GSM Open-source intelligence

Kenneth van Rijsbergen[1]

[1] MSc System and Network Engineering
Faculty of Science
University of Amsterdam

30 June 2016

Table of Contents

Research question

How may GSM be used for gathering OSINT by a red team ?

- How can a Software Defined Radio (SDR) be used to passively capture GSM traffic ?
- How can a Software Defined Radio (SDR) be used to actively capture GSM traffic ?
- What OSINT may be extracted from this GSM data ?

Software Defined Radio

- HackRF One
  - 1 MHz to 6 GHz
  - half-duplex transceiver
  - $299.-
- BladeRF x40
  - 300MHz to 3.8GHz
  - full-duplex transceiver
  - $420.-

FIGURE – HackRF One

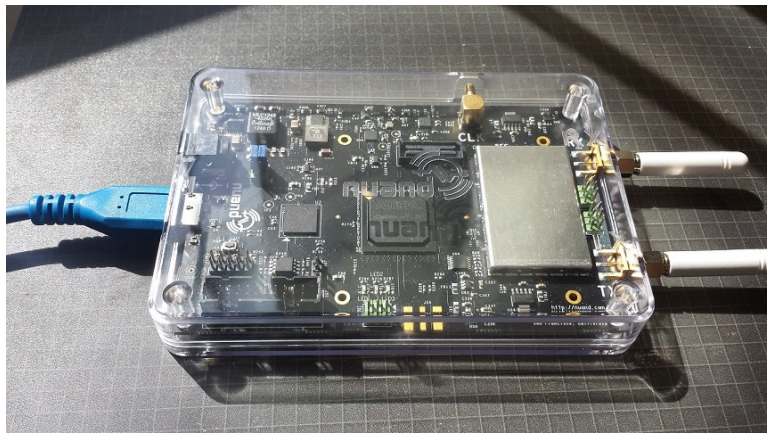


FIGURE – BladeRF x40

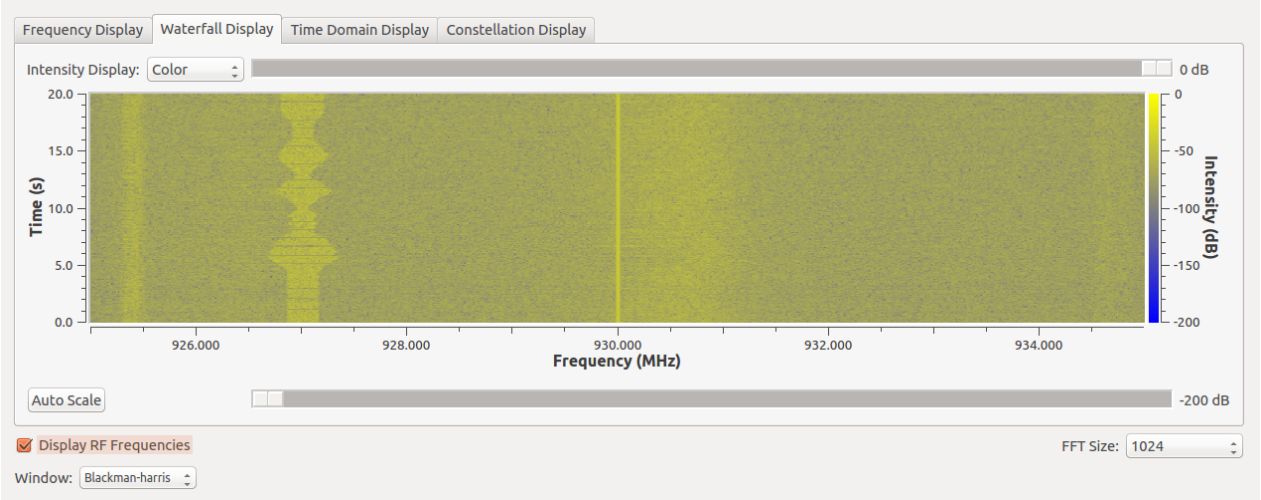


FIGURE – Waterfall (jamming test inside faraday cage)

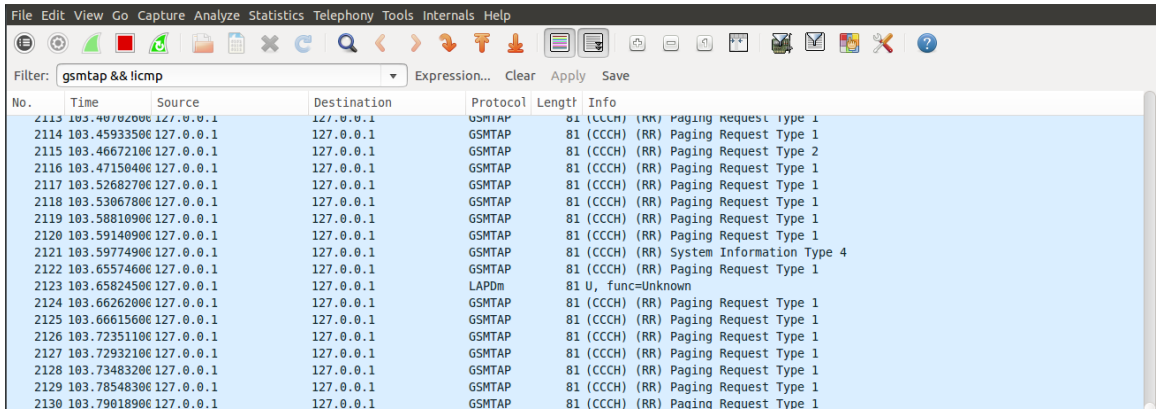


FIGURE – GSM sniffing with HackRF

Overview of mobile generations

First generation (1G)

- 1980's
- Analogue
- Voice only
- Technologies : AMPS, NMT, TACS, C-450, Radiocom 2000, RTMI, JTACS, TZ-801, TZ-802, and TZ-803

Second generation (2G)

- 1990's
- Digital signalling,
- SMS, MMS, voice mail, call forwarding
- Encryption (A5/1 and A5/2)
- technologies : **GSM**, IS-95 (a.k.a. cdmaOne), PDC, iDEN and IS-136 (a.k.a. D-AMPS)
- 2.5G : GPRS
- 2.75G : EDGE

Overview of mobile generations

Third generation (3G)

- 2000's
- Improved crypto (A5/3) and two-way authentication between MS and BS.
- Faster data transfer
- Technologies : W-CDMA (UMTS), TD-SCDMA (only in China), HSPA, and HSPA+, CDMA2000, LTE
- Recently allowed to use the 900 and 1800 Mhz band (same as GSM).

Fourth generation (4G)

- IP based, no more circuit-switched telephone
- Technologies : LTE Advanced and Mobile WiMAX

GSM Architecture + Lingo

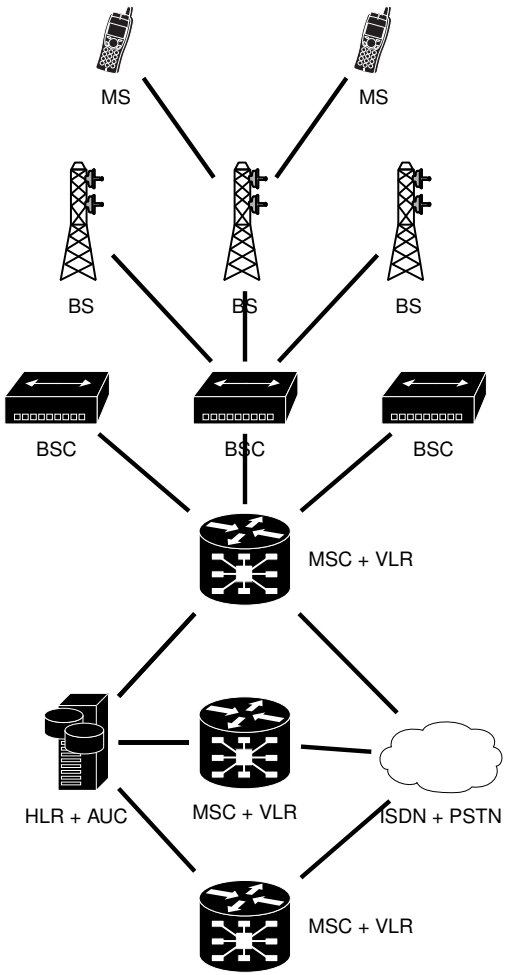


FIGURE – GSM Architecture

MS	Mobile station
BS	Base Station
BSC	Base Station Controller
MSC	Mobile Switching Center
VLR	Visitor Location Register
HLR	Home Location Register
AUC	Authentication Center
EIR	*Equipment Identity Register*

GSM authentication sequence

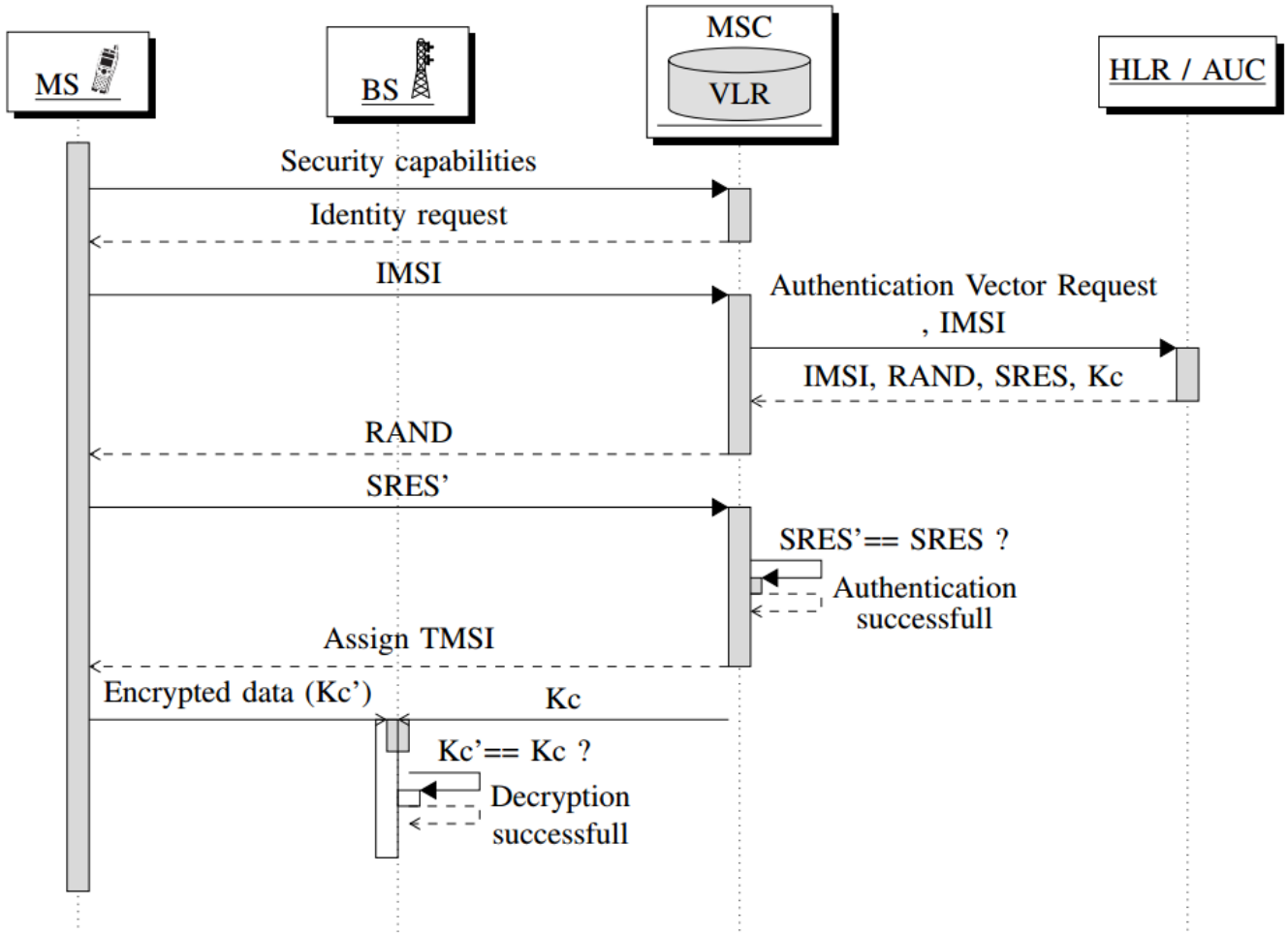


FIGURE – GSM authentication sequence

IMSI catcher

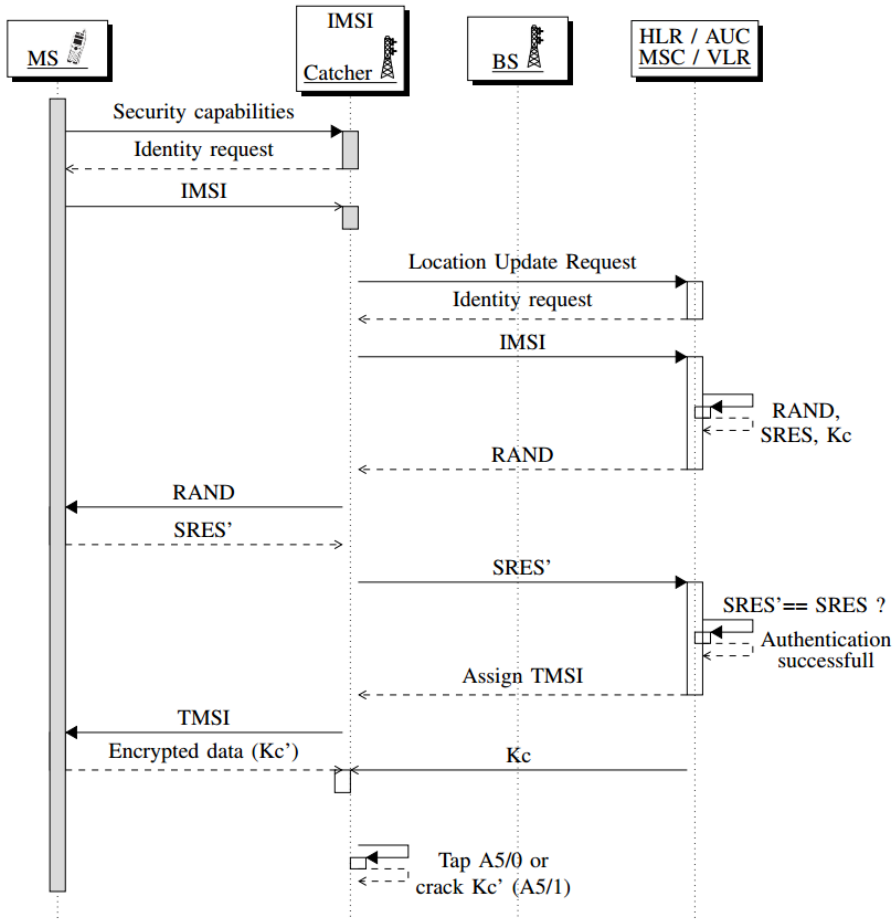


FIGURE – IMSI catcher

GSM Authentication

- A5 used to encrypt the data transmission between the MS and BS.

A5/1 - Developed in 1987. Workings kept secret.
- Reverse engineered in 1999 and published.
- Can be cracked in seconds using rainbow tables.

A5/2 - Extremely weak, developed for export markets
- Can be cracked in real-time.
- Discontinued by the GSM association since 2006.

A5/3 - In use today.
- Designed for 3G but also used for GSM.
- Based on the MISTY block cypher which was later simplified into the KASUMI block cypher.
- A faster than an exhaustive search attack has been found but nothing practical.

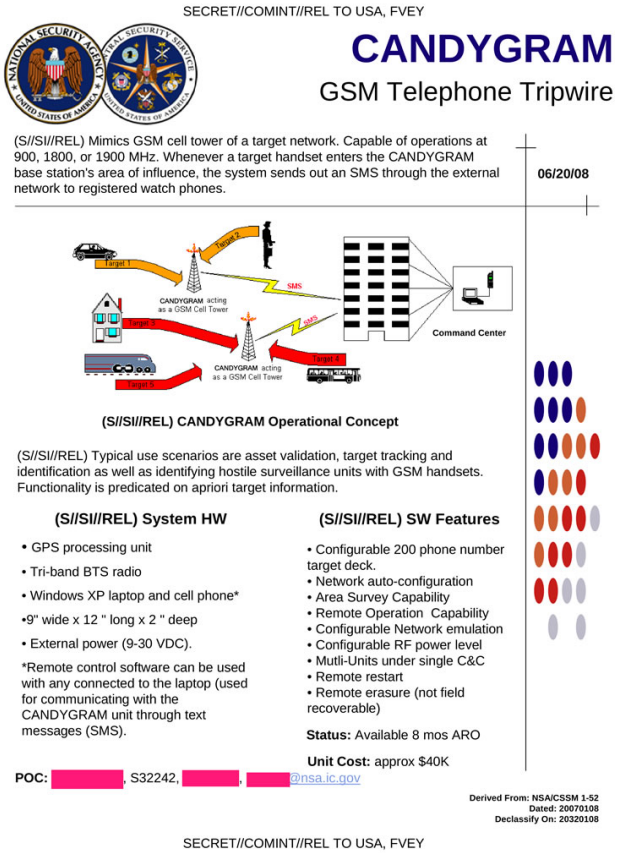
IMSI catcher

IMSI International Mobile Subscriber Identity

- Can be used to identify a mobile subscriber.
- The IMSI is send by GSM unencrypted over the air during authentication. This enables tracking.

- Full IMSI catchers (full MITM)
- Half IMSI catchers (outgoing only)
- Both require a spoofed basestation.

IMSI catcher


SECRET//COMINT//REL TO USA, FVEY

CANDYGRAM

GSM Telephone Tripwire

(S//SI//REL) Mimics GSM cell tower of a target network. Capable of operations at 900, 1800, or 1900 MHz. Whenever a target handset enters the CANDYGRAM base station's area of influence, the system sends out an SMS through the external network to registered watch phones.

06/20/08

(S//SI//REL) CANDYGRAM Operational Concept

(S//SI//REL) Typical use scenarios are asset validation, target tracking and identification as well as identifying hostile surveillance units with GSM handsets. Functionality is predicated on apriori target information.

(S//SI//REL) System HW

- GPS processing unit
- Tri-band BTS radio
- Windows XP laptop and cell phone*
- 9" wide x 12 " long x 2 " deep
- External power (9-30 VDC).

*Remote control software can be used with any connected to the laptop (used for communicating with the CANDYGRAM unit through text messages (SMS).

(S//SI//REL) SW Features

- Configurable 200 phone number target deck.
- Network auto-configuration
- Area Survey Capability
- Remote Operation Capability
- Configurable Network emulation
- Configurable RF power level
- Mutli-Units under single C&C
- Remote restart
- Remote erasure (not field recoverable)

Status: Available 8 mos ARO

Unit Cost: approx $40K

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

SECRET//COMINT//REL TO USA, FVEY

FIGURE – NSA GSM Tripwire (NSA's ANT Division Catalog)

FIGURE – Stingray I (http://arstechnica.co.uk/)

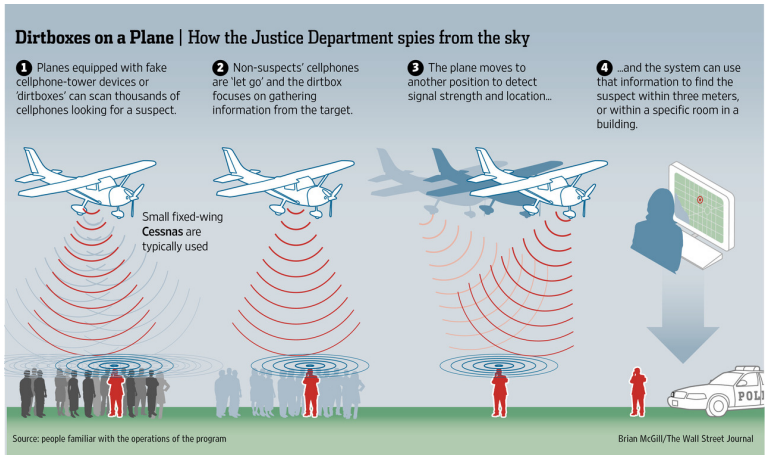


FIGURE – IMSI catcher on planes (Brian McGill | The Wall Street Journal)

Passive Capturing

- Possible but all is encrypted
- Some IMSI's may (in theory) be captured when in initial authentication. But nothing that can be practically used.

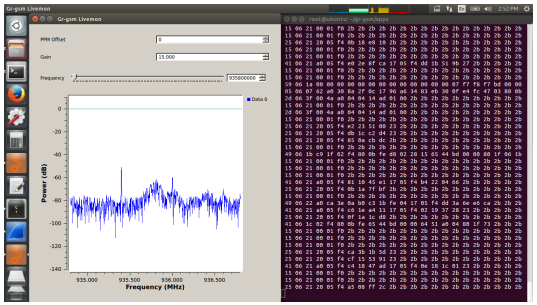


FIGURE – GSM Decoding

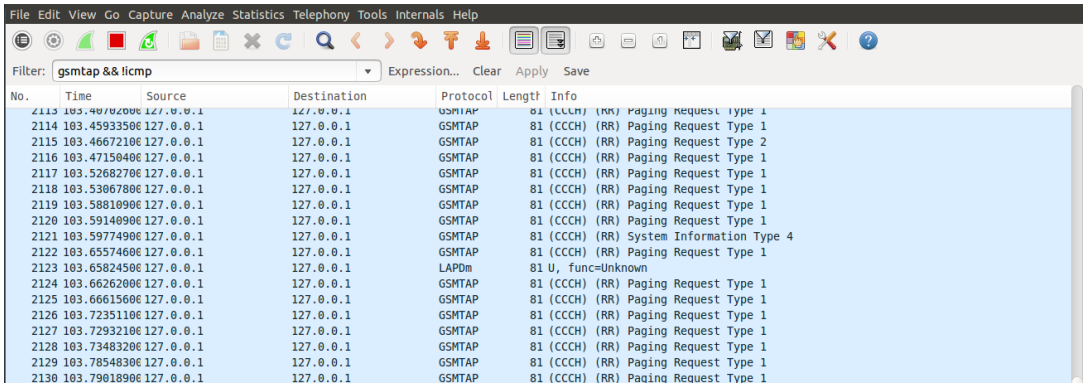
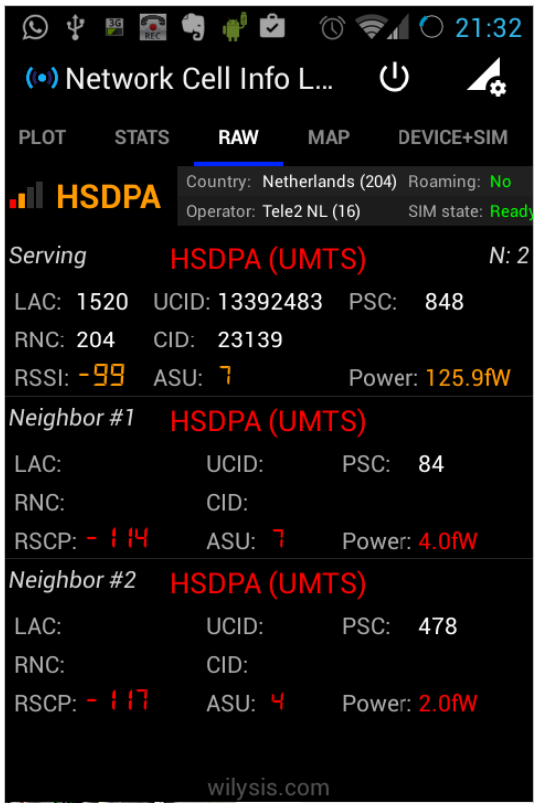


FIGURE – GSM data in Wireshark

Demo

Spoof limitation

- YateBTS only supports 2.5G GPRS
- OpenBTS-UMTS offers 3G UMTS but requires more expensive hardware (a recent USRP)



The phone will always prefer a higher standard, even if the signal is weak

1. ~~4G LTE-Advanced~~
2. ~~3G UMTS~~
3. ~~2.75G EDGE~~
4. 2.5G GPRS <- YateBTS
5. 2G GSM

Jamming

The HackRF is not suitable for jamming

- Test was conducted inside a Faraday cage.
- Jamming a specific 900Mhz GSM channel was possible, but only for the old 2G Nokia.
- 3G HTC phone disconnects, then recovers when setting up a new call.
- Higher bands (like 1800) are too wide for the HackRF to cover.
- Transmitting at a higher frequency requires more power ; HackRF did not have enough to disrupt 2G 1800.
- 3G jamming is even more hopeless due to spread spectrum.

- Would be nice to test with a real 3G jammer.
- The hypothesis would be that the phone drops down to EDGE instead of GPRS.

Conclusion and Future work

Conclusion

- Passive attacks are not effective due to encryption.
- Active attacks can only be effective versus 2G phones or when using jamming attacks (illegal).
- If, however a phone connects, everything outgoing can be intercepted (Internet, Voice, SMS).

Future Work

- Full IMSI Catcher (still relies on a successful spoof)
- Selective jamming* (jam all but one channel)