introduction to femtocells

Kévin Redon

Technische Universität Berlin, Security in Telecommunications
femtocell@sec.t-labs.tu-berlin.de

OsmoDevCon 2012, Berlin, 24th March 2012
Structure of an UMTS network

ME : Mobile Equipment
MT/TE

UE : User Equipment
USIM
UICC

MS : Mobile Station

AN : Access Network

Node B

cell

Uu

Iub

RNC

Iur

Iu,CS

Iu,PS


CS : Circuit Switched

GMSC

NC

MSC

E

Mc

Nb

AN : Access Network

Internet

Internet

PSTN

VLR

HSS

HLR

AuC

SecT / TU-Berlin
Femtocells: offloading technology

- technical name in 3G: Home Node B (HNB)
- technical name in 4G: Home evolved Node B (HeNB)
- traffic offload from public operator infrastructure
- improve 3G coverage, particularly indoor
- cheap hardware compared to expensive 3G equipment
- the user provides power, Internet connection, maintenance, and still pays for the communication
- different architecture (TS 25.467) more security required (TS 33.302, TR 33.820)
small cells
SFR femtocell

- 39 femtocell offers over 24 countries
- target sold by SFR (2nd biggest operator in France)
- cost: mobile phone subscription
- hardware: ARM9 + FPGA for signal processing
- OS: embedded Linux kernel + proprietary services
- built by external vendors (in our case Ubiquisys), configured by operator
- HNB is not only an Node B, but also includes a mini RNC (TS 22.220)
- cell configuration is done by the HMS (TS 32.581)
- HNB<->HMS communication is tr-069 (aka ACS), using SOAP/XML/HTTP
- cells asks HMS, but HMS can also push
- most data provided one time, check at every registration, with rare updates
- provisioning data: SeGW address, HNB-GW address, MNC, MCC, ARFCN, GSC, ...
3G IMSI-Catcher

How to build a 3G IMSI-Catcher:

- cell configuration is kindly provided as a feature of femtocells
- some comfort provided ⇒ hidden web interface

- we can catch any phone user of any operator into using our box
- roaming subscribers are allowed by SFR

⇒ the femtocell is turned into a full 3G IMSI-Catcher
mutual authentication

- classical approach in GSM: IMSI-Catcher
  - fake operator BTS (MCC/MNC)
  - acts as MitM between operator and victim
  - phone usually can't detect
  - used to track and intercept communication

- UMTS standard requires mutual authentication
  - mutual authentication is done with the home operator, not with the actual cell
  - the femtocell forwards the authentication tokens
  - mutual authentication is performed even with a rogue device
I$_u$h protocols:
- I$_u$p: I$_u$b over IP
- IMS/SIP
- Generic Access Network (GAN)

GAN:
- UMA specified by operators in 2004
- standardized by 4GPP in 2005 into GAN (TS 44.318, TS 43.318)
- designed for MS$\leftarrow$MNO communication over IP (WiFi)
- borrowed for femtocells, but needs to be adapted
device is communicating with operator via GAN protocol (UMA)
- TCP/IP mapped radio signaling
- encapsulates radio Layer3 messages (MM/CC) in GAN protocol
- one TCP connection per subscriber
- radio signaling maps to GAN messages are sent over this connection

GAN usage is transparent for the phone
but what about over-the-air encryption?

- only the phone ↔ femtocell OTA traffic is encrypted
  ⇒ encryption/decryption happens on the box

- femtocell acts as a combination of RNC and Node-B: receives cipher key and integrity key from the operator for OTA encryption

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>UMA GA-CSR UPLINK DIRECT TRANSFER[DTAP] (MM) Authentication Resp</td>
<td></td>
</tr>
<tr>
<td>UMA Unknown URR (144)</td>
<td></td>
</tr>
</tbody>
</table>

- reversing tells us: message is **SECURITY MODE COMMAND** (unspecified RANAP derivate), which includes the keys
derived from RANAP, but spec unknown
- OTA encryption optional
- traffic decoded in the HNB
- the only the SeGW access it used for authentication/encryption when connection
- all traffic in plain text
- same in HeNB (with stronger trusted core requirement)
proxies all GAN connections/messages
reconfigure femtocell to connect to our proxy instead of real GANC
proxy differs between GAN message types
attack client controls GAN proxy over extended GAN protocol
- interception (SMS in GAN, voice over RTP)
- modification (because of the point to point design)
- injection (need the phone for authentication)
IMSI detach DoS discovered by Sylvaint Munaut in 2010

\[ \Rightarrow \text{results in discontinued delivery of MT services (call, sms,...)} \]
\[ \Rightarrow \text{network assumes subscriber went offline} \]

- detach message is unauthenticated
- however, this is limited to a geographical area (served by a specific VLR)
- user can not receive calls

\[ ^1 \text{http://security.osmocom.org/trac/ticket/2} \]
proximity constraint not existent in femtocell network

- devices reside in various geographical areas
- but all subscribers meet in one back-end system ⇒ and they are all handled by one femtocell VLR (at least for SFR) 😊

- we can send IMSI detach payloads via L3 msg in GAN
  ⇒ we can detach any femtocell subscriber, no proximity needed!
thank you for your attention
questions?
Nico Golde <nico@sec.t-labs.tu-berlin.de>  
@iamnion

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

Ravi Borgaonkar <ravii@sec.t-labs.tu-berlin.de>  
@raviborgaonkar

or just femtocell@sec.t-labs.tu-berlin.de