Femtocell Security

a femtostep to the holy grail

Ravishankar Borgaonkar
ravii@sec.t-labs.tu-berlin.de

Kévin Redon
kredon@sec.t-labs.tu-berlin.de
Actors

● Ravishankar Borgaonkar
  – PhD student at TU Berlin
  – Area: M2M Security, Mobile Networking Security

● Kévin Redon
  – Master Student at TU Berlin
  – Area: Network Security

● Special thanks to:
  – Collin Mulliner, TU Berlin
  – Prof. Jean-Pierre Seifert, TU Berlin
  – Benjamin Michéle, TU Berlin
  – Monty Python
Plot : the action

- Introduction to femtocell
- Security of the femtocell devices
- Location verification methods
- Beating the location verification methods
- Analyzing one femtocell
- Demo
Subject: femtocells

- $10^0$ macro
- $10^{-3}$ cell
- $10^{-6}$ milli
- $10^{-9}$ micro
- $10^{-12}$ nano
- $10^{-15}$ pico
- Femto
Marketing: Femtocell technology

- Low power access point
- Supports any 3G mobile device
- Provide 3G coverage for places where macrocells cannot
- Offloads traffic from the macrocell layer, and improve macrocell capacity
- IP connection to the core network
- Higher data rates with power saving option to the mobile devices
Distribution: how, where, how much

- currently in the 9 countries (soon in other places)
- you can buy easily
- you need to provide right address to provision since they lock the device to a particular location
- if you change the address, it will not work (as they say so)
- costs < 200 euro + normal phone subscription
- **No Roaming** is allowed on the Femtocells
- Radio licenses are lend by the operator
<table>
<thead>
<tr>
<th>Country</th>
<th>Operator</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>AT &amp; T, Verizon</td>
<td>ip.access, Samsung</td>
</tr>
<tr>
<td>Japan</td>
<td>KDDI, NTT Docomo</td>
<td>Airvana, Mitsubishi</td>
</tr>
<tr>
<td>Portugal</td>
<td>Optimus</td>
<td>Huawei</td>
</tr>
<tr>
<td>France</td>
<td>SFR</td>
<td>Ubiquisys</td>
</tr>
<tr>
<td>Singapore</td>
<td>Singtel, Starhub</td>
<td>Huawei</td>
</tr>
<tr>
<td>Japan</td>
<td>Softbank</td>
<td>Ubiquisys</td>
</tr>
<tr>
<td>Spain</td>
<td>Telefonica</td>
<td>Huawei</td>
</tr>
<tr>
<td>UK</td>
<td>Vodafone</td>
<td>Alcatel-Lucent</td>
</tr>
<tr>
<td>Greece</td>
<td>Vodafone</td>
<td>Huawei</td>
</tr>
</tbody>
</table>
Difference: Femtocell and NodeB

- RNS: Radio Network Subsystem
  - cells
  - Iub
  - NodeB
  - RNC

- CS: Circuit Switched
  - IuCS
  - MSC

- UTRAN: Universal Terrestrial Radio Access Network
  - AN: Access Network
  - HNB-GW
  - SeGW
  - HMS
  - TR-069
  - IPsec
  - luh

- SGSN: Packet Switched
  - luPS
  - CN: Core Network

- UICC [USIM]
  - UE: User Equipment
  - MS: Mobile Station

- ME
  - Uu

Kévin Redon
Femtocell Security
Berlin Sides 2010
Femtocell Architecture

- User Equipment (UE)
- femtocell Device aka HNB (Home NodeB)
- Security Gateway (SeGW)
- Home Management Server (HMS) ~ OAM
Femtocell Security

Only registered SIMs are allowed

3G AKA procedure

Secure phone calls (over-the-air)

Remote controlled HNB

Location verification

IPsec tunnel over broadband

Kévin Redon  Femtocell Security  Berlin Sides 2010
Femtocell Security Requirements

- femtocell should be locked to a specific geographical location to avoid misuse (roaming is good) and to respect radio license
- booting process of the femtocell should be secured by cryptographic means (e.g. no ROOT access)
- device should not reveal any secret information such as IMSI, stored keys etc. (e.g. public keys, IPsec keys)
- ...
- Security of H(e)NB, TR 33.820
Location: locked place

**geoIP**

- UE
- HNB
- Internet
- GW

**macrocells**

- BTS/nodeB signal
- HNB

**GNSS**

- GNSS signal
- HNB

**UE reports**

- GNSS
- ME
- HNB
Beating Location: on travel

- avoid roaming
- avoid localization
- limit lawful interception

**GNSS**
- GNSS jammer
- GNSS spoofer

**macrocells**
- 2G/3G jammer
- fake BTS/nodeB signal

**geoIP**
- Country A
- true location
- Internet
- VPN tunnel
- Country B
- fake location
- VPN exit

Kévin Redon  Femtocell Security  Berlin Sides 2010
Will the good guy win?

what could go wrong? lawful interception
device security analysis
femtocell example

- cheap hardware
  - CPU+FPGA
  - RF chips
  - TPM/UICC/SIM
- fews vendors
- operators only customize
Analyzing the device

different approaches to investigate an access point:

- scan the network
- finding a serial port
- sniffing the communication
Secured device

- no port open apart http
- serial port found, but no login prompt
- all communication is over IPsec
Recovery procedure

- image download over http
- using hashes in the url
- encrypted and signed
- one small https request
- some https notifications

1. small loader getting a recovery file system
2. recovery file system downloads and flashes all other images
Recovery to failure

1. Recovery file system in also available unencrypted

you cannot modify it (signed), but at least analyze (tivo)
Recovery to failure

Usage:
```
datafile filesize signature|sha1 [pubkey1 [pubkey2]]
```

signature is 128 colon-separated hex bytes,
sha1 is 20 hex bytes (no colons), and has no pubkeys

① recovery file system signature verification process is buggy

*it is possible to provide not encrypted and public key*
Recovery to failure ③

③ no mutual authentication over HTTPS

critical customisation data can be provided

```
## CUSTOMISATION.INI START
[General]
pcbid=P04S800...
imei=357539010...
mac=00:1B:67:...
hwflag=2
serial=P04S800...
...
```
Recovery to failure ③

③ given public key is not signed

_own private key can be used, and public key provided_
Recovery to failure ⑤

for each firmware in the list

④ check installed firmware

⑦ get new firmware (if different)

HTTP

encrypted and signed

⑤ firmware

⑥ decrypt file

verify signature

flash firmware

⑧ notify successful flashing

HTTPS (client certificate)

⑤ list of images includes the keys

images can be decrypted, analyzed, and reused

[rootfs.bin]
url=http://….115/store/fbb3d53b…
key=44:d2:13:8e:a7:03:…
sha1=e8e1d6e0c57ca50…
size=6115328
sig=61:e9:b3:47:…
dbid=9
dbval=104
Hidden webpages

- the operator provided custom web pages
  - not in the manual
  - password is IMEI
  - restricted functions
- the vendor also has web pages
  - hidden
  - not protected
  - full customisation
Your mine: pwnd

- setup a fake recovery server
  services: DHCP, DNS, NTP, and HTTP[S]
- re-activate login prompt
- flash modified images

automated process:
- script to patch images
- script to check updates
Recovery to failure ☠

- threat 6 of 29:

  Booting H(e)NB with fraudulent software ("re-flashing")

  **Impact:** up to disastrous. Possibility to use any software can mean any violation of the security

- an opening door for other threats

- all documented in

  3GPP TR 33.820
Doors to heaven

- tunnel access to: OAM, image server, PM
- contact to HNB GW
- 13 of 29 threats accomplished
- next step: controlling IPsec
The End : RTFM

- effective technology in terms of offloading the traffic and of new business cases
- provides higher data rates to the user … but ....
- the device security can become a breach
- some serious threats :
  - could open gates to the Telecom infrastructure elements (like HLR)
  - a very cheap IMSI catcher device
  - might used as MiTM device while calling
References

  http://www.3gpp.org

  http://www.3gpp.org

- Wikipedia Commons for the Cell pictures
  https://secure.wikimedia.org/wikipedia/commons/wiki/Category:Base_stations_%28mobile_phones%29
Questions?

Thank U