Is GSM hacked?

GSM security: a state-of-affairs

Digital Security group - Radboud University Nijmegen

Fabian van den Broek – f.vandenbroek@cs.ru.nl

Bold claims in media

deVolkskrant
GSM-encryptie gekraakt

The New York Times
Cellphone Encryption Code Is Divulged

Possible impact

- Tan codes sent by SMS in Internet banking
- DigiD authentication, also by SMS
  (patient's access to EPD data was cancelled)
- Confidentiality of phone conversations

Ingredients seem to be available

- Hardware (available for around €1000,-):
  - a USRP, Universal Software Radio Peripheral
  - a daughterboard extension capable of receiving the GSM spectrum
  - an antenna
- Software (freely available open-source):
  - GNU Radio `http://gnuradio.org/`
  - AirProbe `https://svn.berlin.ccc.de/projects/airprobe/`
  - Kraken `http://reflextor.com/trac/a51`
- Data (shared via bittorrent):
  - reverse lookup tables currently 1.7TB (`http://reflextor.com/e100torrents/`)

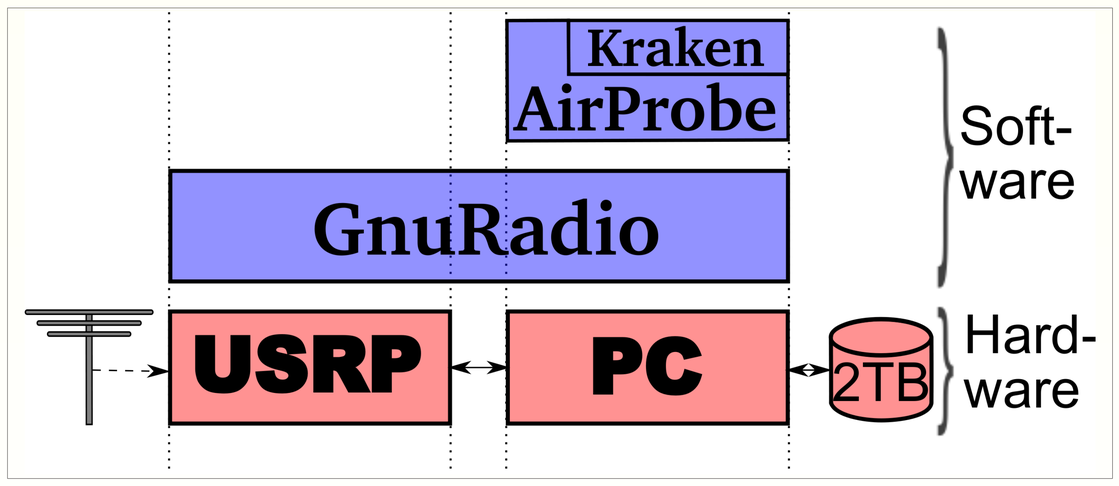


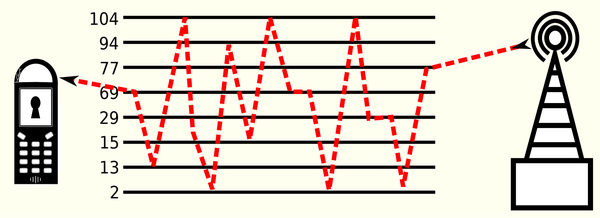
Figure 1: Architecture for an eavesdropping attack.

Problems with GSM security

- The GSM network does not authenticate itself to the user/phone.
- Use of weak encryption algorithms.
  (and using the same session key irrespective of the cipher being used)

Experimental results

- Nokia 3310 useful for studying real-life GSM traffic
- Eavesdropping with open-source tools still not possible due to *frequency hopping*



- Some Man-In-The-Middle attacks are feasible using open-source tools

Countermeasures

- Use A5/3 encryption
  offers no protection against MITM attacks
- Avoid unnecessary known plaintext
  only protects against rainbow table attack
- Switch to UMTS
  dependent on available coverage