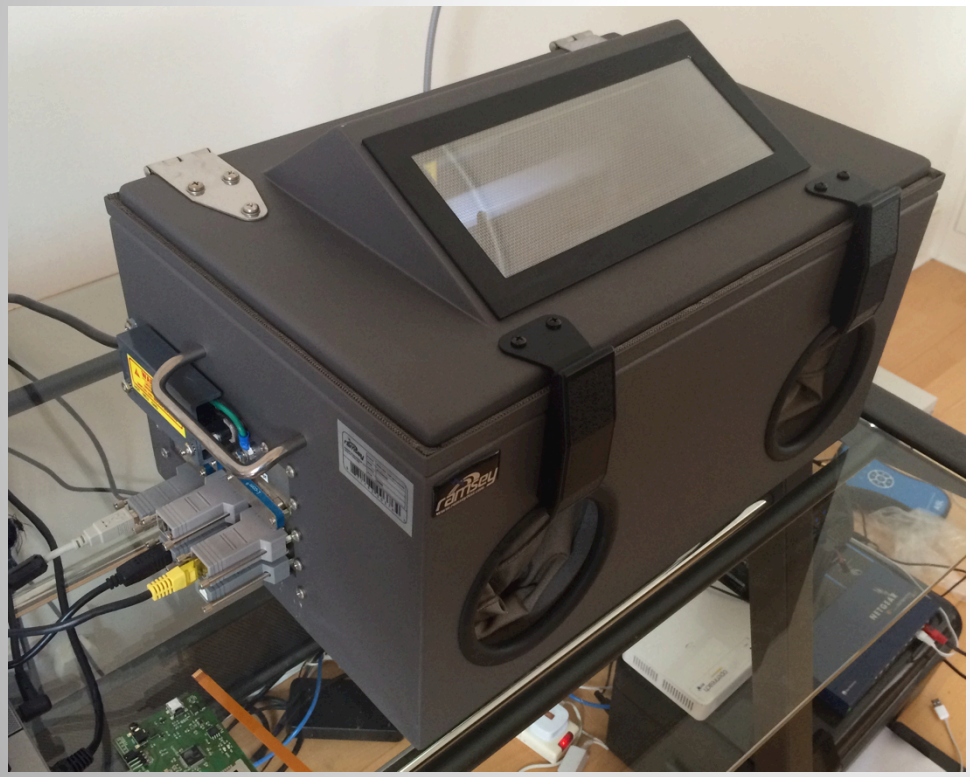
- Gumstix Overo (computer-on-module)
- TI OMAP-3 SoC ARM Cortex-A8
- C64 DSP
- Xilinx Spartan 3A-DSP 1800 FPGA
- SBX (400Mhz – 4.4Ghz) 100 mW
- GPSDO Kit –or- Clock Tamer
- Ettus provide Angstrom Linux Image (e1xx-003) with GNU/Radio 3.6.4.1

2.5G Simulation

EMC & Shielding

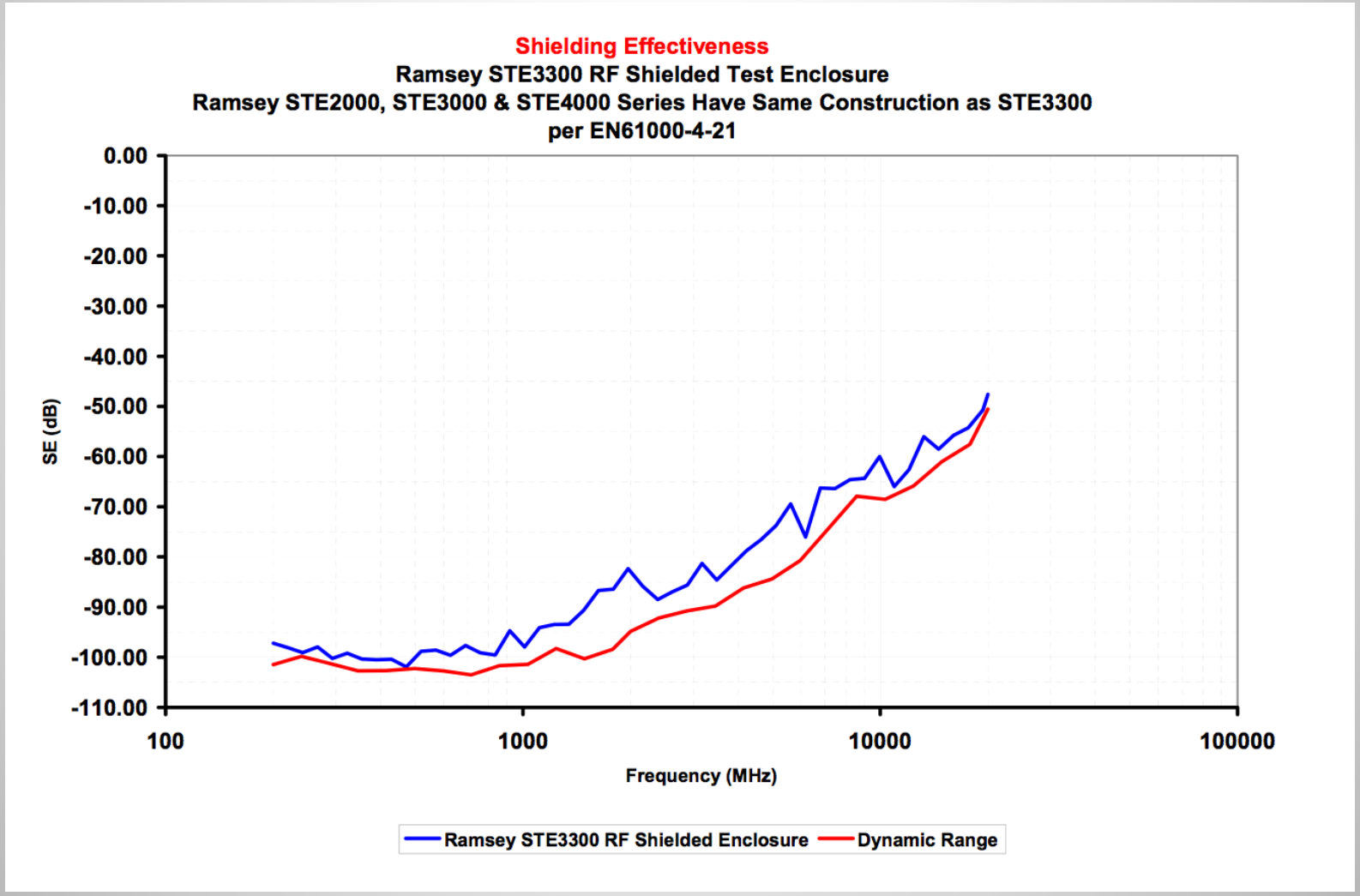
TX 50 Ω (ohm) load & RX 900Mhz omnidirectional antenna.

Spectrum Analyser inside and outside enclosure (use a second SDR!)



2.5G Simulation

EMC & Shielding



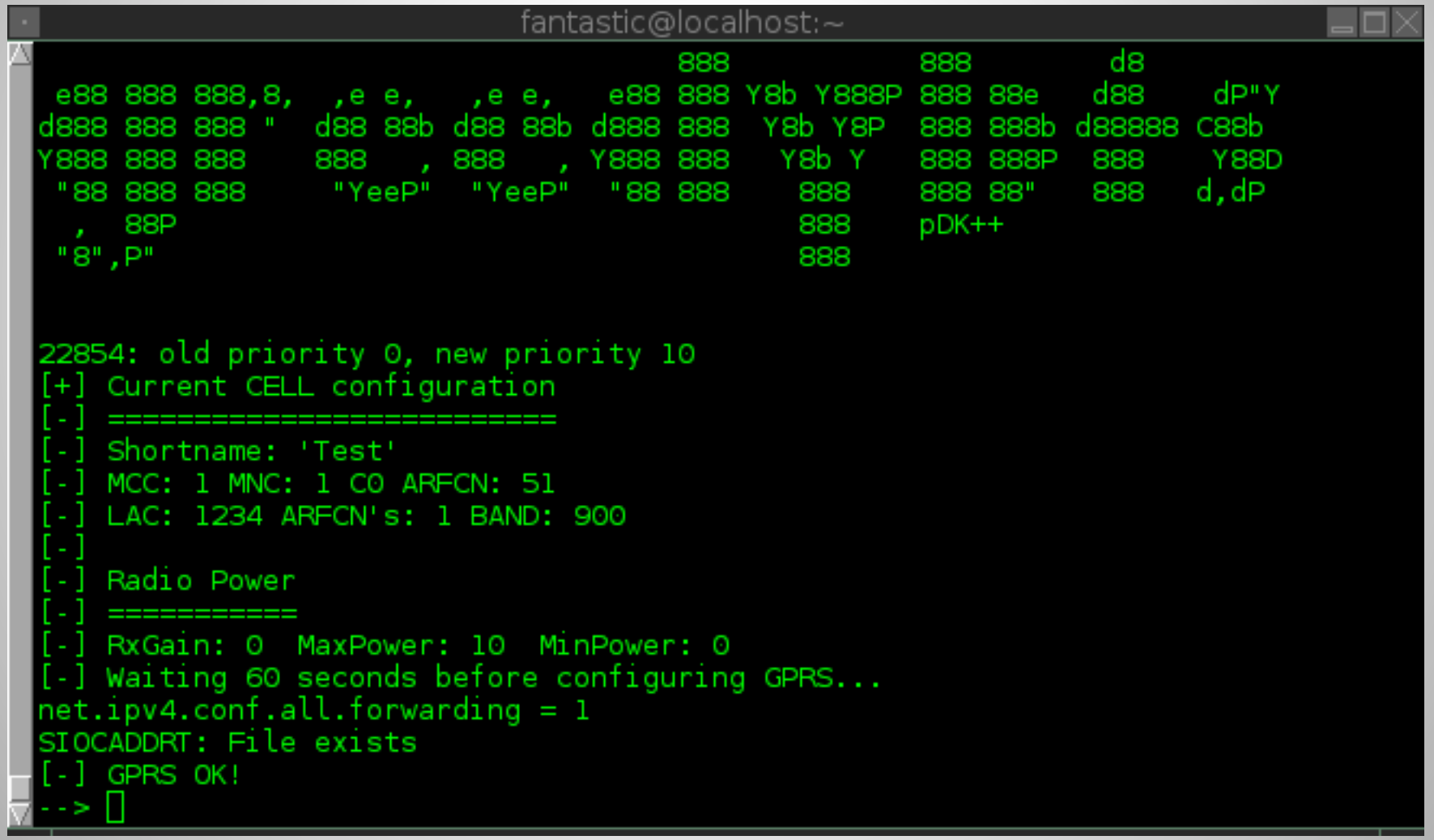
Implementation

GreedyBTS – E100 firmware

- 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

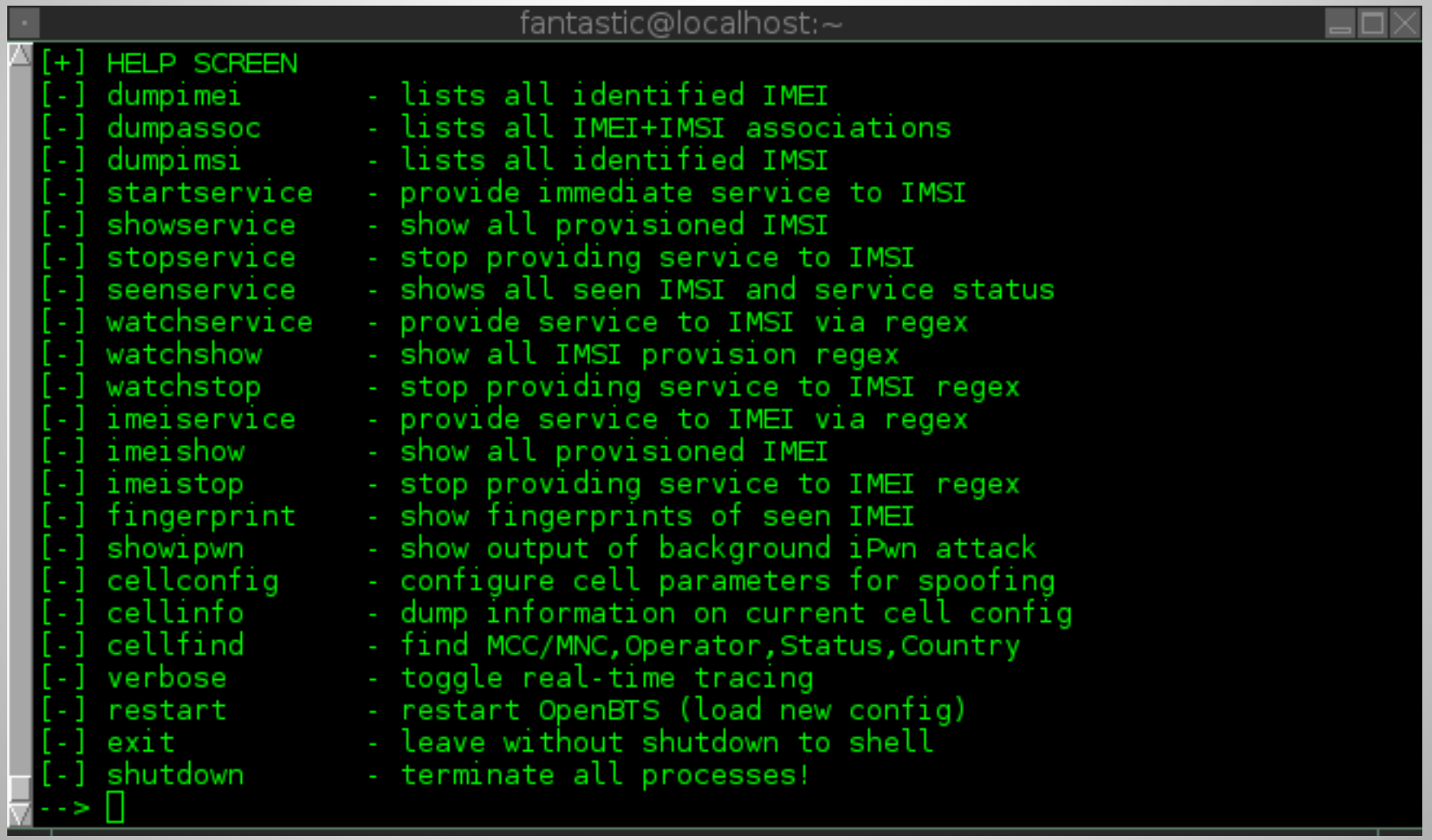


Implementation
GreedyBTS - Features

- 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.
- Use’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.

Implementation

GreedyBTS - Features



Implementation

GreedyBTS + iPwn

- 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-e1xx:~/gsmhax/ipwn#
```

Implementation
Download

- 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!GK54dtAxUVXavcZUGPJPDl7X3_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

GreedyBTS – Hacking Adventures in GSM

Conclusions

- 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

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