GSM Fun by

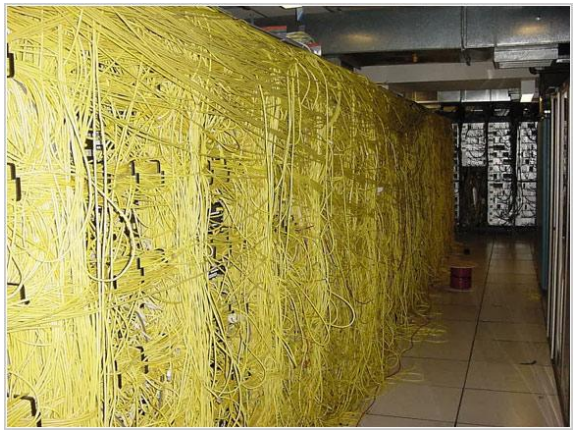
Nicolas Krassas, CISSP.
krasn@deventum.com
twitter.com/dinosn

About:me

- Security Researcher

- Pen-tester

- System/network administrator



GSM

- Global System for Mobile Communications, originally Groupe Spécial Mobile.
- Developed as a replacement for first generation analog cellular networks.
- The GSM Association estimates that technologies defined in the GSM standard serve 80% of the global mobile market.
- The GSM standard is succeeded by the third generation (3G , UMTS)

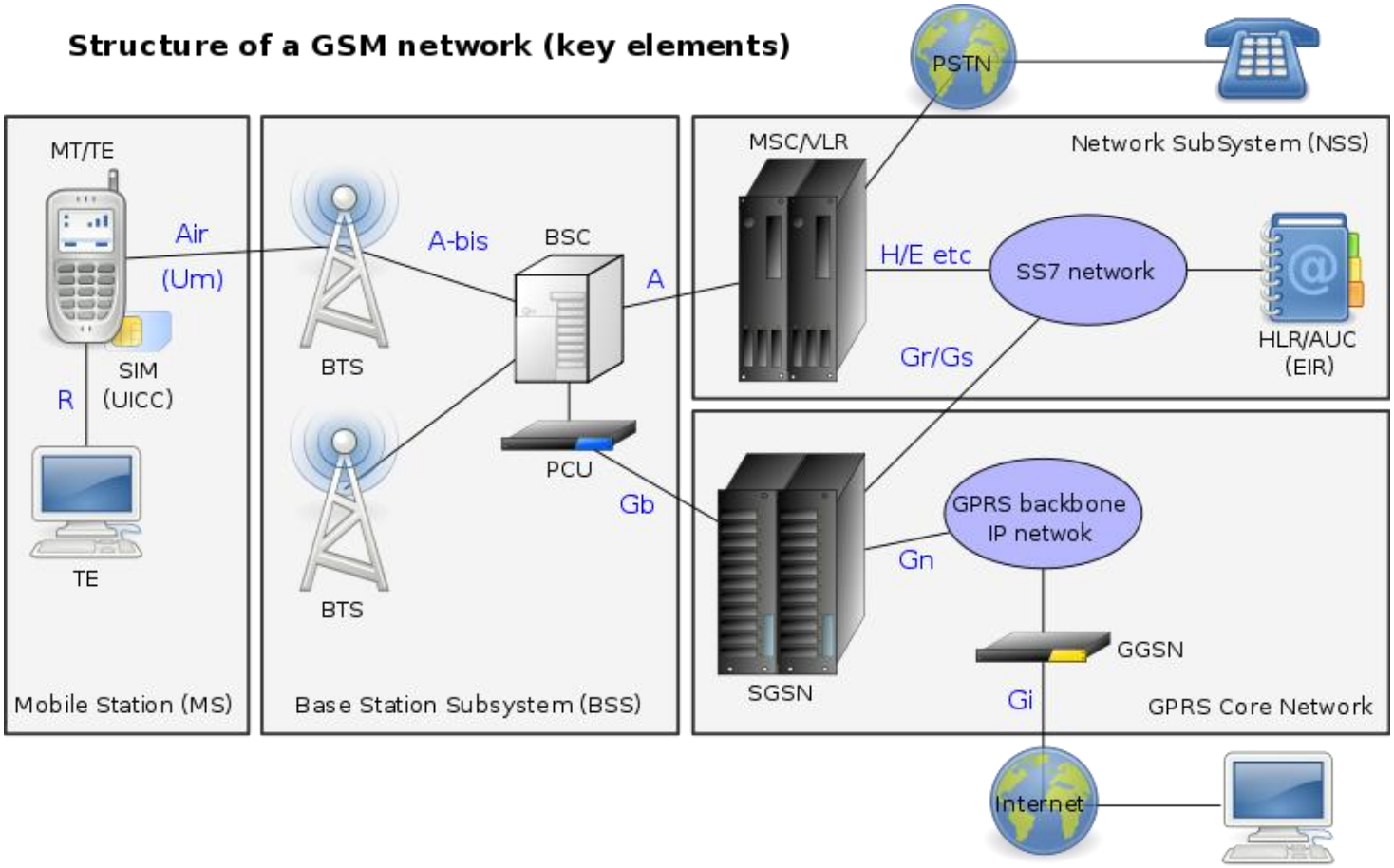
GSM

- GSM is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity.
- GSM networks operate in a number of different carrier frequency ranges, with most 2G GSM networks operating in the 900 MHz or 1800 MHz bands. Where these bands were already allocated, the 850 MHz and 1900 MHz bands were used instead (for example in Canada and the United States)

GSM Network structure

- The Base Station Subsystem (the base stations and their controllers).
- The Network and Switching Subsystem (the part of the network most similar to a fixed network). This is sometimes also just called the core network.
- The GPRS Core Network (the optional part which allows packet based Internet connections).
- The Operations support system (OSS) for maintenance of the network.

GSM Network structure



Subliminal message

- USE 3G

GSM Open Source Software

- gsmd daemon by Openmoko
- OpenBTS develops a Base transceiver station
- OpenBSC is developing a minimalistic, self-contained GSM network
- The GSM Software Project aims to build a GSM analyzer for less than $1000
- OsmocomBB developers intend to replace the proprietary baseband GSM stack with a free software implementation

USRP

- Universal Software Radio Peripheral
- Four high-speed analog-to-digital converters, each capable of 64 MS/s at a resolution of 12-bit, 85dB SFDR (AD9862).
- Four high-speed digital-to-analog converters, each capable of 128 MS/s at a resolution of 14-bit, 83dB SFDR (AD9862).
- An Altera Cyclone EP1C12Q240C8 FPGA.
- A Cypress EZ-USB FX2 High-speed USB 2.0 controller.
- 4 extension sockets (2 TX, 2 RX) in order to connect 2–4 daughterboards.
- 64 GPIO pins available through 4 BasicTX/BasicRX daughterboards (16 pins each).

USRP

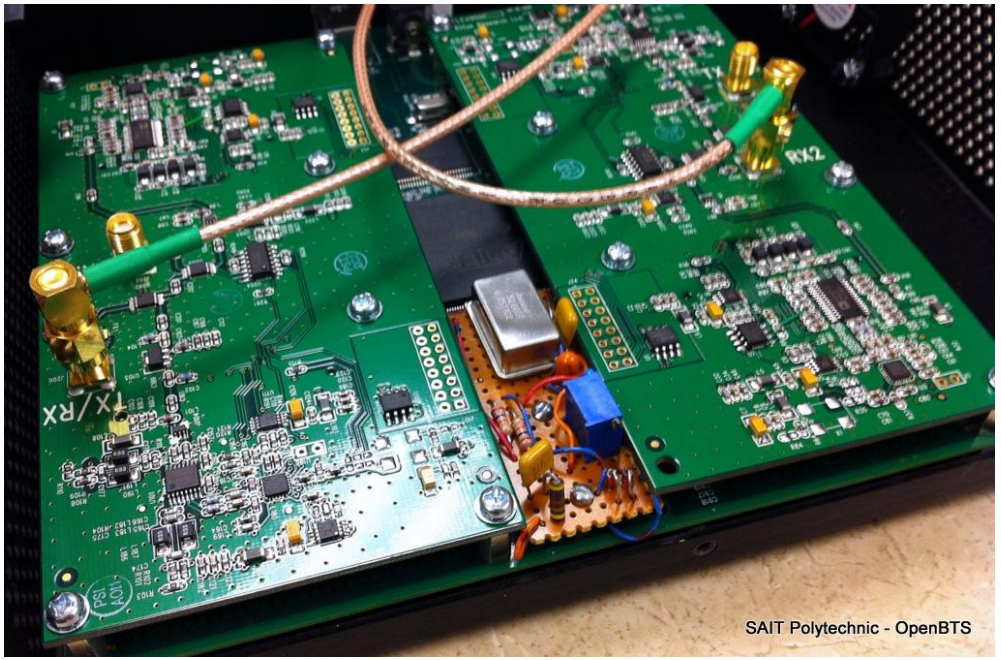
- Daughterboards
- Many to document here

USRP Uses

- An APCO25 compatible Transmitter/Receiver and Decoder
- RFID reader
- testing equipment
- a cellular GSM base station
- a GPS receiver
- an FM radio receiver
- an FM radio transmitter
- a digital television (ATSC) decoder
- passive radar
- synthetic aperture radar
- an amateur radio
- a teaching aid
- Digital Audio Broadcasting (DAB/DAB+/DMB) transmitter
- Mobile WiMAX receiver with USRP N2x0

My USRP

- “modified” 2x RFX900
- External clock FA-Synthesizer ‘FA-SY 1’ 1-160 MHz



USRP Modifications

- Hardware modifications to the USRP to use a external clock.
- Solder an SMA connector into J2001. This is the clock input. Be careful when soldering the SMA connector so you don't break the delicate trace from J2001 to C927.
- Move R2029 to R2030. This disables the onboard clock. R2029/R2030 is a 0-ohm resistor.
- Move C925 to C926.
- Remove C924.
- If you use external clock with CMOS output, then you have to add terminating 50 Ohm resistor to the USRP clock input.

USRP + GSM

- Presentation

Subliminal message

- USE 3G

USRP + GSM

USRP + GSM

- Hints

USRP + GSM

Detection

- A) Possibly slow network response
- B) Network Timeouts
- C) Caller ID is invalid
- D) No sms/gprs/mms functionality

Related work

- HOW to intercept the cell phone - SIM card communication and read out the Kc key for GSM traffic decryption (http://www.pittnerovi.com/jiri/hobby/electronics/gsm/index.html)
- GSM Hacking with USRP & Cracking A5 GSM Encryption (http://www.uaehackers.com/2009/09/gsm-hacking-with-usrp.html) and others

Questions

GSM Fun by

Nicolas Krassas, CISSP.
krasn@deventum.com
twitter.com/dinosn