GSM – have we overslept the last wake-up call?

Domonkos P. Tomcsányi

HACKTIVITY

A moment of silence

What happened?

- 1994 first attack by Ross Anderson
- Theory was ahead but nothing in practice

- Karsten Nohl teamed up with many people during the years and carried out the whole process:

- 2009 A5/1 tables computed and released
- 2010 Capturing data with USRP, decryption possible
- 2011 Capturing data with OsmocomBB, hopping channels
(- 2013 SIM card attack)

I’m all about GSM, so…?

- It is hard to start because there are not many „easy” entry points

- Either you use USRP or OsmocomBB
- USRP: expensive for hobbyists
- OsmocomBB: quite complicate to get it up and running, even harder to understand how it works

- Found 3 theses online which tried to work with OsmocomBB, all 3 of them failed

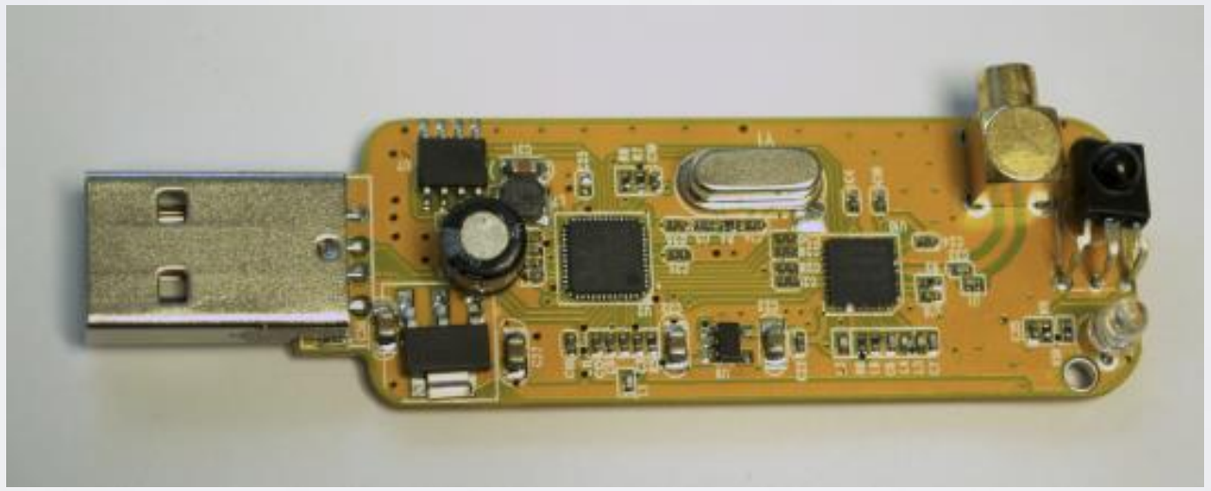
GSM hacking now

2010 „The USRP approach”	2011 „The OsmocomBB approach”
Code: AVAILABLE (limited)	Code: NOT AVAILABLE
Cost of Hardware: HIGH	Cost of Hardware: LOW

So what do we want?

- Something that works (meaning it has code available)
- Something that’s affordable for people
- Something that’s relatively easy to install and start with
- Something that still complies with the rules of responsible disclosure

RTL-SDR comes to the rescue!



HACKTIVITY

RTL-SDR 101

- Cheap Chinese USB DVB-T receivers use RTL2382U chip and some tuner (E4000 or R820T)

- It is possible to set the RTL2832U chip to output raw samples (8-bit, max. 2,5 MS/S)

- 24 MHz – 1766 MHz (R820T) 52 MHz – 2200 MHz (E4000)

- „Poor man’s SDR”

HACKTIVITY

The million dollar question

Is it compatible with the code released for the USRP in 2010?

YES

HACKTIVITY

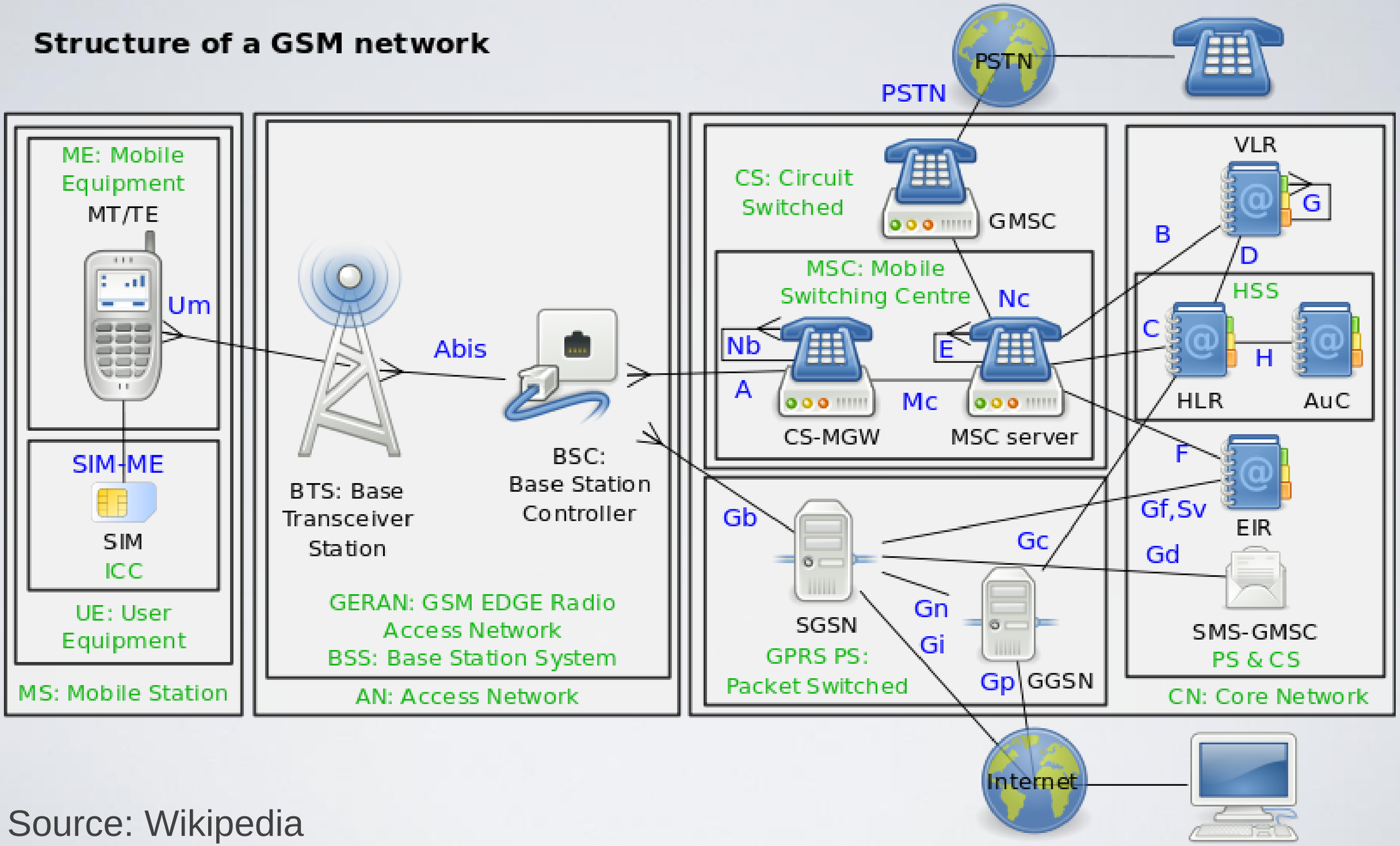
Did we achieve our goal?

- We have cheap hardware, relatively easy installation and code available

- It has limitations:
  - Only downlink
  - Only non-hopping cell
  - The radio needs some calibration

- Just enough limitations that it is safe to be released, but still fun to play with (remember responsible disclosure)

GSM 101



Source: Wikipedia

GSM 101

Terminology:

ARFCN – Absolute Radio Frequency Channel Number

Paging – the base-station pages (‚ARP-request') the ME

TDMA – Time Division Multiple Access

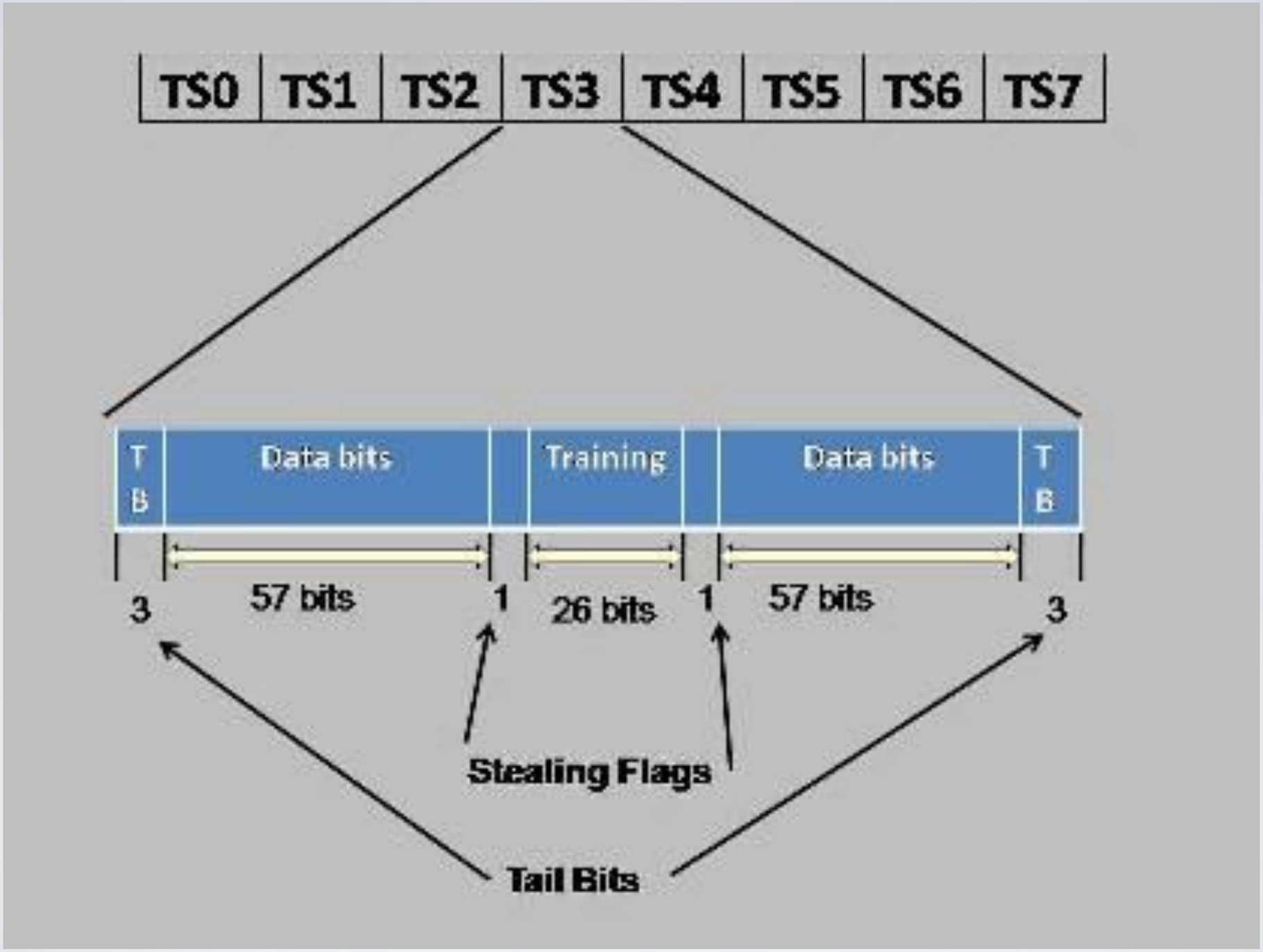
Timeslot – certain logical channels are transmitted at certain times (hence time division)

Burst – Data transmitted during one timeslot (148 bits usable data)

GSM 101

TDMA-frame

Burst



HACKTIVITY

GSM 101

Configuration:

- Timeslot 0 used as beacon/broadcast/signalling channel
- Timeslots 1-7 used for actual data transmission

There could be differences how logical channels organized, it depends on the cofiguration of the carrier.

GSM 101

Logical channels

Broadcast Channels (BCH)

Broadcast Control Channel (BCCH)

Frequency Correction Channel (FCCH)

Synchronization Channel (SCH)

Cell Broadcast Channel (CBCH)

Common Control Channels (CCCH)

Paging Channel (PCH)

Random Access Channel (RACH)

Access Grant Channel (AGCH)

Standalone Dedicated Control Channel (SDCCH)

Associated Control Channel (ACCH)

Fast Associated Control Channel (FACCH)

Slow Associated Control Channel (SACCH)

So how do we hack it?

1. Get into the same cell as the victim and uncover his/her TMSI (Temporary Mobile Subscriber Identifier)
2. Analyze how the cell is configured
3. Capture some data and based on your analysis create input for Kraken
4. After the key is cracked use it to decrypt the conversation

Getting into the same cell

- Using HLR queries (available online for 2-3 eurocents) you can usually get a rough location

- To get closer: we need to uncover the TMSI

- Technique is well known since 25c3

Uncovering TMSI - theory

- Send something to the victim (call/SMS)

- He/She will get paged

- Correlate the number of calls/SMS and their frequency with the paging observed

- Using silent text messages the victim won’t notice anythin

Uncovering TMSI - practice

- We need to simultaneously monitor the air (for pagings), send silent messages and correlate the data

- Architecture:
  Silent SMS sender, Correlator, Pagings monitor

- Android phone, PC, OsmocomBB
- Android phone, PC, RTL-SDR

SilentSMS

HACKTIVITY

Theory of cracking GSM

- Idea: known-plaintext attack

- GSM sends periodically the same messages over the air (mainly System Information), even when encryption is turned on

- Encryption: Keystream XOR Plaintext

- Keystream could be recovered → input for Kraken

Practical problems

- The hard part is to determine which messages contain known-plaintext because there is no differentiator (WiFi: packet length helps a lot – GSM: every burst has the same length)

- Messages arrive periodically, so we can make assumptions like „every third message will be a System Information 1 message”

Kraken

- Tool created by Frank A. Stevenson (DVD-Content Scramble System)

- Uses 2 TB of rainbow-tables to crack GSM

- If you would not like to download the tables contact me, I have them ;-), probably HSBP will have a copy too

- Cloud could be used (cloudcracker.com maybe)

Many thanks

- Vorex & Kaiyou (ZeroSMS - https://github.com/virtualabs/ZeroSMS)
- Dnet (NFCat - https://github.com/dnet/NFCat)
- Srlabs (Karsten Nohl) for airprobe and the rainbow tables
- Harald Welte and Dieter Spaar
- Frank A. Stevenson for Kraken
- rtl-sdr.com blog
- Nico Golde for being patient with me :-)

- Cheers to: Camp0, HSBP

HACKTIVITY

Links

All code used will be / is already released:
https://github.com/domi007

Introduction to GSM, main source of my images and theoretical explanations:
http://web.ee.sun.ac.za/~gshmaritz/gsmfordummies/intro.shtml

Osmocom project:
http://osmocom.org/

Srlabs's tutorial on GSM-cracking with USRP/SDR:
https://srlabs.de/decrypting_gsm/

2010 Blackhat, a complete walkthrough from Karsten Nohl about GSM sniffing and cracking:
https://www.youtube.com/watch?v=0hjn-BP8nro

Some more information on my blog:
http://domonkos.tomcsanyi.net

HACKTIVITY

Q & A

HACKTIVITY

Thank you for your attention!

Domonkos P. Tomcsanyi
domi@tomcsanyi.net
PGP:
811C 3FC3 CFCB 16E4 BAEB F5FB 7440 DF59 E271 2651

HACKTIVITY