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

Domi Tomcsanyi

GSM – what happened?

- Well known results – Karsten Nohl and his team
- Slowly going forward from year to year
  - 2010 – with a USRP it is possible to sniff downlink data, Kraken program can crack it with rainbowtables – code released
  - 2011 – OsmocomBB comes into play – full down and uplink sniffing, code NOT released

Why?

- GSM is broken, people need to know
- How to get the word out to people?
  - Let as many of them as possible play with GSM
  - Just like with WiFi and WEP
- But either the hardware is too expensive (USRP) or there is not much of code released
- RTL-SDR is the savior

RTL-SDR

- 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"

The million dollar question

- Is it compatible with the code already released for USRP?

YES

So what do we have?

- We have cheap hardware and we have code that is released to the public
- 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

GSM 101

- ARFCN: Absolute Radio-Frequency Channel Number – frequency
- Many many channels:
  - Beacon channel: pagings, system information
  - Traffic channel: carries actual data

http://web.ee.sun.ac.za/~gshmaritz/gsmfordummies/tdma.shtml

Steps to crack GSM

- Uncover TMSI (having only the target's phone number)
- Look at the data to determine the input for Kraken
- Crack the key using Kraken
- Use the key to decode the conversation

TMSI uncovering

- HLR query
- Silent SMS

- Technique is well known since 25C3

Data analysis & Kraken

- Idea: known-plain text attack
- It could be done manually, but it is hard and requires knowledge
- Kraken: 2 TB of data
  - Cloud could be used (e.g. Windows Azure)
  - Cludcracker.com contacted
- It will not be presented today

Getting the key from a SIM card

- To analyse data we need the Kc (session key)
- It could be extracted from a SIM card using a simple smart-card reader

What else?

- If you have a key that is being recycled…
  - Nico Golde's Paging attack on SMS (29C3)

Big thanks

- Vorex & Kaiyou (ZeroSMS - https://github.com/virtualabs/ZeroSMS)
- Dnet (NFCat - https://github.com/dnet/NFCat)
- Srlabs for airprobe and the rainbow tables
- Harald Welte
- Frank A. Stevenson for Kraken
- rtl-sdr.com blog
- Nico Golde
- For your attention

Domi Tomcsanyi

domi@tomcsanyi.net

PGP:

811C 3FC3 CFCB 16E4 BAEB F5FB 7440 DF59 E271 2651