



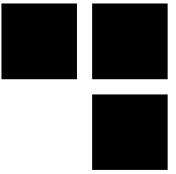
Intercoms Hacking

Call the Front Door and Install Your Back Door
(RELOADED!)

 Presented by Sébastien Dudek

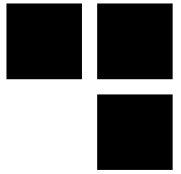


About me



- **Company: Synacktiv** (<http://www.synacktiv.com>)
- **Twitter: @fluxius**
- **Interests: radio-communications (Wi-Fi, RFID, GSM, PLC...), networking, web, Linux security... and intercoms!**
- **Do red team tests at Synacktiv:**
 - spear phishing,
 - remote and physical intrusion...





Red team tests at Synacktiv

- **Physical intrusions: we always need a way to enter to a building**
- **How?:**
 - lockpicking,
 - RF attacks,
 - or attacking Intercoms!

Intercoms today

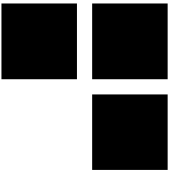


■ Features:

- Pass code
- RF tag access
- Call a resident:

The resident can then open the door

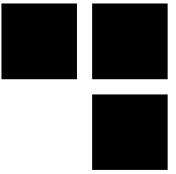
When calling a resident, this intercoms use the mobile network
→ that explains the (+33)6 prefix displayed on the resident's phone



Human curiosity...

- **Would it be possible to play with the intercom?**
- **We tried to directly call the intercom**
but the intercom doesn't answer to the call
- **Dump and modify the flash**
good option, but difficult to do without being spotted in the street...
- **A mobile attack → Better!**
but we need to understand the functioning of these intercoms first!

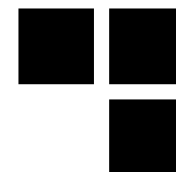
Context



- **Intercom / door phone / house intercom**
- **A voice communication device → within a building**
- **Numeric → Connected to the mobile network (SIM/USIM cards)**
- **Allows to call a resident to identify the visitor and open a door**

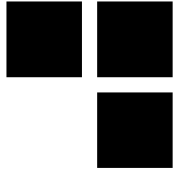
Different types of intercoms exist

Different types of intercoms



	Conventional	Simplified	Numeric
Description	Used for medium sized buildings	/	Medium sized building, or private residents
# of wires	4+n (2 for power, 2 for the door system and n → number of residents)	1 wire for power and door system + n → number of residents	No wires for resident

Numeric intercoms



Wires replaced by:

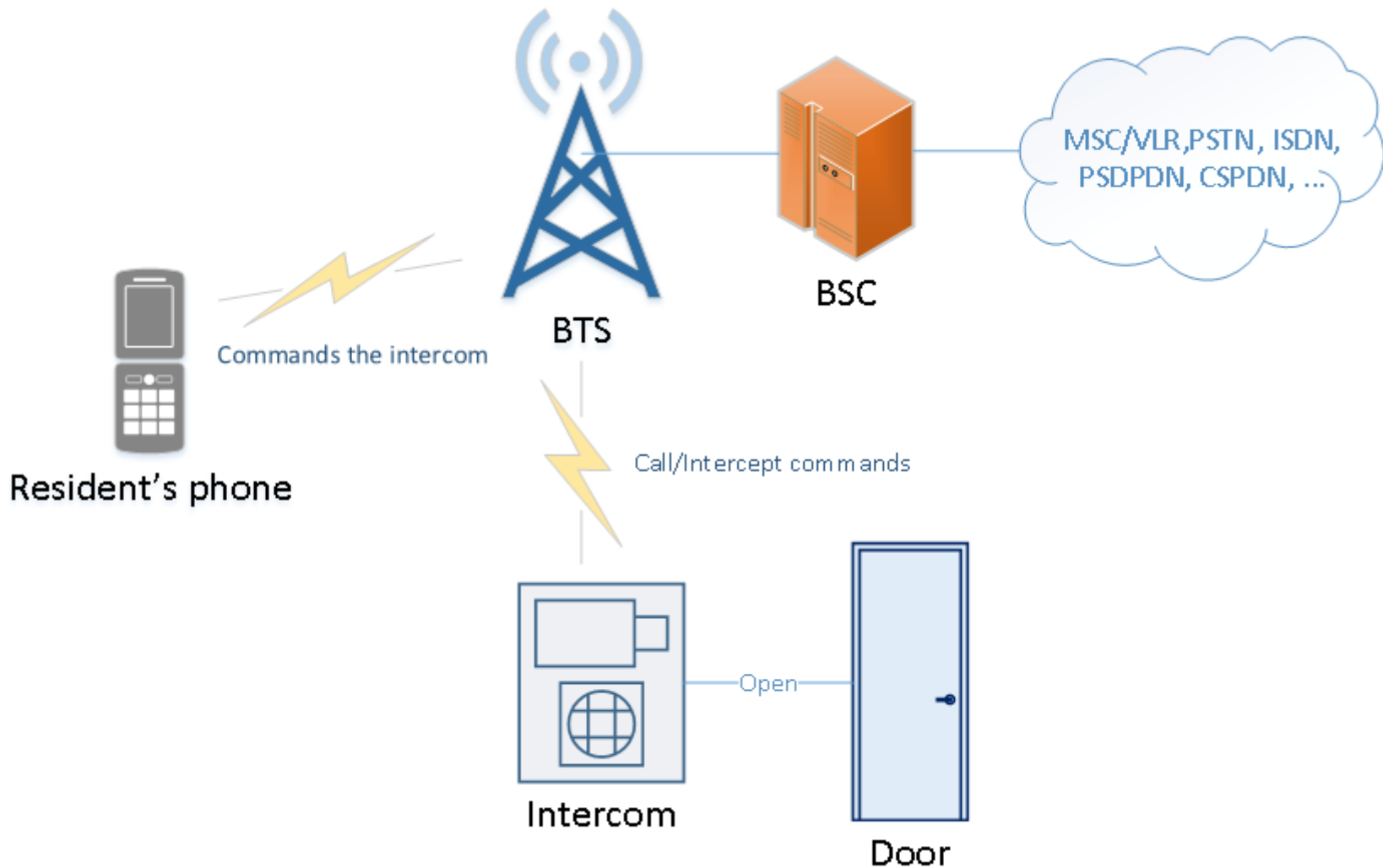
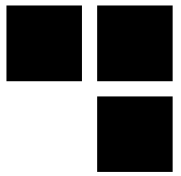
- GSM, 3G, rarely in 4G
- or a TCP/IP stack
- or Wi-Fi...



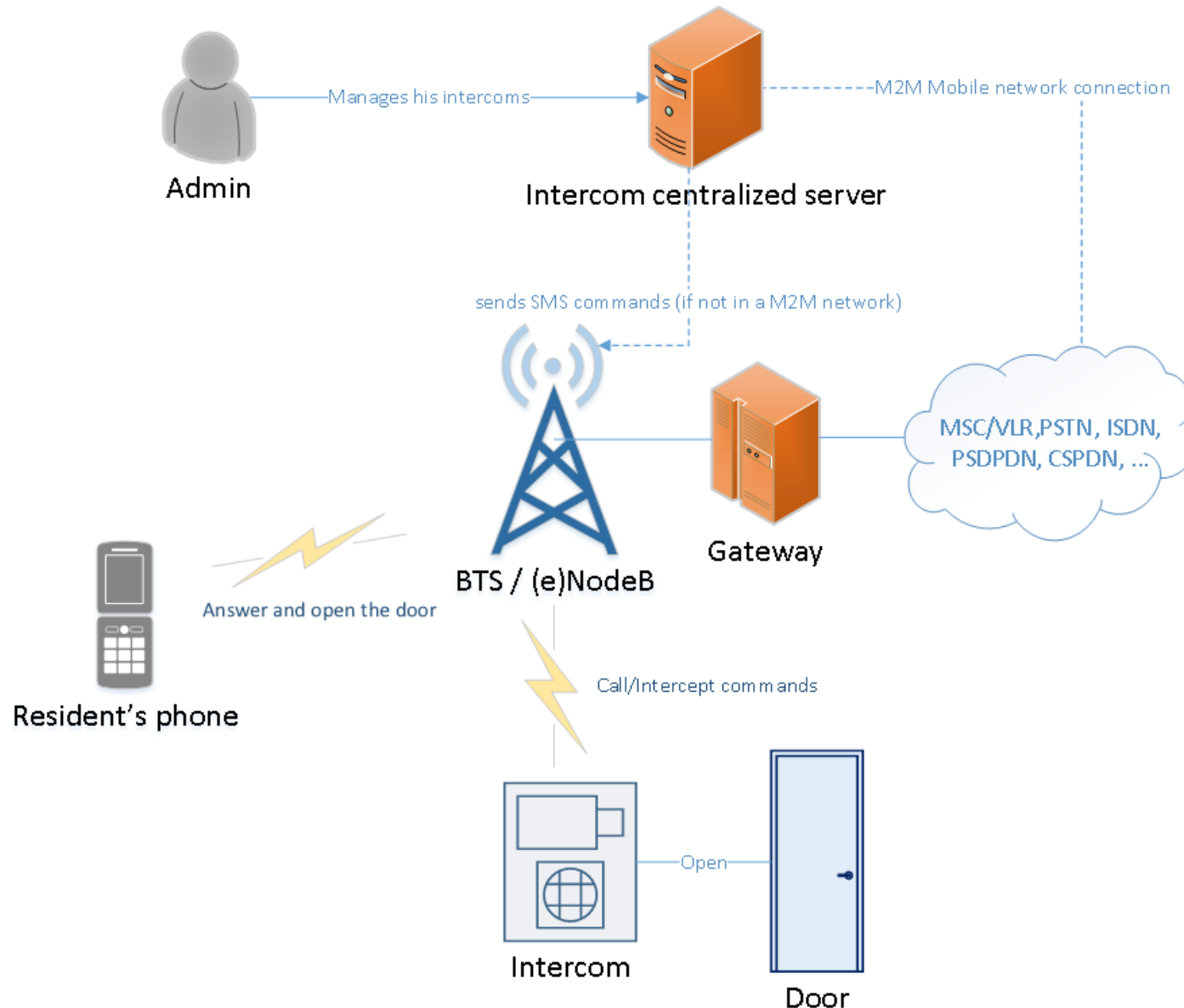
⇒ **Avoid complicated and cumbersome cables**

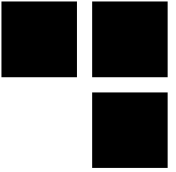
⇒ **Easy installation**

Numeric intercoms: simplified architecture



Network architecture with M2M





Different brands market

- **4 brands are well-known present in France:**

- Comelit
- Intratone
- Norasly
- Urmet Captiv... that cost ~2000€

- **Cheaper alternatives:**

- Linkcom → commonly used by private residents
→ Our choice for our 1st analysis

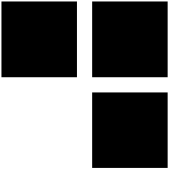
How to recognize a mobile intercom

- Not easy... maybe spotting a nice LCD screen, new stainless steel case...
- Or...



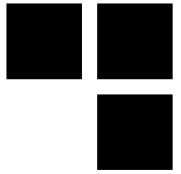
Looks like
a mobile
module?

State Of the Art: intercoms



- **Publications about intercoms are nearly nonexistent**
- **But research on mobile security can be applied to attack these devices...**

State Of the Art: Mobile security



- **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**

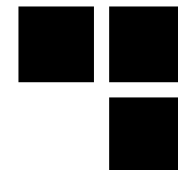
- (In October 2015, Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi and Jean-Pierre Seifert)

- **How to not break LTE crypto**

- (at SSTIC 2016, Christophe Devine and Benoit Michau)

- And many others...

State Of the Art: tools



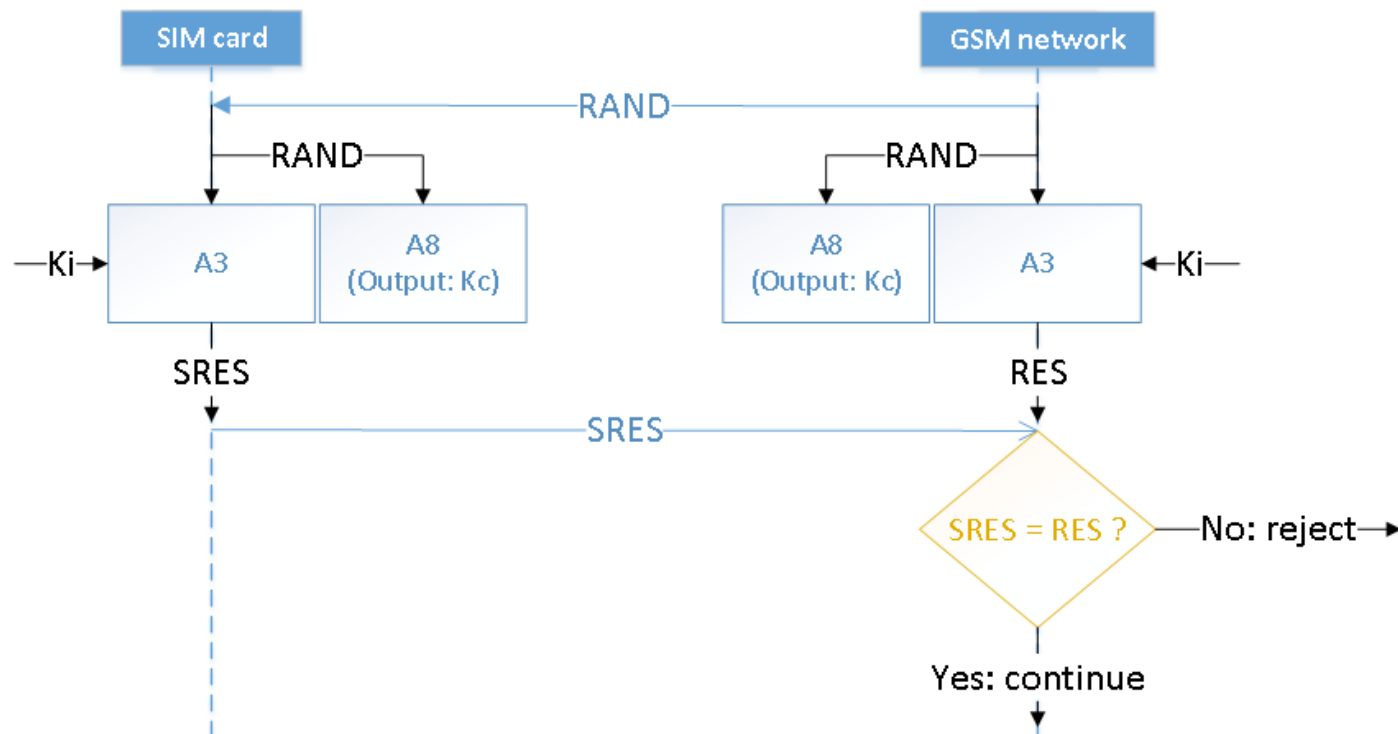
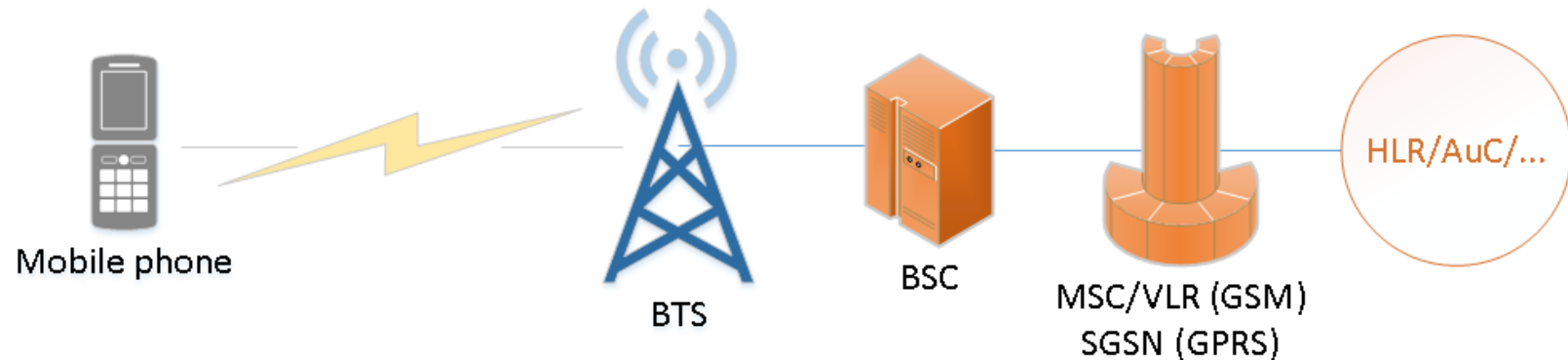
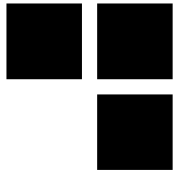
■ Hardware

- USRP from 700 € (without daughter-boards and antennas)
- SysmoBTS from 2,000 €
- BladeRF from 370 € (without antennas)

■ Software

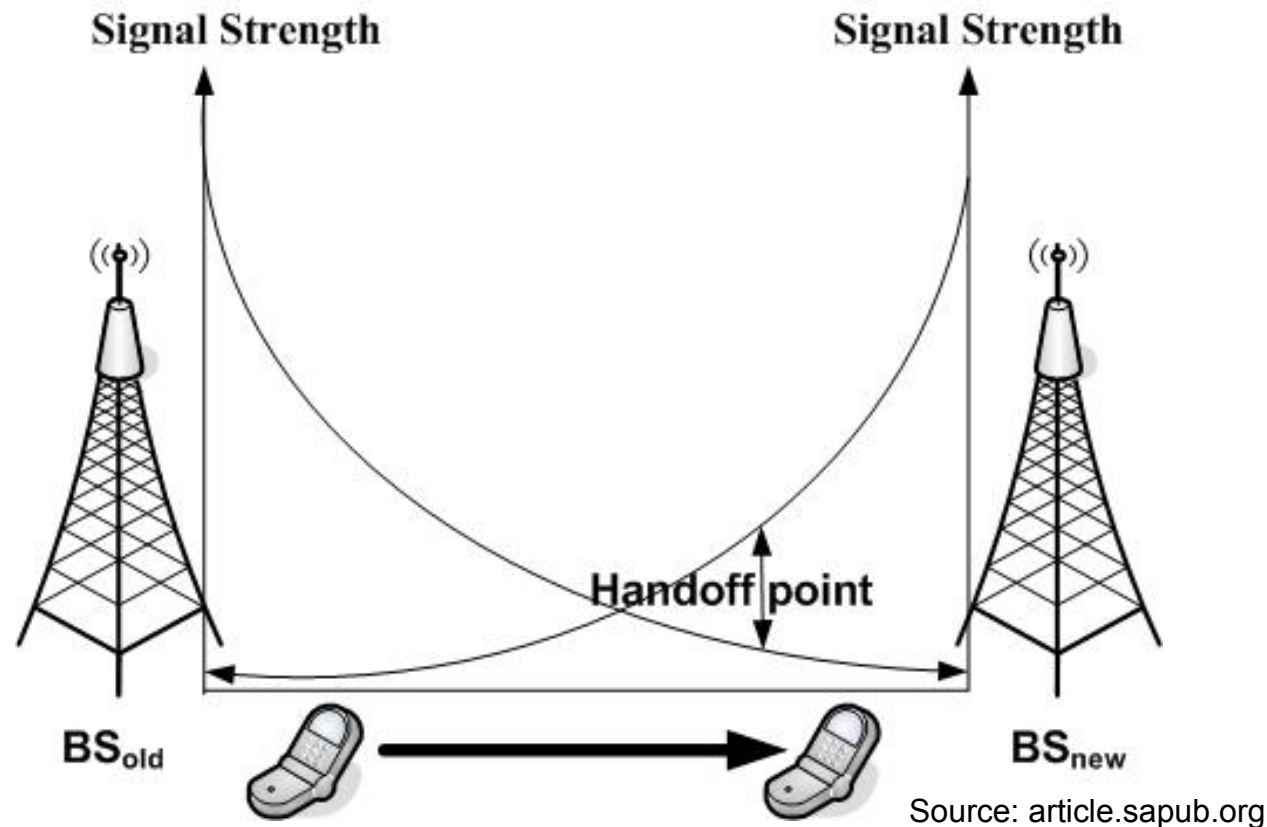
- Setup a mobile network
 - OpenBTS: GSM and GPRS network compatible with USRP and BladeRF
 - OpenUMTS: UMTS network compatible with some USRP
 - OpenLTE: LTE network compatible with BladeRF and USRP
 - OpenAir: LTE network compatible with some USRP
 - YateBTS: GSM and GPRS network compatible with USRP and BladeRF
- Analyze traffic
 - libmich: Analyze and craft mobile packets captured with GSMTAP
 - Wireshark: Analyze GSMTAP captured packets
 - OsmocomBB: sniff and capture GSM packets

GSM and GPRS: authentication



- 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



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

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

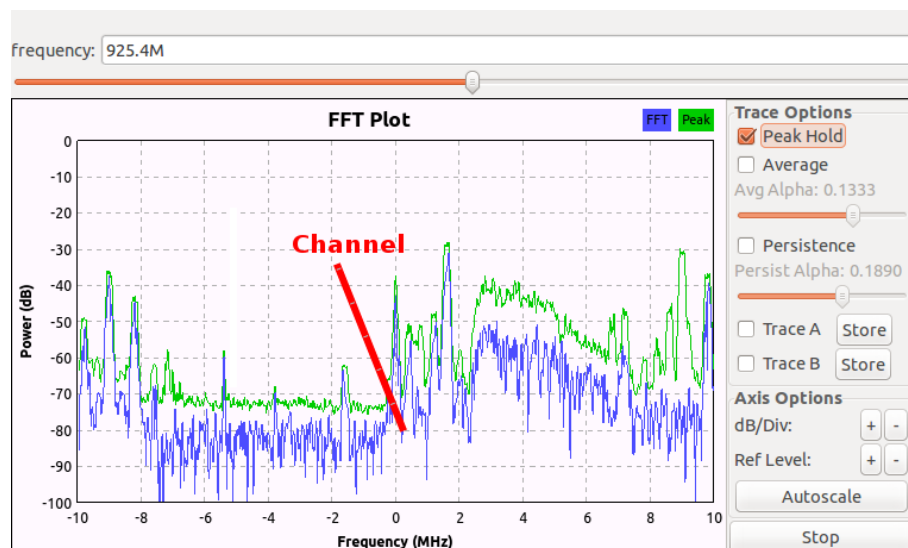
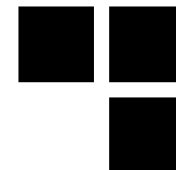


	GSM	3G	4G
Client authentication	YES	YES	YES
Network authentication	NO	Only if USIM is used (not SIM)	YES
Signaling integrity	NO	YES	YES
Encryption	A5/1	KASUMI SNOW-3G	SNOW-3G AES ZUC...

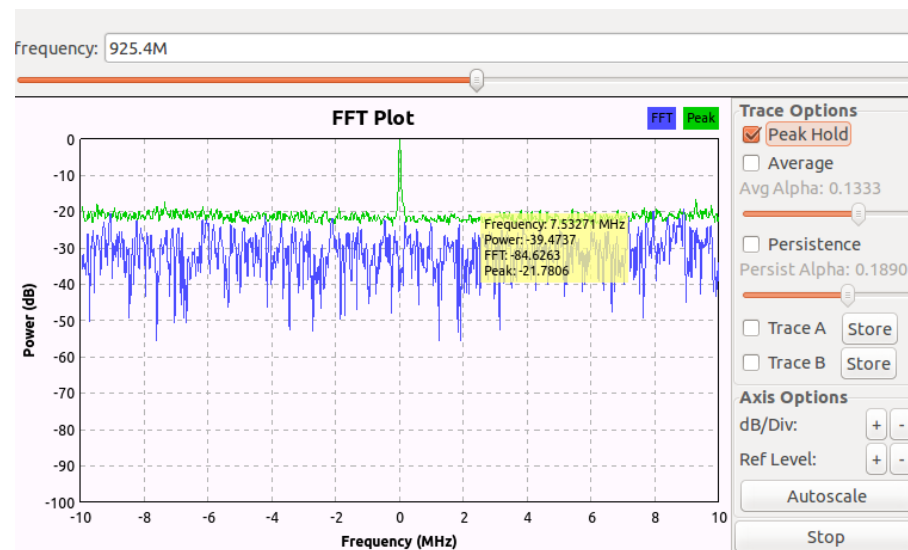
Mobile interception: signal attraction

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

Jamming is generally basic...

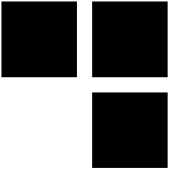


Before



After

The 3G module



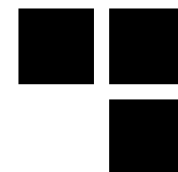
■ Found in a public documentation:

« Lorsque le réseau 3G est inexistant sur les lieux de l'installation, le bloc 3G cherchera le réseau GSM automatiquement et pourra résumer ses fonctionnalités dans ce mode :

- Appel Audio (sans Visio).
- Mise à jour en temps réel sur le réseau GSM et non plus 3G. »

= If 3G is unreachable → use 2G instead!

Downgrade 3G → 2G demo



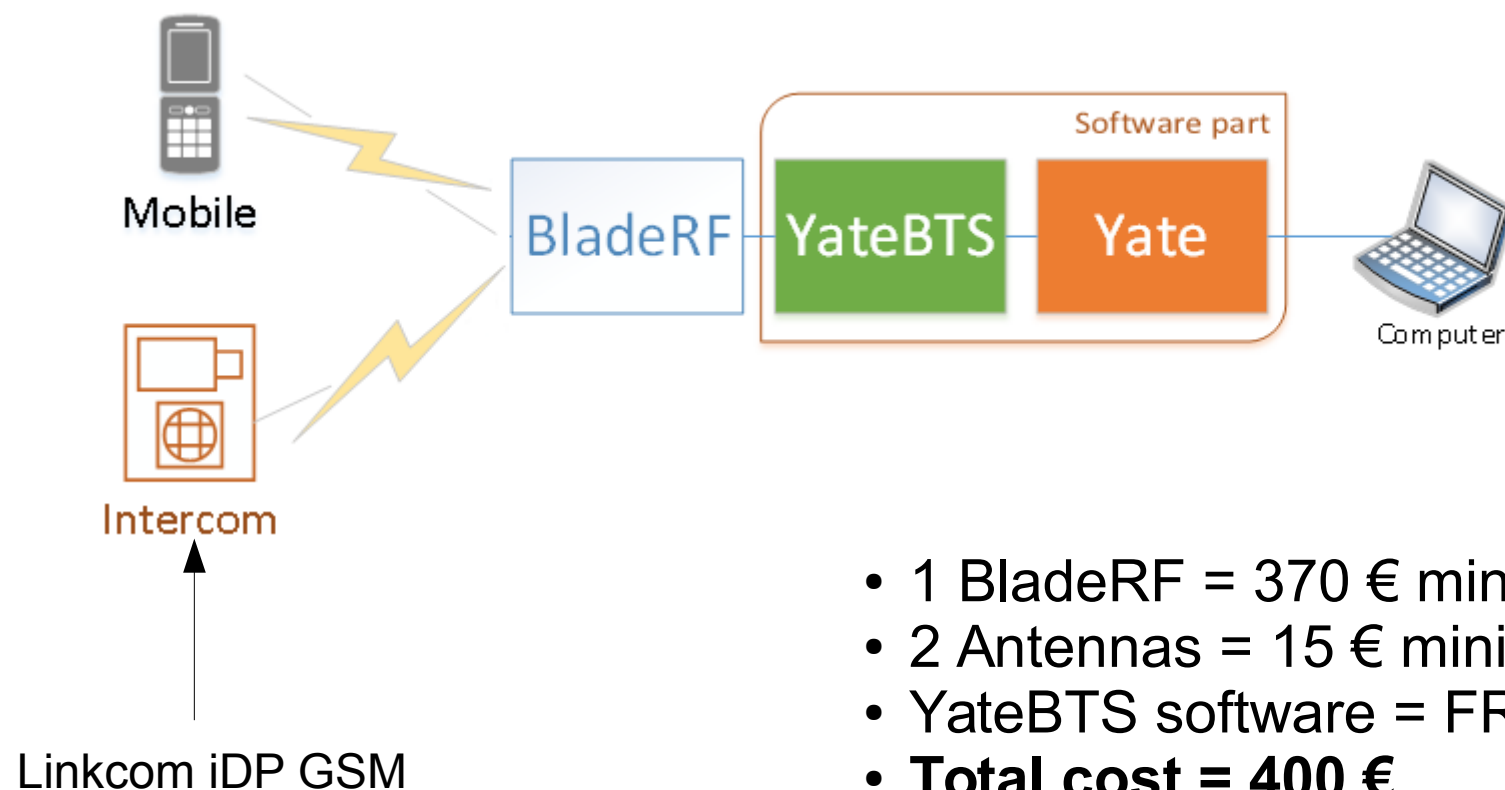
- Targeted channel jamming
- Using a simple HackRF for ~300€
 - works also with a USRP (~700€), or a bladeRF (~400€)

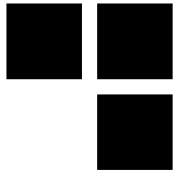


GSM Lab setup: for interception



No full duplex with hackRF → we use a bladeRF instead!

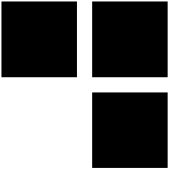




Intercom setup: configuration

- **This intercom can be configured in 3 ways:**
 - With a programming interface and the Link iDP manager software
 - With a SIM card reader/programmer
 - **Via SMS messages**
- **The SIM card is used as a memory → contains all the settings**
- **A first administrator number “ADMIN1” has to be setup in the SIM card contacts**

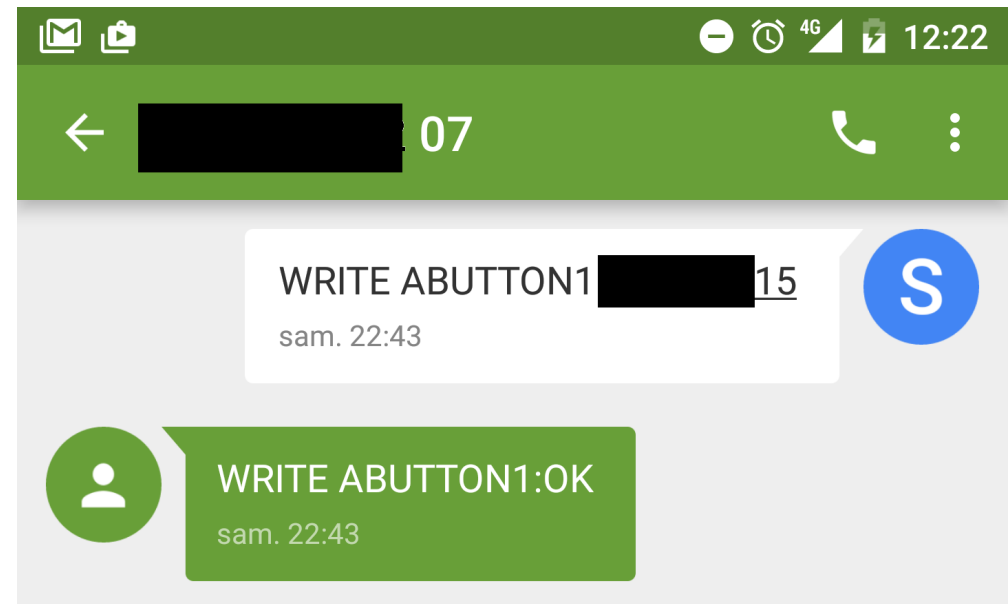
First impressions



■ Our goals:

- impersonate a number, or find a way to bypass it
- then open a door, or send commands to the intercoms
- ...

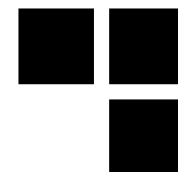
■ A good indicator → after sending commands, an acknowledgment is performed by SMS



Hypotheses as a potential attacker

- **We don't know the mobile operator**
- **We don't know intercom's number**
- **The commands could be found with public or leaked documentations, or by performing a firmware analysis**

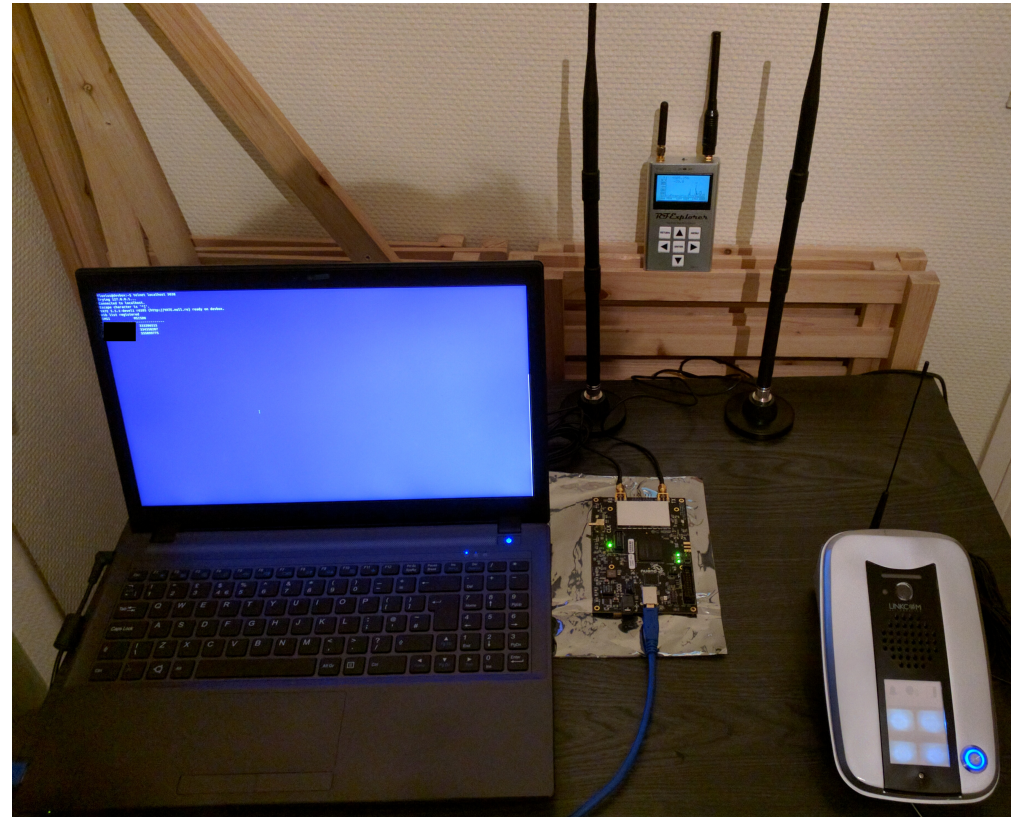
Attacker steps to open the door



- 1. Recognize intercom's operator to trap it**
- 2. Leak, or guess, numbers to impersonate**
- 3. Register my phone with the leaked resident number on the fake BTS**
- 4. Call myself**
- 5. Open the door!**

To trap the intercom

- Bruteforcing the 4 MCC/MNC
 - 15min~ waiting for each MCC/MNC
- Strong GSM signal
- Button push → calling intercepted → success!



Note: The used MCC/MNC but mostly the used channel can be discovered with jamming tests over the different channels.

What's next? Let's leak numbers!

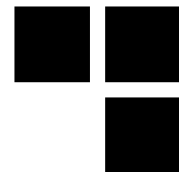
- Activate GSM tapping on YateBTS → Wireshark
- Then push on buttons → CC SETUP

84933	406.0349243...	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=1, N(S)=0(DTAP) (CC) Setup
84935	406.0384471...	127.0.0.1	127.0.0.1	LAPDm	81 S, func=RR, N(R)=1
84947	406.0571079...	127.0.0.1	127.0.0.1	LAPDm	81 I, N(R)=1, N(S)=1(DTAP) (CC) Call Proceeding
84955	406.0582432...	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI
84966	406.0760920...	127.0.0.1	127.0.0.1	LAPDm	81 U, func=UI

GSM Frame Number: 0	
Channel Type: FACCH/F (9)	
Antenna Number: 0	
Sub-Slot: 0	
Link Access Procedure, Channel Dm (LAPDm)	
Address Field: 0x01	
Control field: I, N(R)=1, N(S)=0 (0x20)	
Length Field: 0x49	
GSM A-I/F DTAP - Setup	
Protocol Discriminator: Call Control; call related SS messages (3)	
.... 0011 = Protocol discriminator: Call Control; call related SS messages (0x03)	
0... = TI flag: allocated by sender	
.000 = TIO: 0	
01.. = Sequence number: 1	
..00 0101 = DTAP Call Control Message Type: Setup (0x05)	
Source capability: 1 (No support for fast full rate speech version 1 and half rate speech version 1. MS has a greater preference)	
Called Party BCD Number - (515)	
Length: 6	
1... = Extension: No Extension	
.000 = Type of number: unknown (0x00)	
.... 0001 = Numbering plan identification: ISDN/Telephony Numbering (ITU-T Rec. E.164 / ITU-T Rec. E.163) (0x01)	
Called Party BCD Number: 515	

0000	00 00 00 00 00 00 00 00	00 00 00 00 08 00 45 00E.
0010	00 43 f7 4d 40 00 40 11	45 5a 7f 00 00 01 7f 00	.C.M@. EZ.....
0020	00 01 97 fc 12 79 00 2f	fe 42 02 04 01 04 40 00y./ .B....@.
0030	00 00 00 00 00 00 09 00	00 00 01 20 49 03 45 04 I.E.
0040	06 60 04 02 00 05 81 5e	5 f5 2b
0050	2b		..+

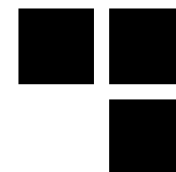
What's next? Let's open the door!



- Leaked number → affect it to your IMSI in *tmsidata.conf*

```
[tmsi]
last=007b0005
[ues]
20820XXXXXXXXXX=007b0003,35547XXXXXXXXXX,XXXXXX
515,1460XXXXXX,ybts/TMSI007b0003
# associating attacker IMSI with a resident number
[...]
```

What's next? Let's backdoor it!



- **Leak the admin number:**

- buttons (call, or alarm triggers, etc.)
- social engineering

- **Find commands:**

- public or leaked documentations
- Passive channel monitoring → good luck!
- or buy the same model in commercial web sites such “leboncoin”, eBay, and so on.

- **In our case with Linkcom iDP:**

Command	Description
READ <NAME>	Read the number of a button, or an admin (ADMIN[1-9]).
WRITE <NAME> <number>	Add or update a number associated to a name.
CAL AT<command suffix>	Send an AT command to the baseband through SMS!

Demo



- **Trapping an intercom**
- **Sending commands**

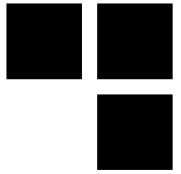
Call premium rate numbers

- We can modify a contact → why not choose a premium number?

- Allopass
- Optelo
- Hipay
- and so on.

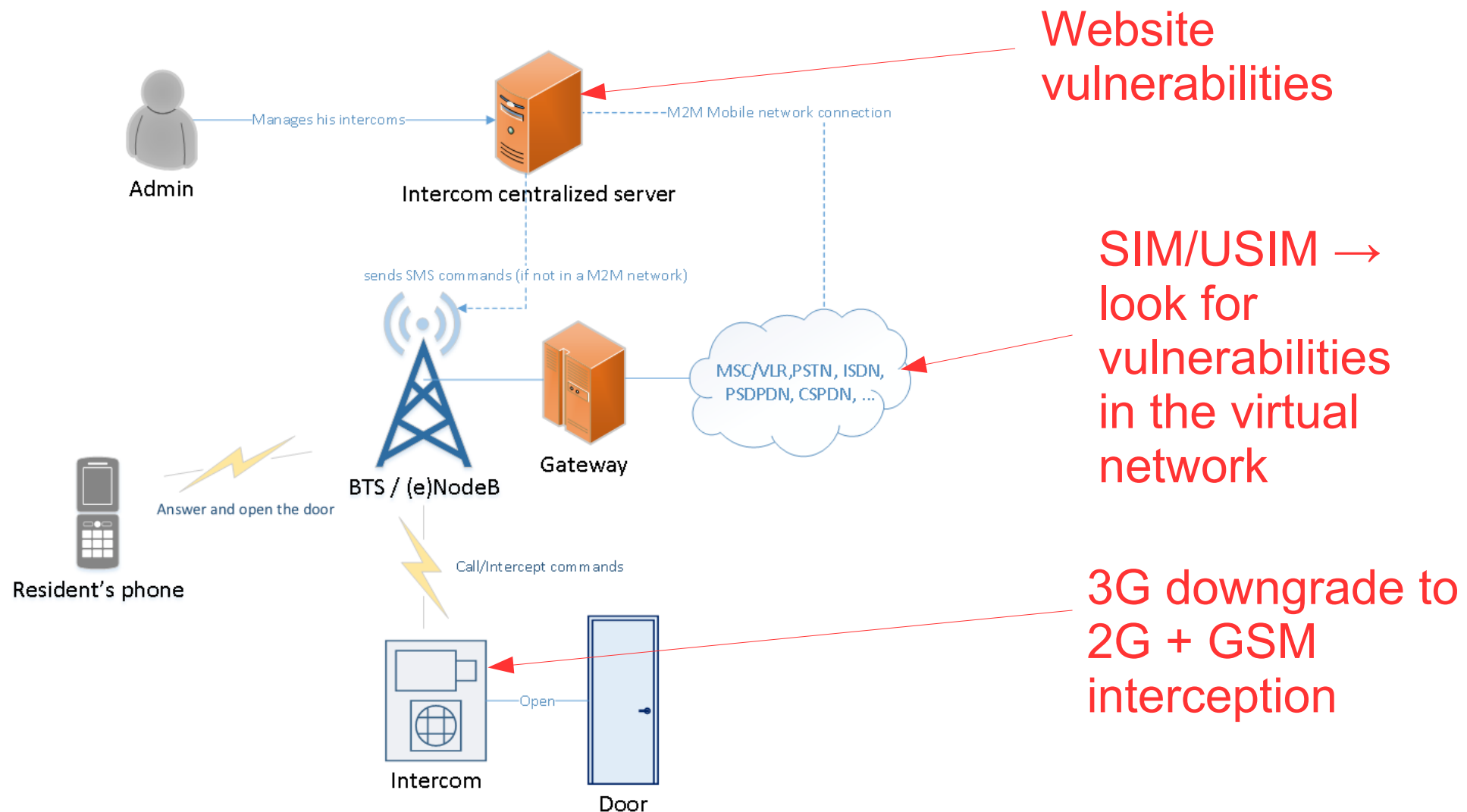
The screenshot shows the Allopass.com website interface. At the top, it says "allopass.com" and "Solution de micro paiement sécurisé / Secured micro payment solution". Below this, it instructs users to insert a code obtained by clicking on their country flag. The "France" flag is selected, and the phone number "08 99 78 05 05" is displayed. The cost of the call is listed as "1.34€/appel + 0.34 €/min. depuis une ligne fixe. Obtention du code <1.30min, coût : 1.80€". Payment options for "CB / CB Payment" (Visa, Mastercard, American Express) and "Neosurf" are shown. A warning states "Votre navigateur doit accepter les cookies". The ICRA logo is also present, indicating the site is labeled with the ICRA procedure. On the right, there is a section for "Autres pays" (Other countries) with flags for various nations. At the bottom right, there are input fields for "Code1" and "Code2", an "ok" button, and a reminder to accept cookies.

Intercoms using M2M SIM/USIM cards



- **Provided with a M2M SIM/USIM card**
 - more than 10 years subscription
 - the mobile operator provides a virtual network to manage the intercoms
- **Use the UMTS network by default**
 - GSM is used if UMTS is unreachable
- **Intercoms → managed by a centralized server**
 - **It's an interesting new vector of attacker, but there are many others...**

Attack vectors with M2M Intercoms

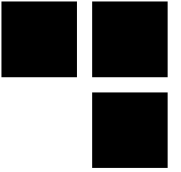




Website vulnerabilities

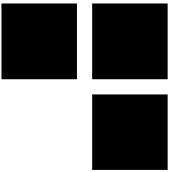
- **Websites → manage one or multiple intercoms thanks to their mobile number**
- **Vulnerabilities could be found:**
 - account guessing + bruteforce → we've tested it on a product
 - authentication bypasses → could be identified crawling with Google!
 - SQL injections
 - LFI, etc.

Our tests on “Product A”



- **We’ve tested a 3G intercom that is provided with a M2M SIM Card**
- **Lets call it “Product A”**

Bruteforce accounts

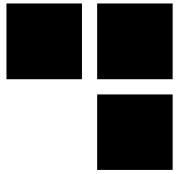


- By default, “Product A” website doesn’t enforce a password to manage intercoms:

Identifiant : Entrez votre n° [redacted] connexion

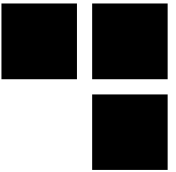
But we need a valid number...

Number enumeration (quick PoC)

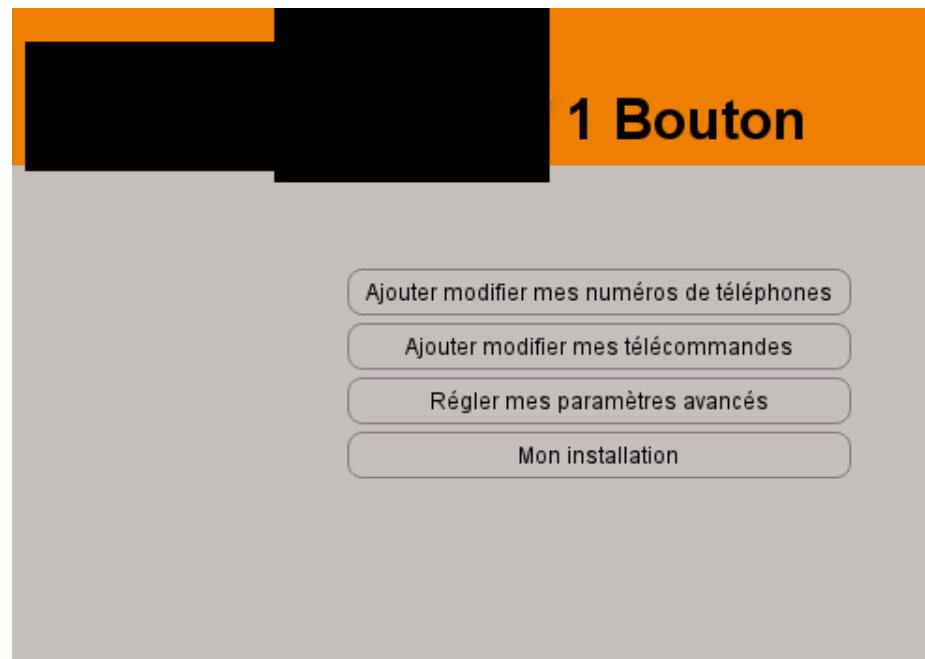


```
url = "http://<login page of product A>/<login page>"
[...]
prefixes = [ "07", "08", "30", "70", "71", "72", "73", "74", [...] ]
prefixes = reversed(sorted(prefixes))
init = 100000
numbers = []
for p in prefixes: # number generation
    init = 100000
    while init <= 999999:
        if init == 100000:
            numbers.append("06" + p + "000000")
            numbers.append("06" + p + str(init))
            init += 1
f = open("numbers.list", "a+")
for x in numbers: # for each generated number, log existing account
    t = int(time.time()) # timestamp added for the POST query
    data = {"**CENSORED1**":x, "**CENSORED2**":t}
    r = requests.get(url, params=data, headers=headers)
    if r.url != u"http://<login page of product A>/<error page>":
        f.write(x+"\n")
```

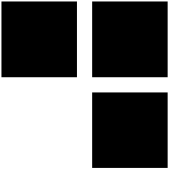

Enumerated accounts



- The server doesn't mitigate wrong tries
- So 90 numbers have been enumerated for 1 prefix (+33 6 77 *****) < 4 hours
- We are able to manage intercoms without the need of SDR tools!



Attack scenarios



- **Without the need of any SDR tool:**

- Update all intercoms with a premium rate number
=/



- open doors → but we need the locations...

How to get the location?

- In general, people add their home number first...

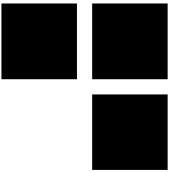
Paramétrer jusqu'à 10 numéros de téléphones (Fixe/ADSL/Mobile)

	Numéro	Commentaire	Appel
1	04 43	Gardien	Video Audio
2	06 94	Portable	Video Audio
3	06 12		Video Audio
4	04 29	Villa D	Video Audio

[+ Ajouter un numéro de téléphone](#)

Plage horaire

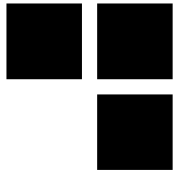
Reverse look-up directories



- Reverse look-up directories → get the precise location

The screenshot shows a web interface for a reverse look-up directory. At the top, there is a search bar with a yellow smiley face icon on the left and the text "04 [redacted] 29" inside. Below the search bar, the results are displayed as "04 [redacted] 29 : 1 résultat". To the right of this text is a printer icon. Below the results header, there is a list of results. The first result is numbered "1" in a yellow box, followed by the letter "A" and a redacted address. Below the address, it says "13 chem [redacted] X". To the left of the address is a placeholder icon for a photo. At the bottom right of the interface, there are two buttons: "PLAN" with a location pin icon and "AFFICHER LE N°" with a telephone icon and a dropdown arrow.

The M2M virtual network as a second attack vector



- **Provided SIM/USIM cards could be plugged on other devices**

→ we can scan the virtual network

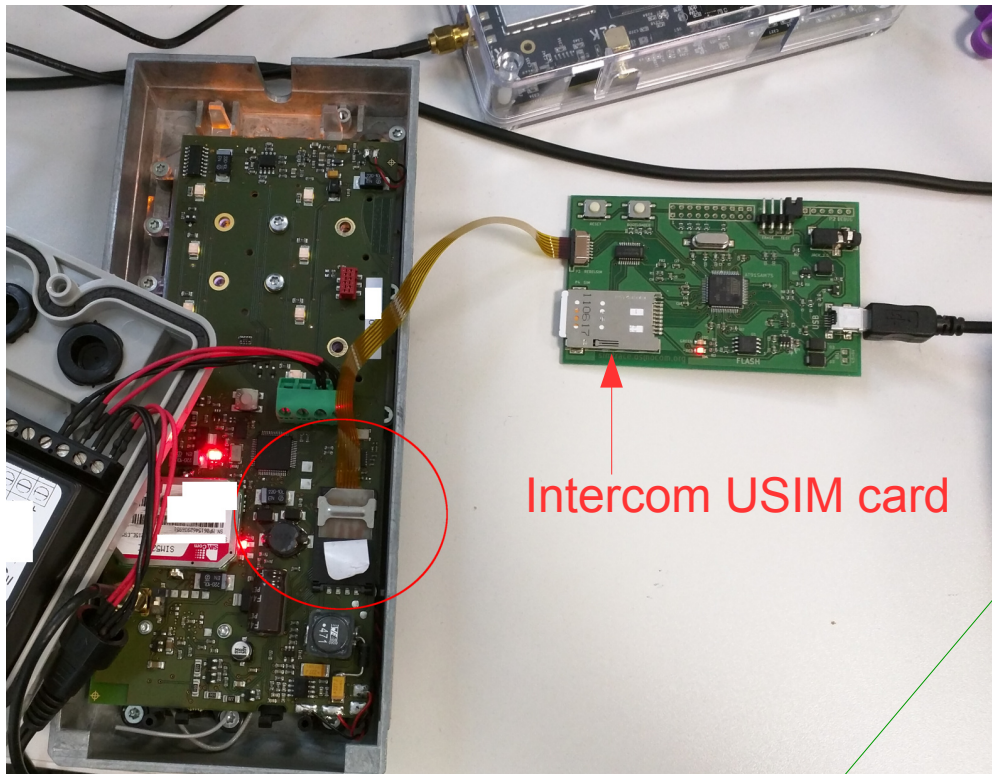
- **But product's “A” SIM/USIM card has a PIN code... =/**

→ not a problem for the SIMtrace tool!

SIMtrace setup and results



SIMtrace as a “proxy” between the SIM/USIM ↔ intercom:



Entering main loop

ATR APDU: 3b 9f 96 80 1f c7 80 31
e0 73 fe 21 1b 64 40 91 11 00 82
90 00 01

PPS(Fi=9/Di=6) APDU: 00 a4 00 04
02 3f 00 61 23

[...]

APDU: 00 20 00 01 08 ** ** ** ** ff

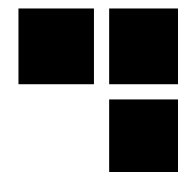
ff ff ff 90 00

APDU: 00 2c 00 01 00 63 ca

[...]

PIN code typed by the “Product A” intercom itself

Connecting to the M2M network



- Put the SIM/USIM in your phone
- Optionally change the IMEI (possible with some Chinese phones)
- Setup the right APN (Access Point Name) of the M2M network → documented
- Tether the communication
→ use a computer



Changing the IMEI within the engineer mode

Traceroute in the M2M virtual network



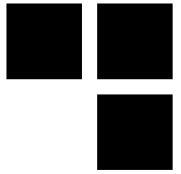
Check the connection with a tethered computer:

```
$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 192.168.42.129 (192.168.42.129) 0.622 ms 0.643 ms 0.705 ms
 2 10.***.***.250 (10.***.***.250) 105.629 ms 125.547 ms 185.628 ms
 3 10.***.***.209 (10.***.***.209) 195.783 ms 195.900 ms 195.831 ms
[...]
14 google-public-dns-a.google.com (8.8.8.8) 50.771 ms 50.248 ms
51.016 ms
```

An attacker will now be able to:

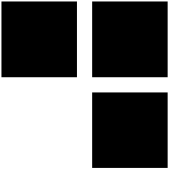
- 1) scan the virtual network
- 2) search for vulnerable services
- 3) then exploit vulnerable services
- 4) and so on... or use the SIM/USIM to get a free internet access ^^

Security recommendations for M2M solutions



- **Enforce a PIN code on SIM/USIM cards → like in “Product A”**
- **Whitelist IMEIs → the case of “Product A”? (not tested yet)**
- **Audit/pentest regularly the management website against web vulnerabilities**
- **Restrict actions and requests on APNs**
- **Is it possible to firewall the virtual network? or do some segmentation?**
- **Audit/pentest the virtual network against network attacks and vulnerabilities in services**
- **Monitor and block SIM/USIM cards that have a suspicious behavior**

Conclusion



- **With GSM intercoms we can:**
 - open a door
 - call premium rate numbers
 - spy on conversations if ATSS is supported
- **Intercoms using the mobile network → same flaws as mobile phones**
- **Other devices in the IoT ecosystem use the mobile network (e.g: Orange MyPlug)**
- **M2M intercoms introduce new vectors of attack → much more destructive → require a simple Internet connection (no SDR tools needed)**
 - But M2M SIM/USIM cards are also used in many other IoT products!
- **Further work:**
 - We are working on a semi-automatic downgrade attack from UMTS to GSM (the jammer will be published soon)



ANY QUESTIONS?



Thanks for your attention !

 **SYNACKTIV**
DIGITAL SECURITY