Femtocells: playing with secured telecommunication device

Ravishankar Borgaonkar, Kévin Redon

Technische Universität Berlin, SecT
ravii/kredon@sec.t-labs.tu-berlin.de

HackCon #6, 17 February 2011
mobile telecommunication history

- 0G - 1950: not so handy
- 1G - 1980: similar to 2G, but with analog voice (like in PSTN)
- 2G - 1991: GSM in Europe, CDMA in the USA. Very successful, ... and now broken
- 3G - 2002: UMTS in Europe, CDMA 2000 in the USA. Usable mobile Internet
UMTS architecture (complex)

Structure of an UMTS network

- ME : Mobile Equipment
- MT/TE
- Cu : USIM, UICC
- UE : User Equipment
- MS : Mobile Station
- RNC
- Node B
- cell
- Uu
- Iub
- Iur
- AN : Access Network
- PSTN
- VLR
- HSS
- HLR
- AuC
- GMSC
- MSC server
- CS-MGW
- Nb
- Mc
- E
- C
- F
- Gf, Sv
- Gd
- EIR
- SMS-GMSC
- PS & CS
- CN : Core Network
- Internet
- Gi
- Gn
- Gp
- Gc
- Gd
- PSTN
- B
- D
- G

R. Borgaonkar, K. Redon
UMTS architecture (simplified)

ME : Mobile Equipment
UE : User Equipment

NodeB

RNC

AN : Access Network

CS-MGW
CS : Circuit Switched

SGSN
PS : Packet Switched
CN : Core Network

I_uCS
I_uPS
I_ub
cells

- femtocell
- using it
- owning it
- abusing it
- and far beyond

3G/UMTS femtocells

HNB Subsystem (HNS)

Macrocells

- cell $10^0$
- mini $10^{-3}$
- micro $10^{-6}$
- nano $10^{-9}$
- pico $10^{-12}$
- femto $10^{-15}$
- atto $10^{-18}$

R. Borgaonkar, K. Redon

femtocell secured?
What is a femtocell:

- it's an access point (sometimes called FAP)
- it connects the mobile phone to the 3G/UMTS network
- compatible with every UMTS capable mobile phone
- small cells, with a coverage of less than 20m
- low power device
- easy to install, you only have provide power and Internet access
- technical name: Home Node B (HNB)
advantages provided to the users:

- can be installed at home to provide coverage (if not available)
- provides high bandwidth (not shared with the public)
- can provide location based services (kids arrived at home)

but nothing Wifi can not provide for free, except you don't have to configure the phone.
advantages for the operator:

- extended coverage, near to the users
- traffic offloads from their public infrastructure
- cheap hardware, that the user even has to buy
- no installation cost
- no maintenance cost
- new revenue possibilities
- IP connectivity

Conclusion: femtocells are a great opportunity for the operators.
**HNB in UMTS network**

- **RNS**: Radio Network Subsystem
- **CS**: Circuit Switched
- **HNS**: Home NodeB Subsystem
- **AN**: Access Network
- **UE**: User Equipment
- **ME**: Mobile Equipment
- **UICC [USIM]**: User Identity Card [Universal Subscriber Identity Module]
- **UE**: User Equipment
- **MS**: Mobile Station
- **HNB**: Home NodeB
- **SeGW**: SGSN Gateway
- **HNB-GW**: Home NodeB Gateway
- **MSC**: Mobile Switching Center
- **SGSN**: Serving GPRS Support Node
- **CN**: Core Network
- **CN**: Circuit Switched
- **PS**: Packet Switched
- **AN**: Access Network
- **Uu**: Air Interface
- **Iu**: Iu Interface
- **Iu,h**: Iu,h Interface
- **Iu,l**: Iu,l Interface
- **Iu,CS**: Iu,CS Interface
- **Iu,PS**: Iu,PS Interface
- **NodeB**: NodeB
- **RNC**: Radio Network Controller
- **IPsec**: IP Security

**Femtocell**
- © using it
- ⚡ owning it
- ☠ abusing it
- X and far beyond

**3G/UMTS**

**Femtocell secured?**

R. Borgaonkar, K. Redon

Page 9/33
How to get a femtocell:

- choose a country from the 12 which deploy them
- get an address and IP from this country, because usage in only allowed within the country
- select an operator from the 18 which offer them
- get a mobile phone subscription from this operator, required to get the femtocell service
- gently ask for a femtocell
- get it for free, one time payment, or monthly fee
- enjoy ☺
Location verification

operators have to verify where the femtocell is, for several reasons:

- prevent you to avoid roaming costs in foreign countries
- UMTS uses the 2.1 GHz freq. band, a licensed spectrum band. The operators own the radio licenses for the femtocell only for their country
- location of the users is required for lawful interception
How to find where the femtocell is located:

- **IP**: geoIP, even knowing the ISP is enough
- **GNSS**: GPS
- **macrocell**: cells bacon county, network, and location information (MCC, MNC, LAC)
attacks

- shielding
- jamming
- spoofing

GNSS

HNB

ME

macrocell

Internet
tunnel

GW

fake macrocell

fake GNSS

ordering

location verification

femtocell

© using it

owl owning it

☢ abusing it

and far beyond

final solution

R. Borgaonkar, K. Redon

femtocell secured?
under the hood
network testing

first approach:

- sniffing
  only DHCP, and NTP. Then everything goes over IPsec
- probing ports (nmap)
  only port 80 is open
  linux has been detected, but the source code is not public
- web interface available
  protected access, no documentation, even the customer service was unaware
- serial port found on PCB
  login prompt not enabled

First impression: the device is secure. ☹
But the first impression is not the last impression. 😊

R. Borgaonkar, K. Redon
**critical point**: the recovery procedure

remember:
- keep femtocells cheap
- no maintenance cost
- no local support

So if something does not work right, do a factory reset. For that, the recovery procedure has been created.
process overview

1. get recovery executable
   HTTP (credentials)
   recovery executable
   encrypted and signed
2. start recovery program
3. get parameter and firmware list
   HTTPS (client certificate)
4. check installed firmware
5. get new firmware (if different)
   HTTP
   firmware
   encrypted and signed
6. decrypt file
   verify signature
   flash firmware
7. notify successful flashing
   HTTPS (client certificate)
8. for each firmware in the list
flaws and exploits

flaws:
- recovery image is downloaded over HTTP
- credentials are in plain text
- normally the image is encrypted, but modified URL will return unencrypted version
- image is still signed. It can't be altered, but viewed

exploit: the recovery process can be analyzed
flaws and exploits

**flaws:**

- integrity of parameter and image list relies only on HTTPS
- file is not signed
- HTTPS uses authentication, but not mutual authentication

**exploit:** you can provide your own lists
flaws and exploits

flaws:
- real name of the files are in the image list
- encryption keys are in the image list

exploit: you can get an decrypt the images
**flaws and exploits**

**flaws:**
- encryption key is derived from the public key
- signature can be overridden

**exploit:** you can even give your own "recovery" image

![Diagram showing the process of getting recovery executable](image)
the parameter list contains some interesting values:

- the login prompt for the serial port can be enabled
- the root password is the same then in the recovery image, stored in md5
- the public key used to verify the signatures is in there
- it's possible to clone femtocells (except the SIM)

```
[General]
pcbhid=P04S...
imei=357539...
mac=00:1B:67:...
hwflag=2
serial=P04S...

[BootSigning]
pubkey=EE:17:C5:F2:...
```
found while analyzing the images:

- credentials for web interface are in a local database
- the previously discovered interface is provided by the operator. It only contains the status and subscriber list
- a hidden web interface is provided by the vendor. It contains the complete configuration
- the hidden web pages can be accessed without authentication
you can provide your own image list:

- the URLs, encryption keys and signatures are in there
- your can provide your own images
- your can use the previously obtained images, and modify them
- now it's possible to install anything
HNS services

use the femtocell to explore behind the security gateway:

- Performance Measurement server: retrieve information about other femtocells
- OAM server: download new and old firmwares images. analyze the modifications
- HMS server: get the provisioning data from other femtocells

<table>
<thead>
<tr>
<th>IMSI</th>
<th>IMEI</th>
<th>Cell ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>xxxx03590389xxx</td>
<td>xxxx39010383xxx</td>
<td>xxxx</td>
</tr>
<tr>
<td>xxxx03490391xxx</td>
<td>xxxx39010441xxx</td>
<td>xxxx</td>
</tr>
<tr>
<td>....</td>
<td>....</td>
<td>....</td>
</tr>
</tbody>
</table>
you can change the femtocell settings:

- disable macrocell sniffing
- add phone to the subscriber list
- provide own security gateway
- change cell configuration
significance of the attacks

the attacks are affecting:

- roaming
- lawful interception
- licenses conflicts
- attacks to the core network
- privacy threat
Attacks, effects, and impact are documented in the 3GPP femtocell standard (TR 33.820)

<table>
<thead>
<tr>
<th>group</th>
<th>threat</th>
<th>impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromise of HNB Credentials</td>
<td>Compromise of HNB authentication token by local physical intrusion</td>
<td>Harmful</td>
</tr>
<tr>
<td>Physical attacks on a HNB</td>
<td>Booting HNB with fraudulent software (&quot;re-flashing&quot;)</td>
<td>up to disastrous</td>
</tr>
<tr>
<td>Configuration attacks on a HNB</td>
<td>Fraudulent software update / configuration changes</td>
<td>Extremely harmful</td>
</tr>
<tr>
<td></td>
<td>Mis-configuration of HNB</td>
<td>Irritating to harmful</td>
</tr>
<tr>
<td></td>
<td>Mis-configuration of access control list (ACL) or compromise of the access control list</td>
<td>Irritating to harmful</td>
</tr>
<tr>
<td>Protocol attacks on a HNB</td>
<td>Man-in-the-middle attacks on HNB first network access</td>
<td>Very Harmful</td>
</tr>
<tr>
<td></td>
<td>Compromise of an HNB by exploiting weaknesses of active network services</td>
<td>Extremely harmful</td>
</tr>
<tr>
<td></td>
<td>Manipulation of external time source</td>
<td>Harmful</td>
</tr>
<tr>
<td></td>
<td>Threat of HNB network access</td>
<td>Harmful</td>
</tr>
<tr>
<td>Attacks on the core network, including HNB location-based attacks</td>
<td>Changing of the HNB location without reporting</td>
<td>Harmful</td>
</tr>
<tr>
<td></td>
<td>Misconfiguration of the firewall in the modem/router</td>
<td>Annoying</td>
</tr>
<tr>
<td></td>
<td>HNB announcing incorrect location to the network</td>
<td>Harmful</td>
</tr>
<tr>
<td>User Data and identity privacy attacks</td>
<td>User’s network ID revealed to Home (e)NodeB owner</td>
<td>Breaking users privacy</td>
</tr>
</tbody>
</table>

It also includes recommendations and countermeasures
femtocells is an effective technology in terms of offloading the traffic and of new business cases.

but... the operators need to do their homework:

- follow the specifications, secure the device and network access

some serious threats (ongoing work):

- re-use the telecom infrastructure elements
- us as a very cheap IMSI catcher
- build a MitM, to be used during communications
Thanks

Thanks to:

- Collin Mulliner, TU Berlin
- Prof. Jean-Pierre Seifert, TU Berlin
- Benjamin Michéle, TU Berlin
Tusen Takk

Questions?