SYNACKTIV
DIGITAL SECURITY

Mobile Security

Practical attacks using cheap equipment

Presented the 07/06/2016

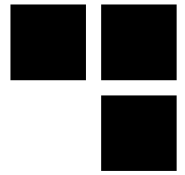
For Business France

By Sébastien Dudek

Content

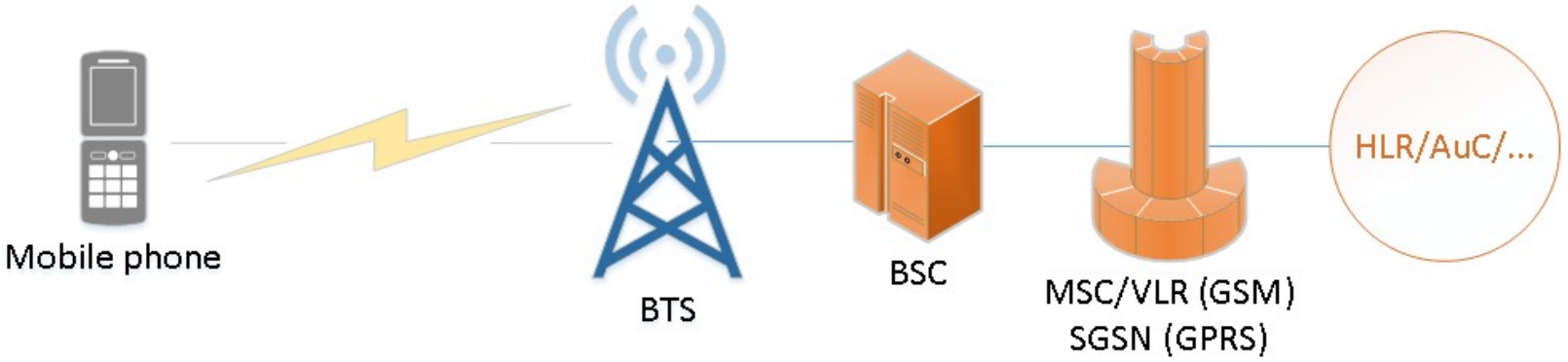
- **Security measures**
- **Recent publications in the hacking community**
- **Practical attacks**
- **Results of our short researches**

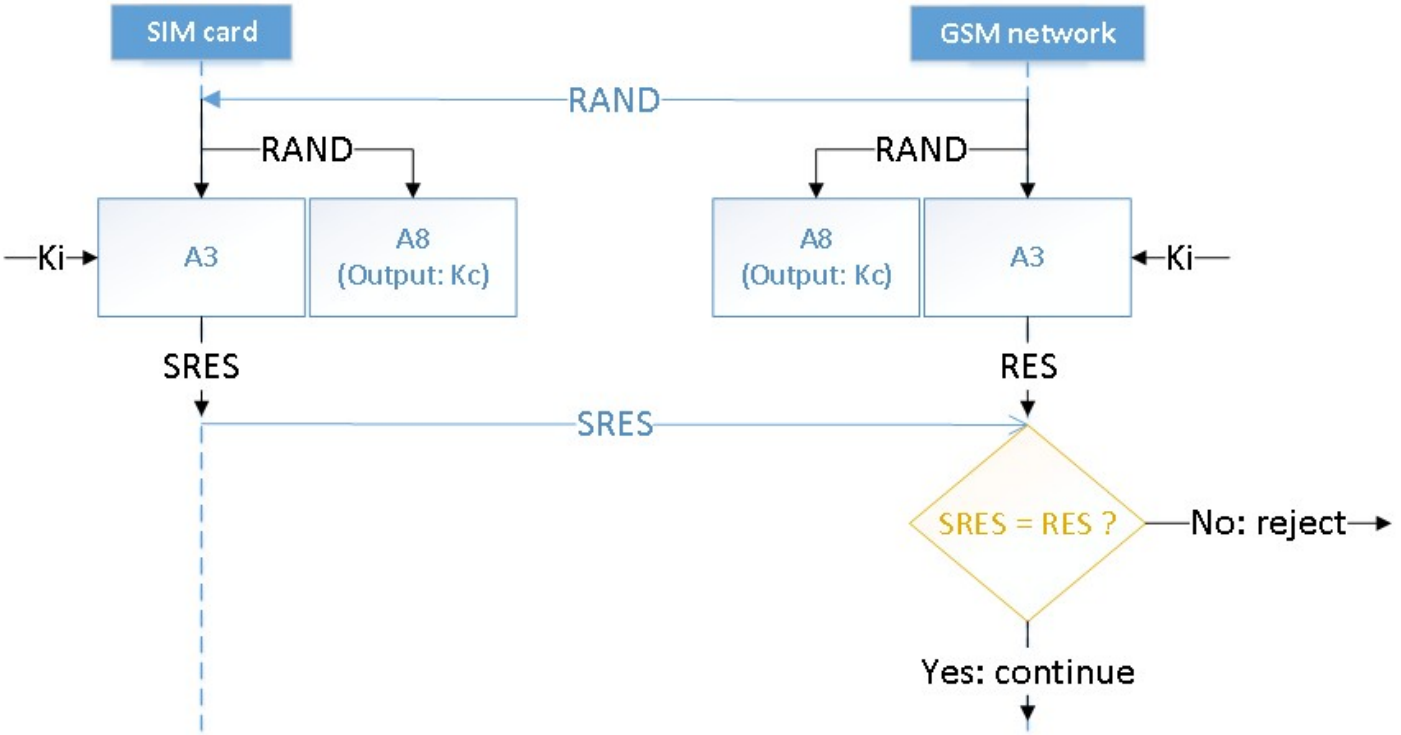
GSM and GPRS: confidentiality



- **GPRS → authentication algorithm A3/A8**
- **Communication ciphered with A5/1 algorithm with a K_c key (derived from K_i)**
- **K_c is generated with the A8 Algorithm**
- **The K_i key is stored in the AuC (Authentication Center) and SIM (Subscriber Identity Module)**

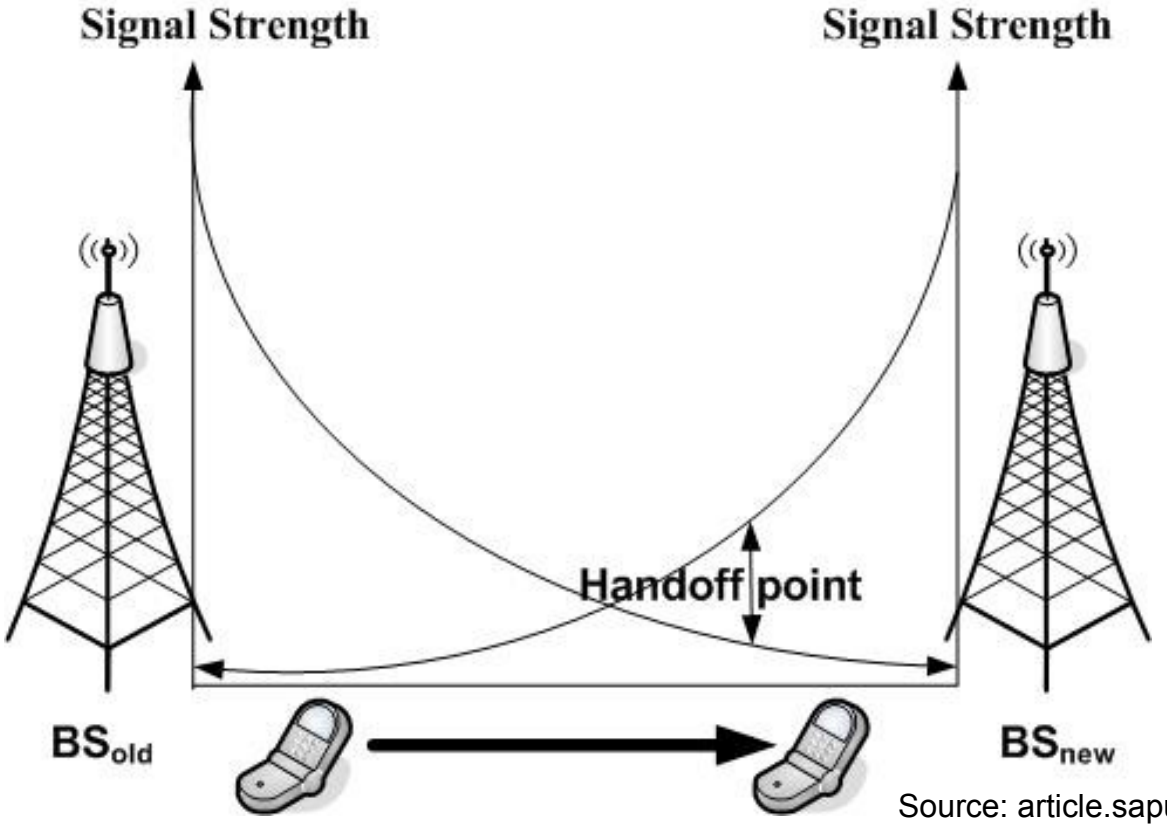
GSM and GPRS: architecture





- BTS: Base Transceiver Station
- BSC: Base Station Controller
- MSC: Mobile Switch Center
- VLR: Visitor Location Register
- HLR: Home Location Register
- AuC: Authentication Center

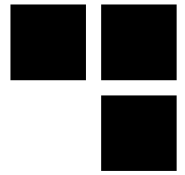
GSM and GPRS: Handover



Source: article.sapub.org

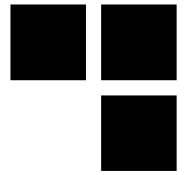
A stronger signal will likely attract User Equipments
→ Useful for attackers

GSM and GPRS: few differences



- **GPRS authentication → SGSN**
- **Ciphering in GSM is done at Layer 1 on the TCH (Traffic Channel) and DCCH (Dedicated Control CHannel)**
- **Ciphering in GPRS is done at Layer 2 LLC (Logical Link Control) with GEA1 algorithm**

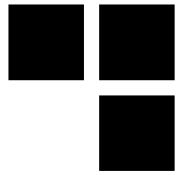
GSM and GPRS: possible attacks



- **No mutual authentication → Fake rogue BTS**
- **Reuse of Authentication triplet RAND, RES, K_c many times**
- **Signaling channel not encrypted → open for attacks**
- **Attacks on the A5/1 algorithm**
- **...**

⇒ Interception is possible on GSM and GPRS

3G/4G: advantages



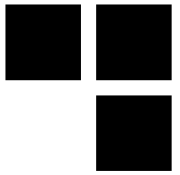
- **3G came with the KASUMI encryption algorithm**
- **Then SNOW-3G → second encryption algorithm for 3G, also used for 4G (in case KASUMI is broken)**
- **Additionally to SNOW-3G, 4G uses AES CBC 128 bits to cipher communications**
- **Thank to USIM → 3G and 4G network use mutual authentication**
- **But accesses to 3G networks are possible with previous SIM card → possible bypass of mutual authentication**
- **In 2011, ZUC algorithm has been introduced with 128 bits key**

⇒ Encryption algorithm is strong and mutual authentication make it difficult to intercept communications

Mobile interception: signal attraction

- **A User Equipment connects to the closer Base Station**
- **3G/4G downgrades to 2G via**
  - jamming attacks → a simple Gaussian noise in targeted channels
  - protocol attacks → difficult
  - baseband strange behaviors

State Of the Art: publications



- **Many publications exist:**
  - **Attacks on GSM A5/1 algorithm with rainbow tables**

    (at 26c3, Chris Paget and Karsten Nohl)
  - **OsmocomBB**

    (at 2010 at 27c3, Harald Welte and Steve Markgraf)
  - **Hacking the Vodaphone femtocell**

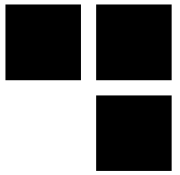
    (at BlackHat 2011, Ravishankar Borgaonkar, Nico Golde, and Kevin Redon)
  - **An analysis of basebands security**

    (at SSTIC 2014, Benoit Michau)
  - **Attacks on privacy and availability of 4G**

    (In October 2015, Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi and Jean-Pierre Seifert)
  - **How to not break LTE crypto**

    (at SSTIC 2016, Christophe Devine and Benoit Michaud)

State Of the Art: tools

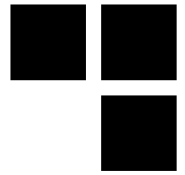


- **Hardware**
  - USRP from 700 € (without daughter-boards and antennas)
  - SysmoBTS from 2,000 €
  - BladeRF from 370 € (without antennas)
- **Software**
  - Setup a mobile network
    - OpenBTS: GSM and GPRS network compatible with USRP and BladeRF
    - OpenUMTS: UMTS network compatible with some USRP
    - OpenLTE: LTE network compatible with BladeRF and USRP
    - OpenAir: LTE network compatible with some USRP
    - YateBTS: GSM and GPRS network compatible with USRP and BladeRF
  - Analyze traffic
    - libmich: Analyze and craft mobile packets captured with GSMTAP
    - Wireshark: Analyze GSMTAP captured packets
    - OsmocomBB: sniff and capture GSM packets

Passive attacks in GSM

- **CCCH (Common Control Channels) give a lot of information**
  - Management messages, sometimes SMS in clear, TMSIs,...
- **CCCH → paging request → can be exploited to locate someone**
- **Tools**
  - OsmocomBB, Airprobe,...

Capture a specific channel (1)



- **List of ARFCN**

```
OsmocomBB# show cell 1
ARFCN   |MCC    |MNC    |LAC    |cell ID|forb.LA|prio   |min-db |max-pwr|rx-lev
-------+-------+-------+-------+-------+-------+-------+-------+-------+-------
   1    |208    |01     |0x     |0xe    |n/a    |n/a    |-110   |   5   |-71
   3    |208    |01     |0x     |0xb    |n/a    |n/a    |-110   |   5   |-76
   7    |208    |01     |0x     |0xa    |n/a    |n/a    |-110   |   5   |-74
  11    |208    |01     |0x     |0xe    |n/a    |n/a    |-110   |   5   |-75
  77    |208    |10     |0x     |0x9    |no     |normal |-105   |   5   |-84
 513DCS |208    |01     |0x     |0xd    |n/a    |n/a    | -95   |   0   |-82
 518DCS |208    |01     |0x     |0x5    |n/a    |n/a    | -95   |   0   |-79
 609DCS |208    |01     |0x     |0xf    |n/a    |n/a    | -95   |   0   |-70
 744DCS |208    |10     |0x     |0xe    |n/a    |n/a    | -95   |   0   |-91
 976    |208    |20     |0x     |0xc    |n/a    |n/a    |-104   |   5   |-81
 978    |208    |20     |0x     |0xc    |n/a    |n/a    |-104   |   5   |-79
 979    |208    |20     |0x     |0x0    |n/a    |n/a    |-104   |   5   |-84
 982    |208    |20     |0x     |0xc    |n/a    |n/a    |-104   |   5   |-74
 984    |208    |20     |0x     |0xc    |n/a    |n/a    |-104   |   5   |-57
 986    |n/a    |n/a    |n/     |n/a    |n/a    |n/a    |n/a    |n/a    |n/a
1011    |208    |20     |0x     |0x9    |n/a    |n/a    |-104   |   5   |-87
1012    |208    |20     |0x     |0xb    |n/a    |n/a    |-104   |   5   |-84
```

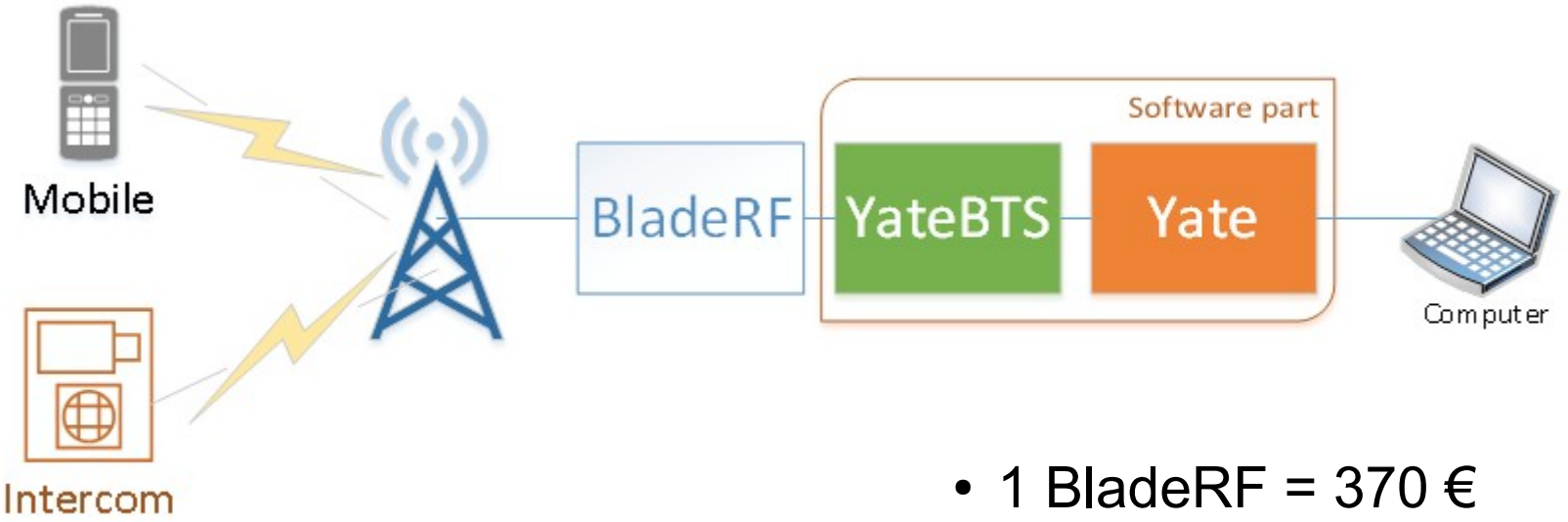
Capture a specific channel (2)

- **Leaked TMSI**

```
<0001> app_ccch_scan.c:312 Paging1: Normal paging chan tch/f to tmsi M(353       1)
<0001> app_ccch_scan.c:312 Paging1: Normal paging chan tch/f to tmsi M(116       0)
<0001> app_ccch_scan.c:312 Paging1: Normal paging chan tch/f to tmsi M(324       5)
<0001> app_ccch_scan.c:312 Paging1: Normal paging chan tch/f to tmsi M(331       4)
<0001> app_ccch_scan.c:312 Paging1: Normal paging chan tch/f to tmsi M(138       6)
<0001> app_ccch_scan.c:312 Paging1: Normal paging chan tch/f to tmsi M(893       )
<0001> app_ccch_scan.c:312 Paging1: Normal paging chan tch/f to tmsi M(131       )
<0001> app_ccch_scan.c:312 Paging1: Normal paging chan tch/f to tmsi M(596       )
<0001> app_ccch_scan.c:312 Paging1: Normal paging chan tch/f to tmsi M(324       5)
<0001> app_ccch_scan.c:312 Paging1: Normal paging chan tch/f to tmsi M(287       )
```

⇒ Use SMS Class-0 messages to track a user

GSM Lab setup: for interception



- 1 BladeRF = 370 €
- 2 Antennas = 15 € each
- YateBTS software = FREE
- **Total cost = 400 €**

GSM interception: User Equipment behaviors

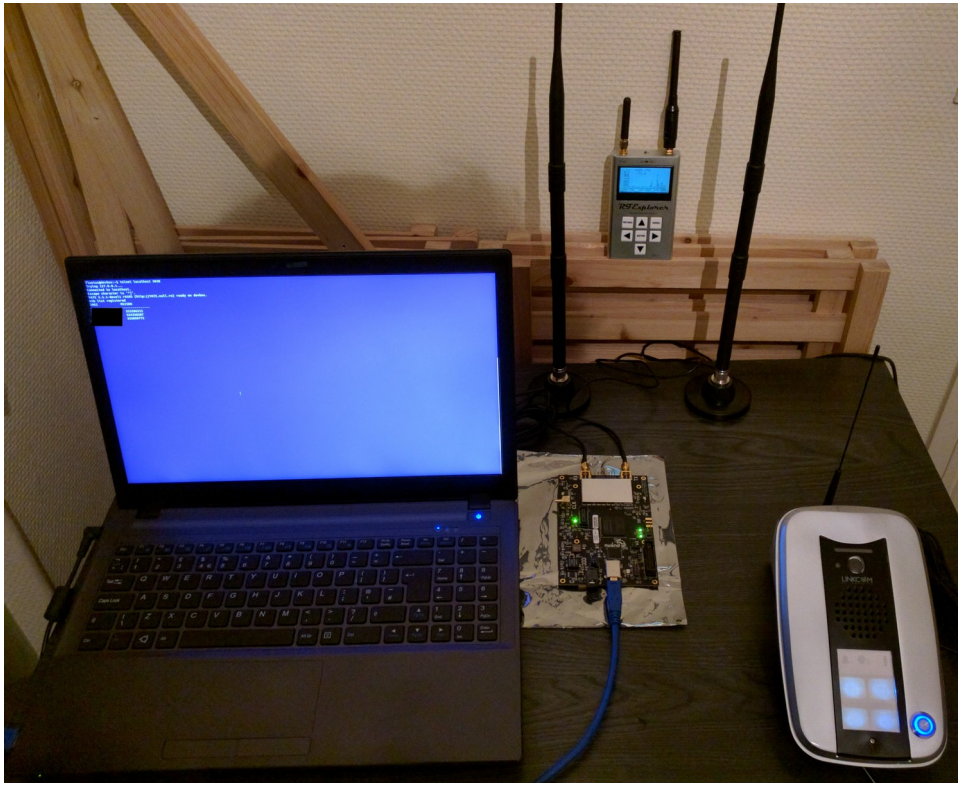
- **A User Equipment decide to register to another base station if**
  - it can register to any MCC/MNC BTS close to it
  - it can register to a test network close to it
  - only the current used network isn't reachable anymore, even if a rogue base station is closer
  - the signal is strong and the mutual authentication succeeded (not the case in GSM/GPRS)
- **Everything depends on the mobile stack implementations...**

Demo...

- **Fake Base Station**

Other vulnerable devices

- **Interception of Intercoms**



Results on intercoms

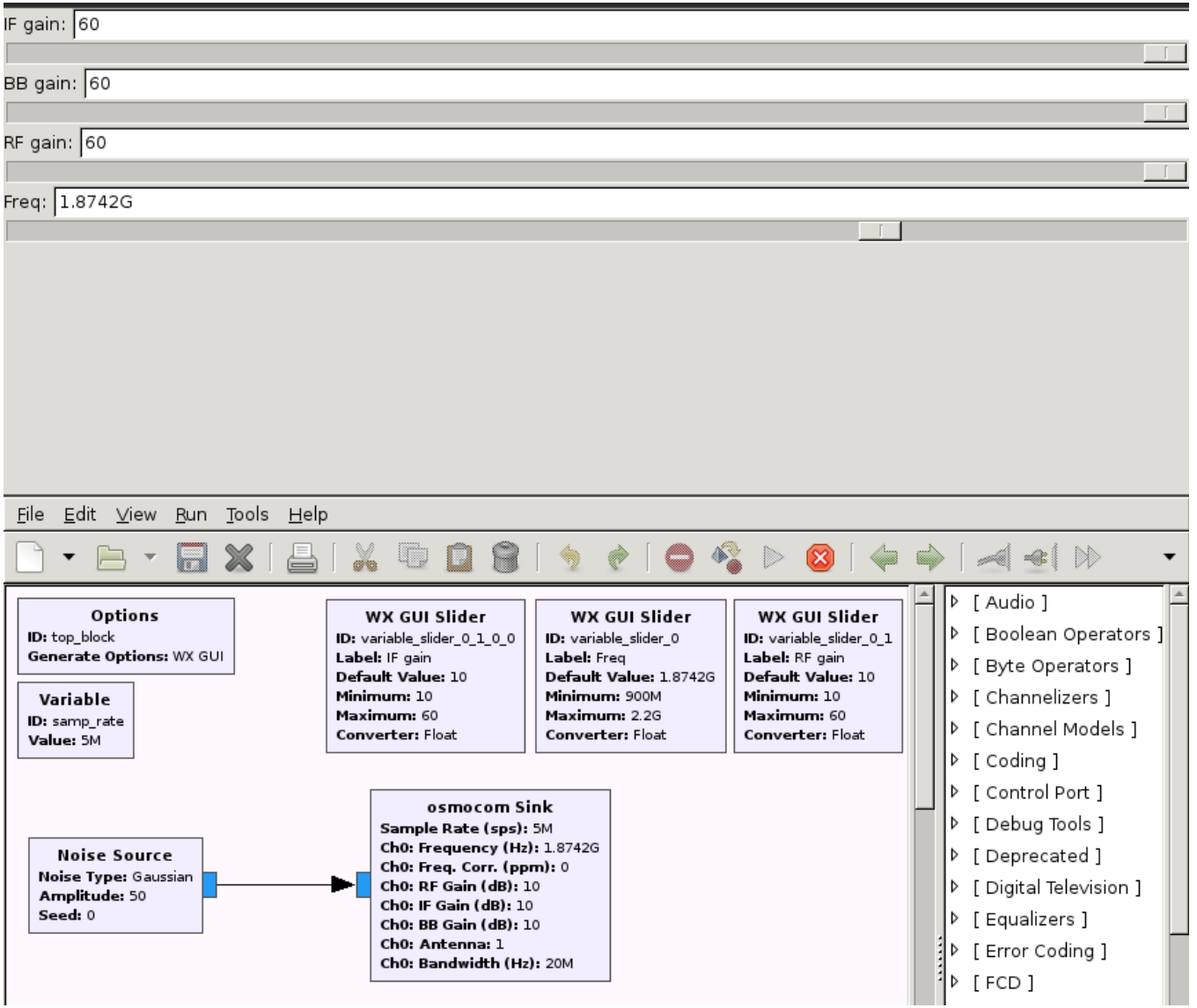
- **On a Link iDP GSM intercom**
  - leak of user phone numbers
  - send Intercom specific commands
  - send AT commands to interact with the targeted baseband
  - update users with premium rated numbers (e.g: Allopass)
- **Further work**
  - Reduce the model replacing the computed with a Raspberry Pi 3, or an ODROID device from about 50 €
  - Semi-automatic channel jamming on 3G
  - Study of protocol attacks on 3G and 4G

3G → 2G downgrade: hardware

- Downgrade is difficult with traditional jammers
- an attacker needs to focus to few specific bands → bands of the targeted operators
- A simple HackRF can

  be used (340 €)

Jamming video demo...

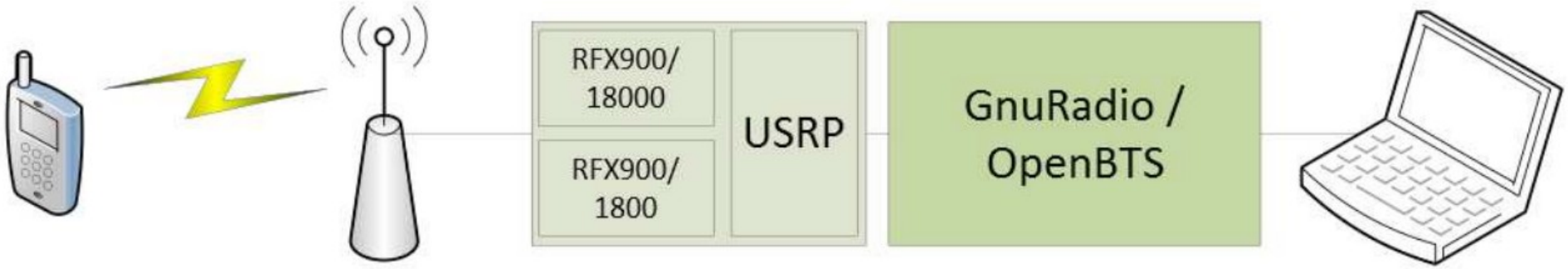


Alternatives to Jamming attacks

- **Protocol attacks on 4G and 3G**
  - using OpenLTE for 4G, or Open-UMTS for 3G
  - a compromized femtocell for 3G, and 4G femtocell
    → thanks to serial port, or unsecure update

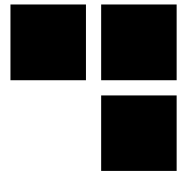
Lab setup: to find bugs

- **1 USRP: 700€**
- **2 daughter boards: about 120 € each**
- **2 TX and RX antennas: about 30€ each**
- **OpenBTS Software: Free**



Fuzzing lab in real

Fuzzing: our results



- **Made a fuzzing test framework *MobiDeke* (not released publicly)**
  - Results found on a HTC Desire Z
  - Found multiple application crashes

    Mostly Java exception → not exploitable
  - 1 exploitable vulnerability on SETUP CALLS handling → used to compromize the baseband
- **Presented at hack.lu conference in 2012 with Guillaume Delugré**

Conclusion

- **Attacks on GSM and GPRS are affordable: less than 1,000 €**
- **Attacks 3G and 4G are difficult, but**
  - mutual authentication could be bypassed depending on the baseband implementation
  - Publicly vulnerable femtocell can be found through Ebay (with serial ports, or unsecure download processes)
- **The IoT ecosystem uses a lot GSM and 3G stacks (for example digital intercoms) → vulnerable to the same attacks as traditional mobile devices**