Hacking Femtocells

a femtostep to the holy grail

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
  – Monty Python
Contents

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

- low power wireless device
- supports any 3G mobile device
- provide 3G coverage for places where macrocells can not
- 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
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 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 < 100 euro + normal phone subscription
- **No Roaming** is allowed on the Femtocells

Small base station?
<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
- NodeB
- RNC
- Uu
- UuCS
- IuPS
- IuCS
- Iuh
- TR-069
- HNB-GW
- SeGW
- IPsec

- CS: Circuit Switched
- MSC
- SGSN
- PS: Packet Switched
- CN: Core Network

- HNS: Home NodeB Subsystem
- UTRAN: Universal Terrestrial Radio Access Network
- AN: Access Network

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

Ravishankar B. & Kévin Redon
Hacking Femtocells
t2'10 infosec
Femtocell Architecture

- femtocell Device aka HNB (Home NodeB)
- Security Gateway (SeGW)
- Operation, Administration & Management server (OAM)
- User Equipment (UE)
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

User controlled

Operator controlled

ME

HNB

Network

Internet

AN

GW

CS/PS
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 Locking Methods

- **geoIP**
  - UE
  - HNB
  - Internet
  - GW

- **macrocells**
  - BTS/nodeB signal
  - HNB

- **GNSS**
  - GNSS signal
  - HNB

- **UE reports**
  - GNSS
  - ME
  - HNB
On the Device

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

<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 :-(
Breaking locks – GNSS (GPS)

- tools you need: GPS jammer or GPS spoofer
- go indoor (low GPS signal)
- not all devices have GPS
Breaking locks - macrocells

- tools you need: GSM jammer, fake BTS, or elevator
- LAC and MCC can be faked using fake BTS
- block the signal (jamming, Faraday cage)
Result

what could go wrong? lawful interception
device security analysis
Rooting the device

different approaches to own 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 image downloads and flashes all other images
Recovery to failure

0. recovery file system in also available unencrypted
   you cannot modify it (signed), but at least analyze (tivo)

1. no mutual authentication over HTTPS

2. given public key is not signed

3. all images can now be decrypted and analyzed
Your mine: pwnd

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

- 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
Doors to heaven

a small eye drop behind the SeGW
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 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


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

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

Thank U