House intercoms attacks

When frontdoors become backdoors

Presented the 02/07/2016
For NDH 2016
By Sébastien Dudek
About me

- Company: Synacktiv
- Interests: radio-communications (Wi-Fi, RFID, GSM, PLC...), networking, web, Linux security… and intercoms!
- Do Red Team tests!
Red team tests at Synacktiv

- And can get spotted sometimes...
Our story with intercoms

- Synacktiv’s team got bigger
  → moved to another place
- The new place got new toys
  → access control systems, alarms, and a digital intercom...
This kind of intercom...

Features:
- Pass code
- Vigik
- Call a resident on his phone

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!
Summary

- **Introduction**
  - Context
  - Wiring topology
  - Leaders in the French market
  - Cheaper alternatives
  - Other variants

- **State Of The Art**

- **Short basics on GSM, GPRS, 3G, and 4G…**

- **Analysis of Intercoms**

- **Conclusion & further work**
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
Conventional intercoms

- Used for medium-sized buildings
- Has 4+n wires:
  - Power (2 wires)
  - door system (2 wires)
  - n → number of residents
Simplified intercoms

- One pair replaces the 4 conventional wires
- The other wires are for each resident
  - Like conventional intercoms...
Numeric intercoms

- No wire for each resident
- 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

- Resident’s phone
- BTS
- BSC
- MSC/VLR, PSTN, ISDN, PSDPWN, CSPDWN, ...
- Intercom
- Door
- Open
- Commands the intercom
- Call/Intercept commands
Leaders in the French market

- 4 brands are strongly present in France:
  - Intratone
  - Norasly
  - Urmet Captiv
  - Comelit
How to recognize a mobile intercom

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

Looks like a mobile module?
The 3G module of Intratone

Documentation is public:
http://www.intratone.fr/media/

The interesting part of the 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. »
Cheaper alternatives

- GSM Activate by a UK company
- Other devices without name
- Linkcom → commonly used by private residents

and already seen in two building in the 15th district of Paris

→ Our choice for analysis
Other variants of wireless intercoms

- Other variants exist:
  - Wi-Fi
  - DECT (Digital Enhanced Cordless Telecommunications)
  - other unsecure radio protocols
  - and so on.

⇒ We will only focus on intercoms that use the mobile network
Summary

- Introduction

- State Of The Art
  - Intercoms
  - Mobile security in the hacking community
  - Existing tools

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

- Analysis of Intercoms

- Conclusion & further work
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 Vodafone femtocell  
  (at BlackHat 2011, Ravishankar Borgaonkar, Nico Golde, and Kevin Redon)
- An analysis of basebands security  
  (at SSTIC 2014, Benoît 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 Benoît 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
Summary

- Introduction
- State Of The Art
- Short basics on GSM, GPRS, 3G, and 4G...
  - GSM and GPRS authentication and confidentiality
  - Mobile handover
  - Differences between GSM and GPRS and possible attacks
  - 3G and 4G advantages
  - Signal attraction...
- Analysis of Intercoms
- Conclusion & further work
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

Source: article.sapub.org
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
- and so on.

⇒ Interception is possible on GSM and GPRS
## 3G/4G: advantages

<table>
<thead>
<tr>
<th></th>
<th>GSM</th>
<th>3G</th>
<th>4G</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client authentication</strong></td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td><strong>Network authentication</strong></td>
<td>NO</td>
<td>Only if USIM is used (not SIM)</td>
<td>YES</td>
</tr>
<tr>
<td><strong>Signaling integrity</strong></td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td>A5/1</td>
<td>KASUMI</td>
<td>SNOW-3G</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A5/1</td>
<td>AES, ZUC...</td>
</tr>
</tbody>
</table>
Mobile interception: signal attraction

- A User Equipment connects to the closest Base Station
- 3G/4G downgrades to 2G via
  - jamming attacks → a simple Gaussian noise in targeted channels
  - protocol attacks → difficult
  - baseband strange behaviors
Jamming is generally basic...

Before

After
Downgrade 3G → 2G demo

- Targeted channel jamming
- Using a simple HackRF for ~300€
Summary

- Introduction
- State Of The Art
- Short basics on GSM, GPRS, 3G, and 4G...
- Analysis of Intercoms
  - Tests environment
  - Passive attacks
  - Active attacks → control it and make money out of it!
- Conclusion & further work
GSM Lab setup: for interception

- 1 BladeRF = 370 € minimum
- 2 Antennas = 15 € minimum each
- YateBTS software = FREE
- Total cost = 400 €
Intercom setup: hardware part

- For the beginning → Link iDP GSM for ~300€
- Can be powered in AC as in DC
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

1. Recognize intercom’s operator to trap it
2. Leak, or guess, numbers to impersonate
3. Configure the rogue base station → associate the attacker IMSI (International Mobile Subscriber Identity) to a resident number
4. Open the door!
5. And manage it with an “admin” number?
Passive attack: Monitoring

- CCCH (Common Control Channels) gives a lot of information
  - Management messages, sometimes SMS in clear, TMSIs (Temporary Mobile Subscriber Identity),...
- CCCH → paging request → can be exploited to locate someone → our target?
- Tools: OsmocomBB, Airprobe, and so on.
Capture a specific channel (1)

- List of ARFCN (Absolute Radio Frequency Channel Number)
Capture a specific channel (2)

- Leaked TMSI with `ccch_scan` OsmocomBB tool:

```
<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

Problem ⇒ paging requests to the intercoms are mostly rare + we will need more phone to monitor all cells =/
→ what about active attacks?
Active attacks

- A User Equipment decides to register to another base station if
  - it can register to any Mobile country code (MCC)/Mobile Network Codes (MNC) BTS close to it
    => For example with Orange in France: MCC = “208” and MNC = “01”
  - it can register to any 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...
Trap the intercom

- Brute forcing the 4 MCC/MNC
  - 15 min~ 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
What’s next? Let's open the door!

- Before updating a number → find an admin number:
  - leaked with calling buttons, or alarms
  - if not → use your social engineering tricks
- Once found → affect this number to your IMSI in `tmsidata.conf`

```
[tmsi]
last=007b0005
[ues]
20820XXXXXXXXXXX=007b0003,35547XXXXXXXXXXX,XXXXXX
515,1460XXXXXX,ybts/TMSI007b0003
# associating attacker IMSI with a resident number
[...]
```
What’s next? Let's backdoor it!

- **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:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>READ &lt;NAME&gt;</td>
<td>Read the number of a button, or an admin (ADMIN[1-9]).</td>
</tr>
<tr>
<td>WRITE &lt;NAME&gt; &lt;number&gt;</td>
<td>Add or update a number associated to a name.</td>
</tr>
<tr>
<td>CAL AT&lt;command suffix&gt;</td>
<td>Send an AT command to the baseband through SMS!</td>
</tr>
</tbody>
</table>
AT commands?

- We can interact with Intercom’s baseband:
  - retrieve SMS messages → \textit{AT+CMGL}="ALL"
  - spying building door conversations with auto-answer feature (if not disabled) → \textit{ATS0}=1
  - and so on.
Call premium rate numbers

- We can modify a contact → why not choose a premium number?
  - Allopase
  - Optelo
  - Hipay
  - and so on.
Demo

- Trapping an intercom
- Sending commands
Conclusion & further work

- Intercoms using the mobile network are vulnerable to the same flaws as mobile phones.
- Other devices in the IoT ecosystem use the mobile network (e.g.: Orange MyPlug).
- Further work:
  - include a semi-automatic 3G jammer
  - study 3G and 4G protocol downgrades
  - attack other intercoms
ANY QUESTIONS?

Thanks for your attention!