House intercoms attacks: when frontdoors become backdoors

Sébastien Dudek - sebastien.dudek@synacktiv.com

Abstract

To break into a building, several methods have already been discussed, such as trying to find the code paths of a digicode, clone RFID cards, use some social engineering attacks, or the use of archaic methods like lockpicking a door lock or breaking a window. New methods are now possible with recent intercoms. Indeed, these intercoms are used to call the tenants to access the building. But little study has been performed on how these boxes communicate to request and grant access to the building.

In the past, they were connected with wires directly to apartments. Now, these are more practical and allow residents to open doors not only from their classic door phone, but to forward calls to their home or mobile phone. Private houses are now equipped with these new devices and its common to find these "connected" intercoms on recent and renovated buildings.

In this short paper we introduce the Intercoms and focus on one particular devices that is commonly installed in buildings today. Then we present our analysis on an interesting attack vector, which already has its own history. After this analysis, we present our environment to test the intercoms, and show some practical attacks that could be performed on these devices.

Acknowledgement

I would like to thank my employer Synacktiv for giving me time to study this subject and many other cool ones, as well as my teammates for their time reviewing this paper and giving me advices and feedbacks.

I hope also this short paper will be interesting to read and any other feedback would also be appreciated to complet this research subject.

Contents

1 Introduction

1.1 Context

An intercom [1], door phone, or a house intercom, is generally a voice communication device for use within a building. Independent from the public telephone network, this device allows people to call a local resident to access to a building.

The classic version of intercom consists of a device that establishes a communication between the street door and the door phone device of a house. The device of the street door is generally equipped with a loudspeaker, a microphone, and buttons to a call residents. These classic versions of intercoms generally have $4 + n$ wires where 4 wires are used for power, door system, and where n is the number of homes to call.

New generation of intercoms become installed especially in new or renewed buildings. This new generation is called "Digital" and includes a GSM and 3G/4G module, but could also includes a Wi-Fi module as well. This generation avoids complex installations and ensure a maximum capacity, and they can easily include video communication in addition to the voice system.

1.2 Wiring topology

Three different types of house intercoms exist [2]:

- conventional: which are the classic version connected with $4 + n$ wires. This system is used in medium-sized buildings;
- simplified: one pair of wire that replaces the 4 wires of the conventional system and a wire for each house. This system is also used in medium-sized buildings.
- digital: the wire for each house is replaced by a mobile technology like GSM, 3G, or 4G. Sometimes an Internet cable could be used with a TCP/IP stack, but communication through GSM, 3G, or 4G is often chosen over a cumbersome cable for the ease of installation.

More outputs can also be included to control other doors and increase the number of cables.

1.2.1 Digital intercoms

Digital intercoms need less wires to link resident door phones to the building intercom. These intercoms offer a video call system, and also many other features to seduce the customers.

One of these practical features allows a resident to use it's own telephone, or mobile phone, to open the building street door. The figure 2 represents a simple architecture of a Digital Intercom installation.

When a person is calling a resident; the intercom uses a mobile network (GSM, 3G, or 4G) to reach the phone of the resident. The resident doesn't have to move anymore but only to reply with its smartphone and open the door.

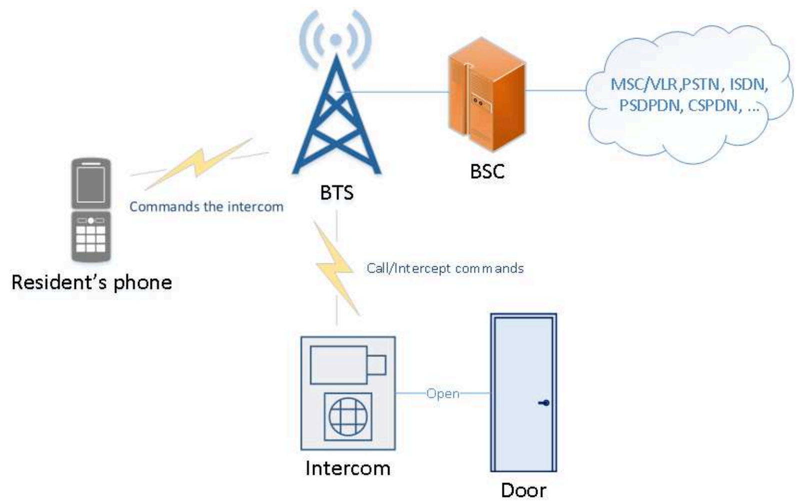


Figure 1: *Simple digital intercom architecture*

1.3 Leaders in the French market

In this market, 4 brands are generally present:

- Intratone;
- Noralsy;
- Urmet Captiv;
- Comelit.

It's not easy to recognize digital intercoms with a mobile module, but they generally come with a new stainless steel case, and sometime with a LCD screen and a front camera.

Some of these intercoms can be directly spotted thanks to the installation of a mobile network block. Indeed, as shown in figure 2 Intratone provide a 3G block that is connected to the intercom. If we look at the documentation, we can also read an interesting point saying that if the 3G network is not reachable, the intercom will automatically fall back to the GSM network [25]. This allows us to think that a downgrade attack is possible on these intercoms.

These devices are pretty expensive and cost around 1k€, but cheaper devices that provide pretty the same functionalities exist.

1.4 Cheaper alternatives

For those who are not seduced by the price, few alternatives exist:

- Linkcom which is commonly used by private residents;
- GSM Activate (UK company);
- and other devices that even don't have a name [26].

Figure 2: *3G block of an Intratone intercom*

1.5 Other variants of wireless intercoms

Other variants of intercoms exist that use the Wi-Fi, or DECT. These Wi-Fi or DECT intercoms hare surely very interesting to look and will probably inspire people in the area. In addition to Wi-Fi and DECT, other devices could be found on the market with a weaker communication protocol that could be broken easily with a 433/868/915 MHz frequency and an On-Off Keying modulation receiver and transmitter [27][3].

As we can see, wireless intercoms exist in every tastes and colors, but we will only focus on intercoms that communicate throught the mobile network like GSM, 3G or 4G.

2 State Of the Art

2.1 Publications

Very few publications exist on the subject of digital intercoms, and probably none about their security. But, some non-security publications could be inspiring like the article of Oliver Nash, which explains how to modify a conventional intercom to open the door with a cell phone [4]. Moreover, as they use the mobile network to communicate we can mention some good publications that would help to attack these intercoms.

An interesting paper was published about IMSI Catcher by Daehyun Strobel, showing that GSM tracking and taping is not a difficult task [8]. At Black Hat Briefings 2008, Steve Dhulton has highlighted some methods to capture and crack the GSM signal. It should be noted that between 2007 and 2008, The Hacker Choice (THC) group also regrouped and documented a lot of materials on GSM internals and A5/1 cracking. These documentation have been deleted in 2009, but are still available when browsing the archives. At the 26c3 in 2009, Chris Paget and Karsten Nohl presented attacks on GSM with rainbow tables [5]. In 2010 at 27c3, Harald Welte and Steve Markgraf have presented their OsmocomBB project that aims to run an open source GSM stack on few Motorola models, and capture the GSM traffic [6]. Using the same OsmocomBB stack, Sylvain Munaut and Kastern Nohl also showed at 27c3 that it is possible to intercept hopping calls using a cheap phone [7].

At BlackHat 2011, the hacking Vodaphone Femtocell gateways was presented by Ravishankar Borgaonkar, Nico Golde, and Kevin Redon. The unauthenticated firmware update vulnerabilities allowed attackers to push their own firmware to get a shell and turn these gateways into 3G IMSI-Catcher, without having to care about the mutual authentication constraint in UMTS [9]. Some details are also available in the THC Wiki [10].

At SSTIC 2014, Benoit Michau has presented an analysis of baseband security and highlighted the existance of bugs in some baseband implementations that could lead to a mutual authentification bypass in 3G and 4G [34].

Later in October 2015, attacks on privacy and availability of 4G were presented by the researchers Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi and Jean-Pierre Seifert [11]. The paper describes some attacks on the RRC (Radio Resource Control) and the EMM (EPS Mobility Management) protocols, that could lead to some leaks and downgrade the 4G UE to 3G or GSM.

2.2 Tools

In addition to the publications, the following tools will be useful to analyze and to attack intercoms:

- OpenBTS [12] and YateBTS [13]: software to run a GSM and GPRS Base Station;
- USRP [14], bladeRF [15], and so on: hardware to run a Base Station and capture mobile traffic;

- HackRF [16]: software-defined radio hardware that could be used to monitor mobile traffic, or that could be used for downgrade attacks for our case;
- GNU Radio [17] software-defined radio development toolkit;
- OpenLTE [18]: Open implementation of the 3GPP LTE specifications;
- OsmocomBB [31]: Open source GSM baseband;
- Airprobe [32]: GSM sniffer.

3 Short basics on GSM, GPRS, 3G, and 4G

Before attacking the digital intercoms, a better understanding of mobile security mechanisms and weaknesses is required.

3.1 Brief overview of GSM and GPRS authentication mechanisms

GSM (Global System for Mobile communications) and GPRS use an authentication mechanism A3/A8 called COMP128-3. The figure 3 shows the authentication process using the COMP128-3 mechanism. Only the SIM card and the AuC (Authentication Center) know the value of the subscriber key Ki (128 bits) that will be used to generate the RES (32 bits) resulting from the $RAND$ value in A3 and processed on the BSC/MSC side. Then RES will be compared to $SRES$ (32 bits) processed in the UE side. If $RES = SRES$ then the user will be authenticated to the network.

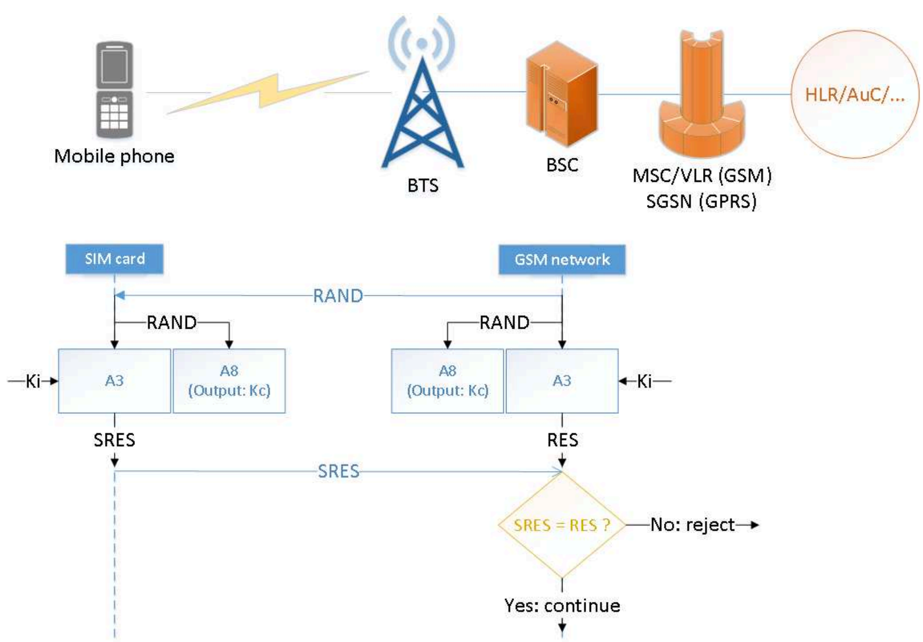


Figure 3: *GSM authentication process*

The ciphering in GSM is initially made with the A5/1 algorithm [20] at Layer 1 on the TCH (Traffic CHannel) and DCCH (Dedicated Control CHannel) [19]. To encrypt and decrypt the conversation, the key *Ki* generate a *Kc* key with the A8 mechanism as shown in figure 3. In GPRS, the user equipment authenticate to a SGSN and the ciphering is done at Layer 2 LLC (Logical Link Control) [21] initially with the GEA1 algorithm. So one of the main difference between GSM and GPRS is their way to maintain the confidentiality. In GSM the communication is confidential unlike GPRS where the data is confidential including user traffic and the signalization.

On GSM and GPRS an attacker is able to perform different known attacks:

- attract a victim to its rogue Base station, and intercept the communication with some forwarding tricks;
- reuse the authentication triplet $RAND, RES, Kc$ many times;
- attack the signaling channel which is not encrypted at all in GSM;
- attack the A5/1 algorithm [24];
- and son on.

3.2 The advantages of 3G/4G networks compared to GSM/GPRS

The security of mobile evolved with UMTS (3G) and LTE (4G) networks. Indeed, other algorithms for integrity and ciphering of radio access have been adopted. It stared with KASUMI [23] deployed for UMTS initially. Then SNOW-3G [22] appeared as a second algorithm for 3G but also for 4G. Additionally to SNOW-3G, 4G uses the AES CBC with 128 bits key to cipher the communication.

Thanks to the USIM (Universal Subscriber Identity Module), 3G and 4G networks use mutual authentication. The access to a UMTS network is possible with the previous SIM card, while in LTE the use of USIM is mandatory. So some attacks applied on GSM are possible on 3G with a targeted subscriber that uses a SIM card instead of a USIM card. An other attack would be to jam the radio signal to let the user equipment select a GSM cell instead.

3.3 Signal attraction

Wireless technologies use handover techniques, especially when users are generally mobile like in Wi-Fi, GSM, 3G and 4G. Devices always look for the best reception, so a user can move to one place and its UE will try to connect to the closer station. Attackers in this area know if there is no mutual authentication, it is easy to attract a UE in a rogue base station which has stronger signal than a legit station. Others method like jamming, or precise attacks on the targeted protocol can be used to downgrade the UE to GSM and bypass the mutual authentication.

Note that jamming is pretty basic and only requires a transmitter to send random data over-the-air in a specific frequency bandwidth. The example figure 4 below shows a GSM station channel at 925.4MHz before getting jammed by a transmitter as shown in figure 5.

As a consequence, devices close to the jammer will not be able to see the targeted channel.

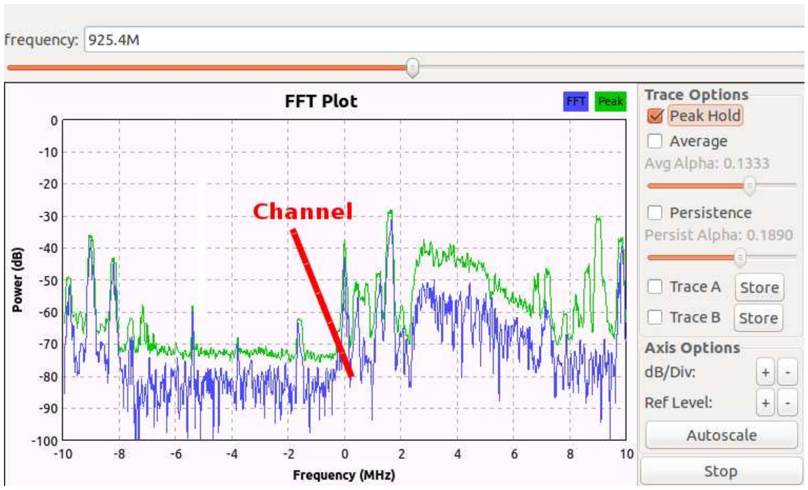


Figure 4: *FFT sink displaying the beginning of a channel*

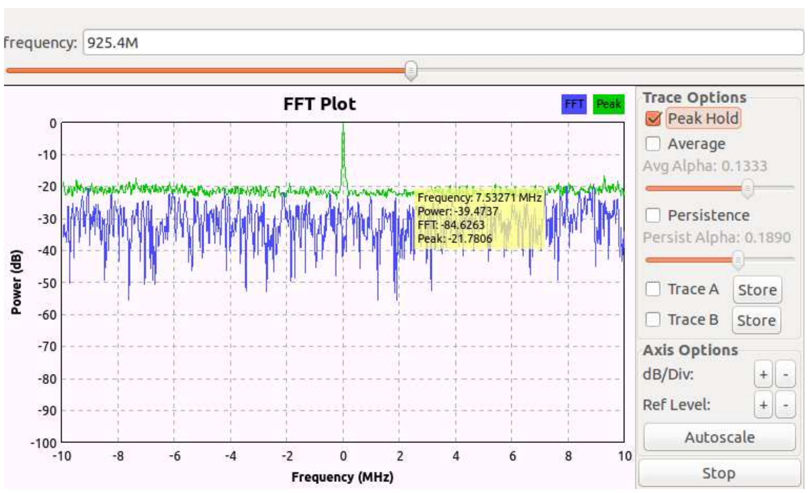


Figure 5: *FFT sink showing a station channel jammed by our transmitter*

4 Intercoms analyses

4.1 Environment

4.1.1 Lab setup

To analyze the intercoms we use a bladeRF x115 [28] powered through USB 3.0 by a computer, 2 antenna with 9 dBi for transmission (TX) and reception (RX) , and YateBTS as a radio access network software, like OpenBTS, as shown in figure 6.

As a first sample, we use a Link GSM iDP [29] intercom with a USIM card that belongs to Bouygues Telecom provider. To be powered, the intercom accepts 12 AC but also DC voltage, so

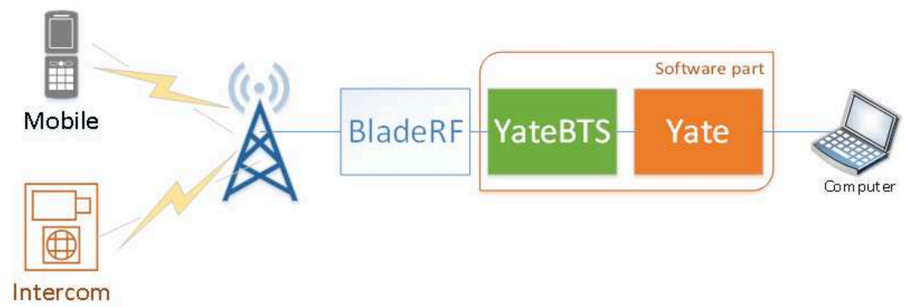


Figure 6: *Lab setup*

we powered it with a 12V and 1A DC switch adapter.

4.1.2 Intercom configuration

Following the Link iDP GSM manual [30] there are 3 ways to configure the intercom:

- programming the SIM manually thanks to a mobile phone, or a SIM reader/programmer;
- via SMS messages;
- or via the Link iDP manager software;

For security reasons, a first administrator "ADMIN1" number is required to command the intercom via SMS messages. So we have added a contact "ADMIN1" number to the SIM card with a mobile phone that is supposed to belong to the manager of this intercom. As a first impression, our goal as an attacker will be to impersonate a number, or find another way to bypass the number verification remotely to send commands to the intercom.

After that a valid ADMIN number can send commands to the intercom. For example, this subscriber can send a command update to change "ABUTTON1" number associated to a resident, as shown in figure 7.

The ADMIN user who sent the text gets an acknowledgement message.

4.1.3 Hypotheses

Before attacking the intercom, we have to put ourself to an attacker's place to keep things real:

- the attacker don't know the operator used by the intercom;
- the attacker don't know the number associated to the SIM of the intercom;
- the targeted intercom cannot be opened;
- and commands could be retrieved with public or leaked documentations, or retrieved with a firmware analysis of the same product.

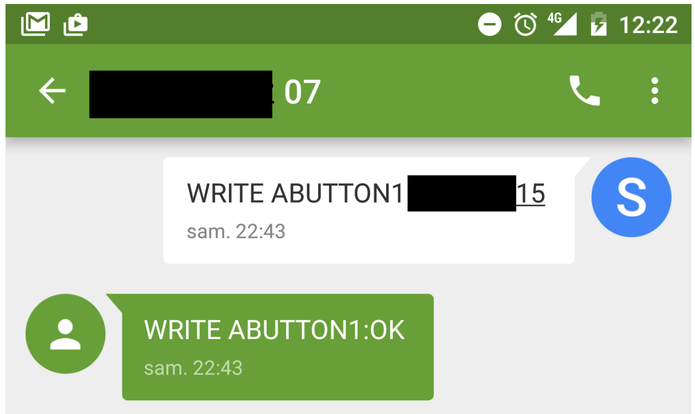


Figure 7: *ABUTTON1 updated through a SMS message*

4.2 Monitoring: passive attack

In our case, we know the intercom use GSM to communicate, but the operator and the mobile number are unknown. To get this information, we will listen to CCCHs (Common Control Channels) and try to locate the intercom.

4.2.1 Looking for paging messages

To establish a call, or to receive an SMS, the MSC/VLC (Mobile Switching Center/Visitor Location Center) need to locate the subscriber in the netwrwork. To locate this subscriber, or more precisely the subscriber, the stations send paging messages to the suscriber. If the subscriber is connected a a cell, it will to reply to this cell with a paging response to update its location.

To analyze these paging messages, two relevant tools exist:

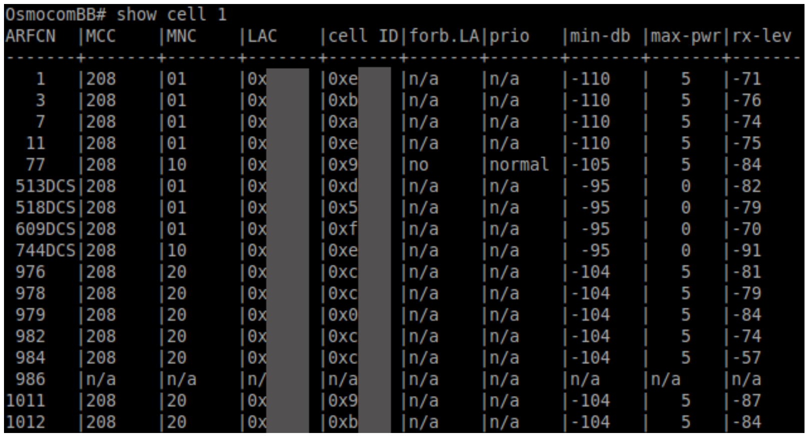
- Airprobe (supported by BladeRF, RTL-SDR, USRP, and so on);
- OsmocomBB (only supported by some Motorola equipped with a Calypso baseband).

We have chosen the OsmocomBB and used the `mobile` command to walk automatically through the different ARFCN (Absolute Radio Frequency Channel Number) indexes, and list operators that surround us as shown in figure 8.

Then we used the `ccch_scan` command and jumped on different ARFCN to capture messages on the CCCHs. As we can see in figure 9, many TMSIs can be collected.

With `ccch_scan` it is also possible to perform a GSMTAP to script a frequency analyzer based on the use of the TMSI. This GSMTAP can be observed also in Wireshark as shown in figure 10.

Based on the fact that a subscriber will be paged each time someone wants to call or text him, the main idea is to send a lot of paging requests to highlight the TMSI of our target. This type of attack inspired a lot of attacker who also where looking for a way to discretely send paging requests sending SMS Class 0 messages [33] (known as Flash SMS or Silent SMS).



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

Figure 8: *Cell information with OsmocomBB*

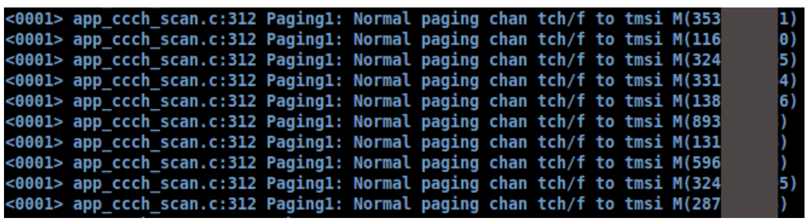


Figure 9: *TMSIs leaked in paging message*

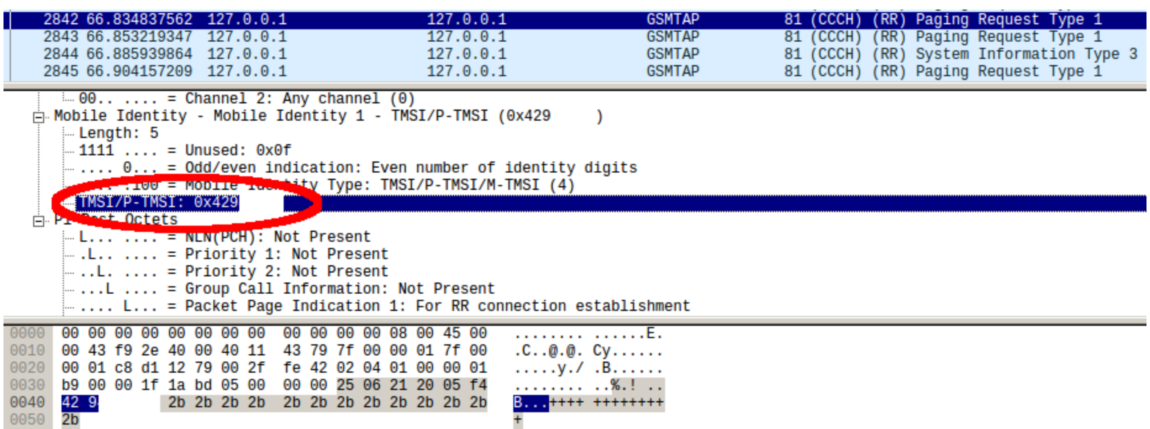


Figure 10: *GSMTAP with OsmocomBB and Wireshark to leak TMSIs*

Nevertheless, paging requests are difficult to sent without knowing the number, and paging responses are also rare for intercoms. Indeed, calling or texting an intercom is uncommon. Morever, to succeed in this path, a lot of sniffers have to be setup to monitor has many cells as possible like in figure 11.

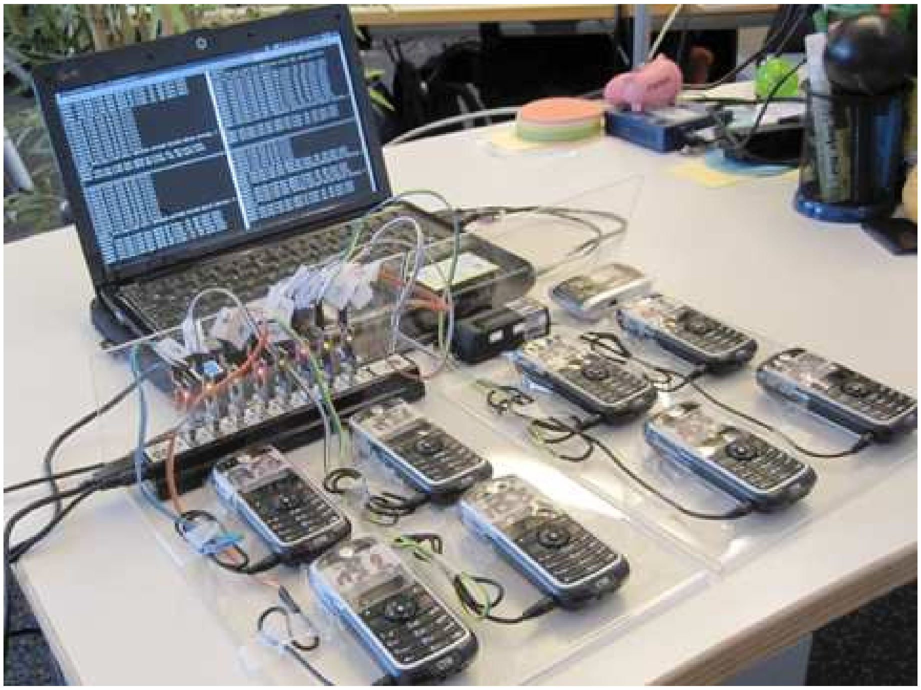


Figure 11: *GSMTAP with more OsmocomBB phones (source: malanris.ru)*

An other way would be to use some Social Engineering tricks to ask to a resident the number displayed by its intercom. But for our case, we will make use of active attacks to attract this intercom without knowing the MCC/MNC.

4.3 Trapping the intercom: active attack

Basebands behaviors are sometimes unpredictable when it comes to handover, even if specification make this clear. As far as we would know, a mobile phone is always looking for better signal. But with a certain experience, researchers observed also that a baseband can decide to move to another BTS 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).

To attract the Link GSM iDP we used different MCC/MNC codes, and wait few minutes (approximately 15 minutes) to let a chance to our rogue station to trap the intercom. After few minutes with a MCC/MNC that belongs to the operator SIM card installed in the intercom, the Link intercom connects to our rogue station as shown in figure 12.

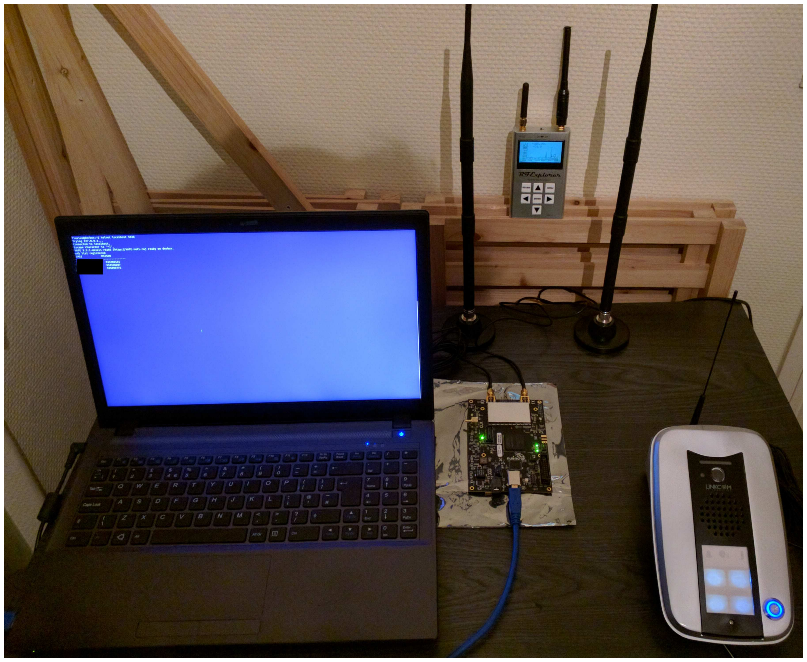


Figure 12: *The Link iDP GSM intercom trapped by our rogue station*

4.3.1 Leaking numbers

The intercom is now trapped in our rogue station and we have the full control of the routing. The first attack that could be made in this situation, is to leak the numbers saved in the intercom just by pressing the calling buttons. Like OpenBTS, YateBTS is capable of opening a GSMTAP UDP socket when enabling the feature in the `ybts.conf` like in figure 15.

```
[tapping]
; GSM: boolean: Captures GSM signaling at the L1/L2 interface via GSMTAP.
; Do not leave tapping enabled after finishing troubleshooting.
; Defaults to no.
GSM=yes
```

Figure 13: *Enabling GSMTAP in ybts.conf*

The figure 14 shows the leaked "ABUTTON1" number displayed with Wireshark.

Refering to the documentations of the Link iDP GSM intercom[30], there is a possbility to leak number saved for alarms if the contact `ALARMON` and `ALARMOFF` are configured.

4.3.2 Door openning

Thanks to leaked numbers, we can forward number associated to a resident's to a IMSI we control just by modifying the `tmsidata.conf` configuration file displayed in figure 15.

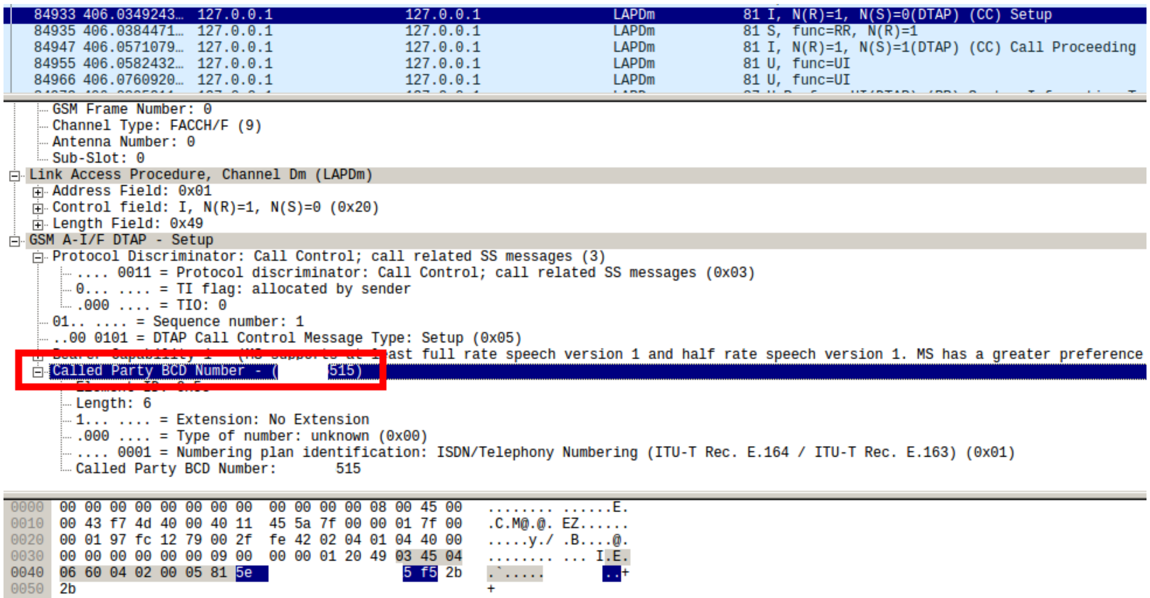


Figure 14: *Leaked number from rogue station GSMTAP after pushing the button 1*

```
[tmsi]
last=007b0005

[ues]
20820XXXXXXXXXX=007b0003,35547XXXXXXXXXX,XXXXXX515,1460XXXXXX,ybts/TMSI007b0003
# associating attacker IMSI with a resident number
[...]
```

Figure 15: *Affecting a resident number to an arbitrary IMSI in* `tmsidata.conf`

When this file is reloaded to YateBTS, we are able to capture the traffic with GSMTAP. When pressing the targeted resident's buttons the intercom call our mobile phone that is connected to our rogue GSM network, and we are able to open the door to penetrate the building.

This same technique could be used to command the intercom with an administrator number and have other dangerous impacts.

4.3.3 Backdooring

After leaking the administrator number with `ALARMON`, `ALARMOFF`, social engineering, or other methods, we can use the same tricks explained in section 4.3.2 to impersonate an administrator and send commands to the intercom. The new difficulty here is to find the commands accepted by the targeted intercom.

To find these commands, two main ways exist:

- look for public or leaked documentations of the targeted intercom;

- or buy the model in sites classified ads, like "Leboncoin.fr" (in France), dump the firmware and reverse it.

In our case, Link iDP GSM manual is public [30] and describes also commands that could be sent through SMS messages.

So reading the manual we can highlight some commands that interest us to read and write paramaters:

Command	Desciption
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!

Note that AT commands can be sent also, so it could be possible to:

- retrieve SMS messages sent by managers or residents with the command `AT+CMGL="ALL"`;
- spying building door conversations, when setting the Auto-answer parameter with the command `ATS0=1` (0: no auto-answer, 1: GSM module goes off-hook after the first ringing signal);
- and so on.

4.3.4 Call premium rate numbers: All I wanna do is "Bang Bang" and take your money!

As we are now able to write any number we want, why we couldn't make money out of this hack? All we need is to add or update a resident number with the following premium rated numbers:

- Allopass;
- Optelo;
- Hipay;
- and so on.

As an example, code given after calling the Allopass service can be used to fill a personal account. Then, these valid codes just have to be entered in our Allopass form (figure 16).

Note that the quality of the speaker as to be good enough to understand the code given when calling the Allopass with the intercom.

5 Summary

As described in this short paper, and combining the different researches in the GSM security field, we are able to attract an intercom to our rogue base station, impersonate any legit subscriber user and administrator, backdoor the intercom and update a resident number to a premium rated number to make money.

Figure 16: *The standart Allopass form*

We are currently working on tools to automate the attacks. Moreover, we will be looking on other intercoms products, including 3G and possible 4G intercoms, to complet this paper with practical downgrade attacks.

To finish, it should be noted that these attacks require more time in real life than in a laboratory with the perfect conditions. Indeed, depending on the baseband it will take time to get the intercom to be attracted by our rogue base station (while playing with the gain, MCC/MNC, jamming, etc.), but attacks could be adjusted quickly once the targeted baseband behavior is known.

References

[1] Intercom, Wikipedia definition - https://en.wikipedia.org/wiki/Intercom

[2] Doophone, Wikipedia definition - https://en.wikipedia.org/wiki/Door_phone

[3] RFCat tool - https://bitbucket.org/atlas0fd00m/rfcat

[4] A GSM based remote control for intercoms by Oliver Nash, http://olivernash.org/2009/10/31/locked-out-at-2am/

[5] GSM - SRSLY?, at 26c3 by Kastern Nohl and Chris Paget - https://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf

[6] Running your own GSM stack on a phone, at 27c3 by Harald Welte and Steve Markgraf - https://events.ccc.de/congress/2010/Fahrplan/attachments/1771_osmocombb-27c3.pdf

[7] GSM Sniffing, at 27c3 by Sylvain Munaut and Karsten Nohl - https://events.ccc.de/congress/2010/Fahrplan/attachments/1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf

[8] IMSI Catcher, by Daehyun Strobel - https://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_

[9] Femtocells: a Poisonous Needle in the Operator's Hay Stack, Back Hat 2011 by Ravishankar Borgaonkar, Nico Golde, Kévin Redon - https://www.isti.tu-berlin.de/fileadmin/fg214/bh2011.pdf

[10] The Vodafone Access Gateway / UMTS Femto cell / Vodafone Sure Signal, by THC - https://wiki.thc.org/vodafone

[11] Practical attacks against privacy and availability in 4G/LTE mobile communication systems, by Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi and Jean-Pierre Seifert - http://arxiv.org/pdf/1510.07563v1.pdf

[12] OpenBTS project website - http://openbts.org/

[13] YateBTS project website - http://yatebts.com/

[14] USRP ETTUS website - https://www.ettus.com/

[15] bladeRF website - http://nuand.com/

[16] HackRF One - https://greatscottgadgets.com/hackrf/

[17] GNU Radio website - http://gnuradio.org/redmine/projects/gnuradio/wiki

[18] openLTE project - http://openlte.sourceforge.net/

[19] ETSI TS 145 002 - http://www.etsi.org/deliver/etsi_ts/145000_145099/145002/09.03.00_60/ts_145002v090300p.p

[20] A5/1 algorithm - http://www.scard.org/gsm/a51.html

[21] ETSI TS 141 061 - http://www.etsi.org/deliver/etsi_ts/141000_141099/141061/04.00.00_60/ts_141061v040000p.p

[22] LTE Security, 2nd Edition by Dan Forsberg, Gunther Horn, Wolf-Dietrich Moeller, Valtteri Niemi

[23] Specification of 3GPP Confidentiality and Integrity Algorithms - http://www.garykessler.net/library/crypto/3G_KASUMI.pdf

[24] Decrypting GSM phone calls - https://srlabs.de/decrypting_gsm/

[25] Installation et raccordement du bloc 3G (Intratone) - http://www.intratone.fr/media/bloc_3g__067364900_1850_20082014.pdf

[26] (Noname) INTERPHONE AUDIO GSM - http://www.laboutiqueduportail.com/audio/419-interphone-audio-gsm-.html?gclid=CNL5zrTg3ssCFUmeGwodvI8KnQ

[27] You can ring my bell! Adventures in sub-GHz RF land, by Adam Laurie - http://adamsblog.aperturelabs.com/2013/03/you-can-ring-my-bell-adventures-in-sub.html

[28] bladeRF x115 from Nuand website - https://www.nuand.com/blog/product/bladerf-x115/

[29] Link GSM iDP - http://www.linkcom.fr/en/product-detail/link-gsm-idp/

[30] LinkCom iDP GSM manual - http://downloads.linkcom.fr/DoorPhone/Link_GSM_iDP/Manuel/Link_GSM_iD

[31] OsmocomBB - http://osmocom.org/projects/baseband

[32] Airprobe - https://svn.berlin.ccc.de/projects/airprobe/

[33] 3G TS 23.038, Technical Specification Group Terminals; Alphabets and language-specific information - ftp://www.3gpp.org/tsg_t/TSG_T/TSGT_04/Docs/PDFs/TP-99127.pdf

[34] Analyse sécurité des modems des terminaux mobiles by Benoit Michau at SSTIC 2014 - https://www.sstic.org/2014/presentation/Analyse_securite_modems_mobiles/