Immature Femtocells

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

Kevin Redon
kredon@sec.t-labs.tu-berlin.de
Introduction

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

● Kevin 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
Contents

Introduction to Femtocell
Security of the Femtocell devices
Location locking methods
Beating the location locking methods
Hacking into the device
Demo
Femtocell Technology

- Low power wireless device
- Transmits mobile voice & data to operator's core network via a broadband connection
- An extension of 3G coverage in the home with improved wireless data rates
- Any 3G handsets supports
- IP connection to the core network
- Low cost availability
Femtocell Future

Someday, all Basestations will be Made Like This
Nigel Toon - CEO, picoChip

Femtocells - Playing A Pivotal Role In 4G Networks
Timo Hyppola - Head of Indoor Radio, Nokia Siemens Networks
How and where?

- Currently in the US, France, & UK market (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 < 100 euro + normal phone subscription
- No roaming is allowed on the Femtocells

Small base station?
Difference: Femtocell and NodeB

- **ME**: Mobile Equipment
- **UICC**: User Identity Card
- **UE**: User Equipment
- **MS**: Mobile Station
- **NodeB**: Radio Network Subsystem
- **RNS**: Radio Network Subsystem
- **UTRAN**: Universal Terrestrial Radio Access Network
- **AN**: Access Network
- **CN**: Core Network
- **PLMN**: Public Land Mobile Network

Unsecure link between ME and HNB.
Femtocell Architecture

- Femtocell Device aka HNB (Home NodeB)
- Security Gateway
- Operation, Administration & Management server
- User Equipment

![Femtocell Architecture Diagram]
Femtocell Security

Only registered SIMs are allowed

3G AKA procedure

Secure phone calls (over-the-air)

Remote controlled HNB

IPsec tunnel over broadband
Femtocell Security Requirements

- Femtocell should be locked to a specific geographical location to avoid misuse and conflict.
- 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).

But we know :-)
Location Locking Methods

- Using IP address of the femtocell device
- Using location area code and Mobile country code (by sniffing)
- Using GPS (Global Position System) signal
- Using UE reports (requesting neighboring cell ID or GPS coordinates from UE)
- OR mixed approach
On the Device

Enable 2G Sniff: true
Configured Bands: GSM900 + 1800
OPLMN Search Enable: true
GSM Neighbour List Type: Reselection & Han

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Activation time</th>
</tr>
</thead>
<tbody>
<tr>
<td>CannotSelectRFProfile:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>SoftwareFault:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>PMReportFailure:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>LocationChanged:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>PoorRFQos:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>PoorBackHaulQoS:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>OverTemperature:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>UpgradeFailure:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>FilesystemFailure:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>HotSpotIndication:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>NoNtpServer:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>InvalidCountry:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>GatewayChanged:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>AllTimingServerConnectivityLost:</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>NoTimingSource:</td>
<td>INACTIVE</td>
</tr>
</tbody>
</table>
Breaking locks - IP address

- Use VPN (Virtual Private Network)
- Only need to show that you are at home :-)

Diagram:

- UE
- HNB
- True location
- Internet
- VPN tunnel
- Country A
- VPN exit
- Country B
- Fake location
Breaking locks - GPS

- Tools you need: GPS jammer or GPS spoofer
- Attacker can block GPS signals and signals are weak inside the home
- Not all devices have GPS
Breaking locks - LAC and MCC

- Tools you need: GSM jammer or BTS (e.g. nanoBTS)
- LAC and MCC can be faked using nanoBTS
- Or simply use a GSM jammer (most of the femtocells use a GSM receiver chip)
Result
No risk, no fun

Lets Hack the box now

Rooting process.....
Rooting the device

Different approaches to own the device:

- Over the network: telnet/SSH
- Finding a serial port and get login prompt
- Sniffing on the Ethernet line
- JTAG or Re-flashing
Finding a serial port

- We analyzed two devices
- There are many testing points available on the board, look near the CPU
- Simply find 3.3V pins using a multimeter
- Can also use oscilloscope to confirm the serial output
Getting login prompts

- Both the devices provide serial ports

- The first device was simple to 'Root':
  - Has login prompt activated by default
  - Even boot loader can be stopped and used to boot in single user mode

- The second device has a bit “advanced” security:
  - It does not give login prompt, doesn't react to any keystroke combination
  - The boot loader can not be interrupted
  - It stops printing out information on the screen after a certain point
Monitoring the network

- When it starts, everything goes over IPsec
  - Some DNS and NTP request at the beginning
  - It has a webserver (and that's the only port/service available)
  - Almost everything can be configured over this interface
  - The credentials are unknown and maybe provided by the operator over IPsec

- When put into recovery mode, it's more interesting and less secured
  - Recovery mode is existed to update the device firmware
  - Or to repair the partitions if broken
Recovery procedure

1. Small recovery bootloader (uboot)
2. Download and start a recovery image
3. Get the latest download list
4. Download and flash the new images
5. Reboot

Every steps seems to be secured:
- The images are encrypted and signed
- The download list is grabbed over HTTPS
Recovery to failure

1. Small recovery bootloader
   - Can also boot unencrypted recovery image (flaw 1)

2. Download and start a recovery image
   - Over HTTP, with credentials. The recovery image is encrypted
   - Look around, and find an unencrypted version (flaw 2)
Recovery to failure

3. Get the latest download list
   − Over HTTPS with certificates, but not secured (flaw 3)
   − Unsigned and unencrypted (flaw 4)

4. Download and flash the new images
   − Over plain HTTP but encrypted
   − Keys are available to decrypt (do the same undex scratchbox)
   − Flashing success is reported (over HTTPS, with ack)

Resolving sect.ubiquisys.com... 192.168.10.1
Connecting to sect.ubiquisys.com[192.168.10.1]:443... connected.
WARNING: Certificate verification error for sect.ubiquisys.com: self signed certificate
WARNING: certificate common name `sect.ubiquisys.com` doesn't match requested host name
HTTP request sent, awaiting response...
HTTP/1.1 200 OK
Your mine: pwnd

- Setup a fake recovery server (DNS, NTP, and HTTP[S])
- Change some parameters
  - The download list is unprotected and contains critical settings
  - The encryption and signing process have classical weaknesses (flaw 5) may add a trojan here
- Be root
  - A several modes available: commercial, testing, ...
  - Choose the right one: get login prompt
  - The root password is MD5 stored: ask John
Analysis of the Research

- Effective technology in terms of offloading the traffic and of new business cases
- Provides higher data rates to the user … but ....
- The device security is very weak
- Some serious threats
  - Could open gates to the Telecom infrastructure elements (like HLR)?
  - A very cheap IMSI catcher device? (We have not tried it, swear to God!)
  - Might used as MiTM device while calling
  - Might be used as a free home gateway for VoIP
References

  http://www.3gpp.org.


- 3GPP TR 33.820 V8.3.0: 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Security of H(e)NB;(Release 8)

- The nanoBTS: small GSM basestations.
  http://www.ipaccess.com/picocells/nanoBTS picocells.php
Demo
Questions?

Thank U

for more information: www.securityint.de