

introduction to femtocells

Kévin Redon

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

OsmoDevCon 2012, Berlin, 24th March 2012

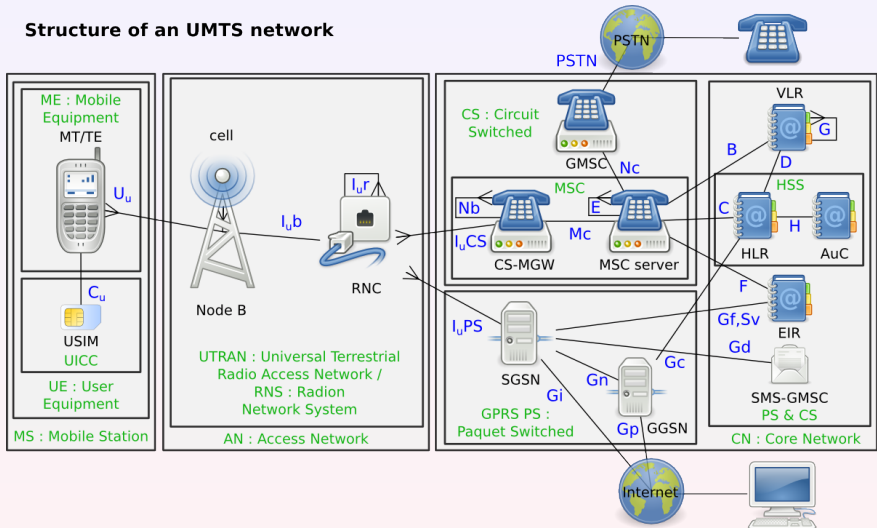


OsmoDevCon



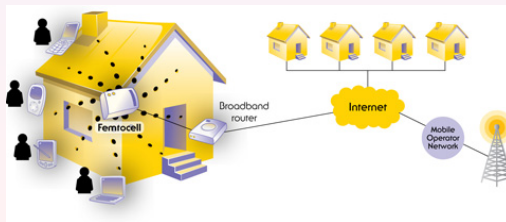
UMTS architecture

Structure of an UMTS network



femtocells: offloading technology

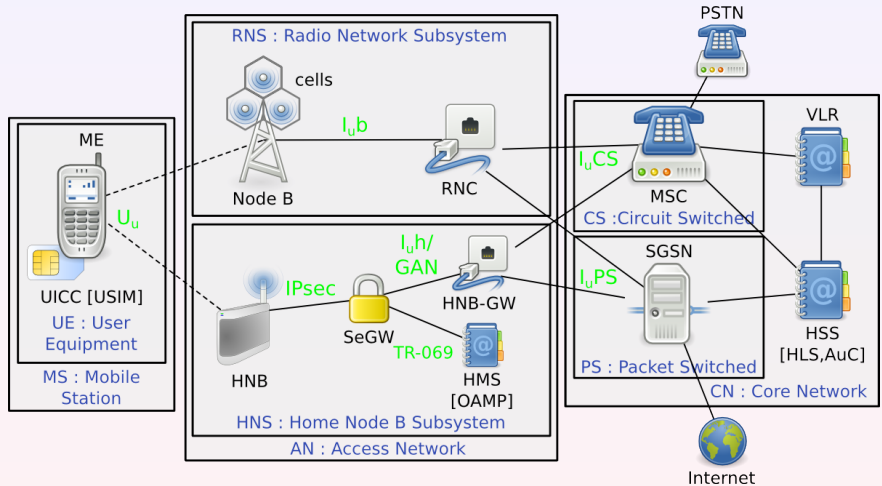
- technical name in 3G: Home Node B (HNB)
- technical name in 4G: Home evolved Node B (HeNB)
- traffic offload from public operator infrastructure
- improve 3G coverage, particularly indoor
- cheap hardware compared to expensive 3G equipment
- the user provides power, Internet connection, maintenance,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



small cells



Home Node B Subsystem (HNS)



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



Command and Control

- 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 communicatio 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

Howto build a 3G IMSI-Catcher:

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

Access Control Mode

Max Open-Access Users

Calls Reserved For Registered Users

MCC (3 digits 0-9)

MNC (2 or 3 digits 0-9)

Open Access

Open Access

Semi-Open

Closed

208

11

Home Zone SFR Home 3G

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



HNB<->HNB-GW communication

■ I_uh protocols:

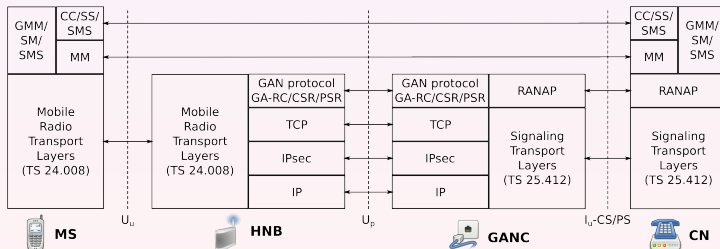
- I_up: I_ub over IP
- IMS/SIP
- Generic Access Network (GAN)

■ GAN:

- UMA specified by operators in 2004
- standardized by 4GPP in 2005 into GAN (TS 44.318, TS 43.318)
- designed for MS<->MNO communication over IP (WiFi)
- borrowed for femtocells, but needs to be adapted

Generic Access Network (GAN)

- 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 \Leftrightarrow femtocell OTA traffic is encrypted
 \Rightarrow 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

| Protocol | Info |
|----------|--|
| UMA | GA-CSR UPLINK DIRECT TRANSFER(DTAP) (MM) Authentication Resp |
| UMA | Unknown URR (144) |

- reversing tells us: message is **SECURITY MODE COMMAND** (unspecified RANAP derivate), which includes the keys

SECURITY MODE COMMAND

- derived from RANAP, but spec unknown

| | | | | | | | | | | | | | | | | | | | |
|--|-----|----|----------------|----|----|----|------|-----|----|-----|-----|------------|----|-------|---------|----------|--|--|--|
| Header length: 20 bytes | | | | | | | | | | | | | | | | | | | |
| ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Default) | | | | | | | | | | | | | | | | | | | |
| Total Length: 99 | | | | | | | | | | | | | | | | | | | |
| Identification: 0xeffc (61436) | | | | | | | | | | | | | | | | | | | |
| ▷ Flags: 0x02 (Don't Fragment) | | | | | | | | | | | | | | | | | | | |
| Fragment offset: 0 | | | | | | | | | | | | | | | | | | | |
| 0000 | 02 | 02 | 02 | 02 | 02 | 02 | 01 | 01 | 01 | 01 | 01 | 08 | 00 | 45 | 00 | | | | |
| 0010 | 00 | 63 | ef | fc | 40 | 00 | 3e | 06 | 8d | 00 | ac | 14 | 28 | 14 | ac | 13 | | | |
| 0020 | 3f | 5c | integrity prot | | | | algo | | | | key | | | | enc key | | | | |
| 0030 | 00 | 0c | cb | 72 | 00 | 00 | 01 | 01 | 00 | 0a | 58 | ff | 58 | 20 | 00 | 0a | | | |
| 0040 | d5 | 6f | 00 | 2d | 01 | 90 | 4b | 11 | 00 | 14 | e8 | 79 | a8 | 7b | d6 | 2f | | | |
| 0050 | ac | 55 | c5 | 9a | 8e | 1e | 60 | 44 | 8c | 4d | 01 | 01 | 4c | 13 | 02 | 6e | | | |
| 0060 | 08 | db | c4 | ba | 4d | 5e | f4 | d1 | 63 | a6 | 37 | 12 | 92 | d4 | e4 | 01 | | | |
| 0070 | 00 | 01 | 02 | 03 | 04 | 05 | 06 | key | | | | key status | | | | algo num | | | |
| 0080 | alg | 01 | 2f | 2c | 81 | 29 | 20 | 45 | 19 | len | | | | value | | | | | |
| choice list | | | | | | | | | | | | | | | | | | | |

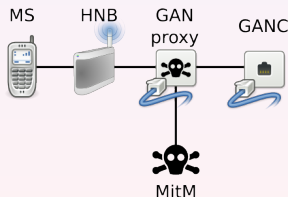
plain text

- 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)



GAN proxy/client

- 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)

```

~Unlicensed Mobile Access
Length Indicator: 38
0000 .... = Skip Indicator: 0
.... 0001 = Protocol Discriminator: URR (1)
URR Message Type: GA-CSR UPLINK DIRECT TRANSFER (112)
~L3 Message
  URR Information Element: L3 Message (26)
  URR Information Element length: 34
  .... 1001 = Protocol discriminator: SMS messages (9)
  L3 message contents: 39011f00010007913306091093f013151c0f810094712627...
  ▶ GSM A-I/F DTAP - CP-DATA
  ▶ GSM A-I/F RP - RP-DATA (MS to Network)
  ~GSM SMS TPDU (GSM 03.40) SMS-SUBMIT
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0... .... = TP-UDHI: The TP UD field contains only the short message
    ..0. .... = TP-SRR: A status report is not requested
    ...1 0... = TP-VPF: TP-VP field present - relative format (2)
    .... 1... = TP-RD: Instruct SC to reject duplicates
    .....01 = TP-MTI: SMS-SUBMIT (1)
    TP-MR: 28
    ▶ TP-Destination-Address - (0049176272)
    ▶ TP-PID: 0
    ▶ TP-DCS: 0
      TP-Validity-Period: 63 week(s)
      TP-User-Data-Length: (3) depends on Data-Coding-Scheme
  ~TP-User-Data
    SMS text: Tdd
  
```


return of the IMSI detach

- IMSI detach DoS discovered by Sylvaint Munaut in 2010 ¹
 - ⇒ results in discontinued delivery of MT services (call, sms,...)
 - ⇒ 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<http://security.osmocom.org/trac/ticket/2>

imsi detach in femtocell ecosystem

- proximity constraint not existent in femtocell network
- devices reside in various geographical areas
- but all subscribers meet in one back-end system \Rightarrow and they are all handled by one femtocell VLR (at least for SFR) 😊
- we can send IMSI detach payloads via L3 msg in GAN
 \Rightarrow we can detach any femtocell subscriber, no proximity needed!

the end

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