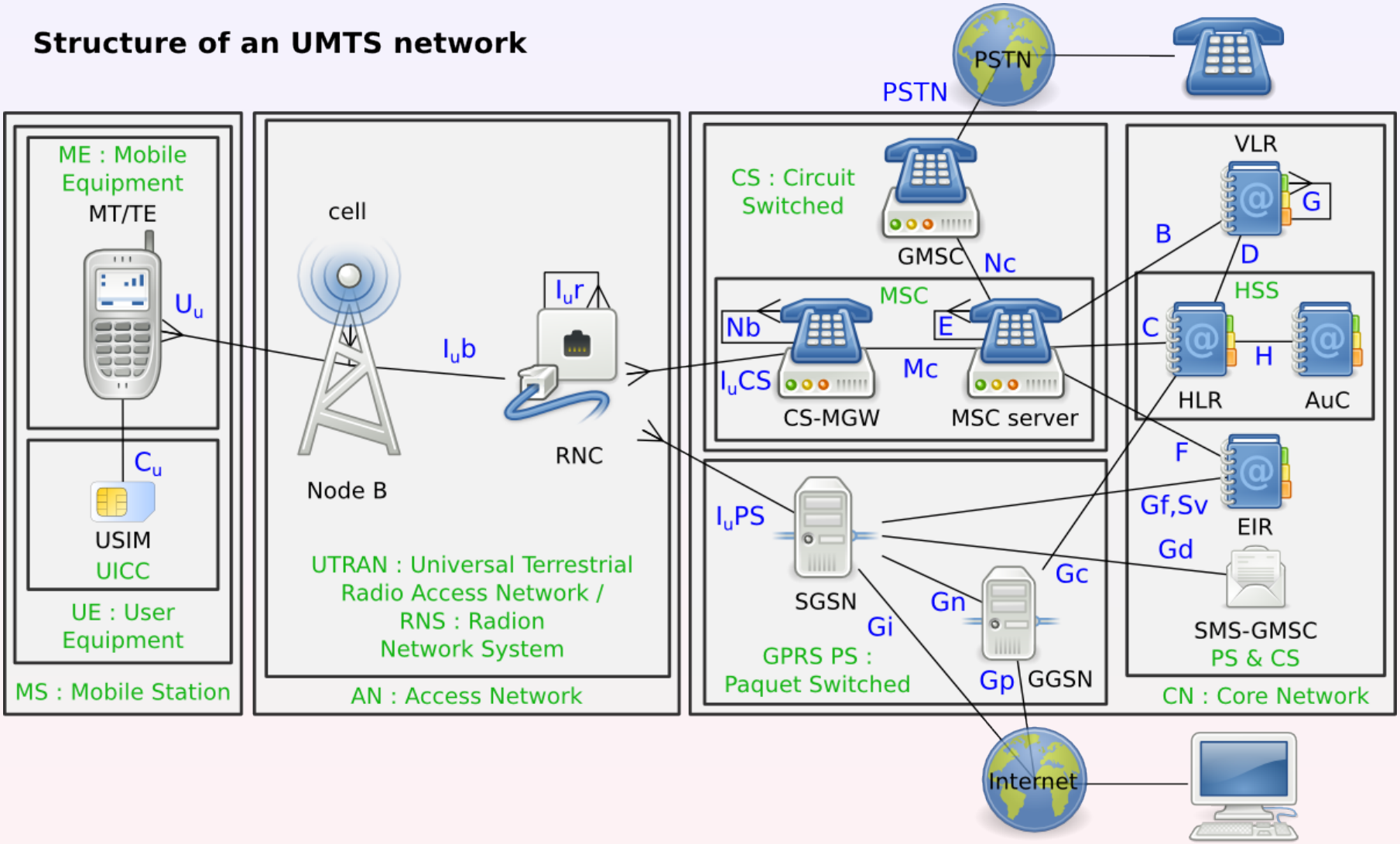
introduction to femtocells

Kévin Redon

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

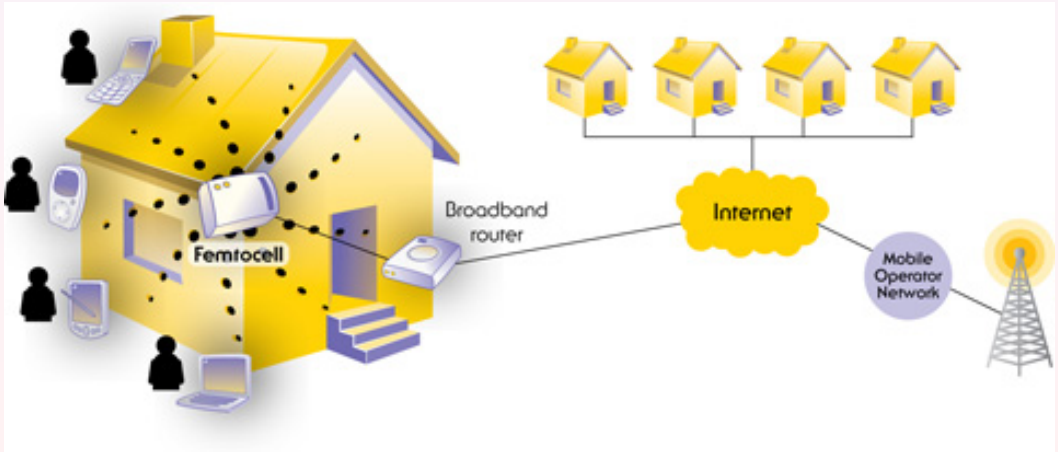
OsmoDevCon 2012, Berlin, 24th March 2012

UMTS architecture



femtocells: offloading technology

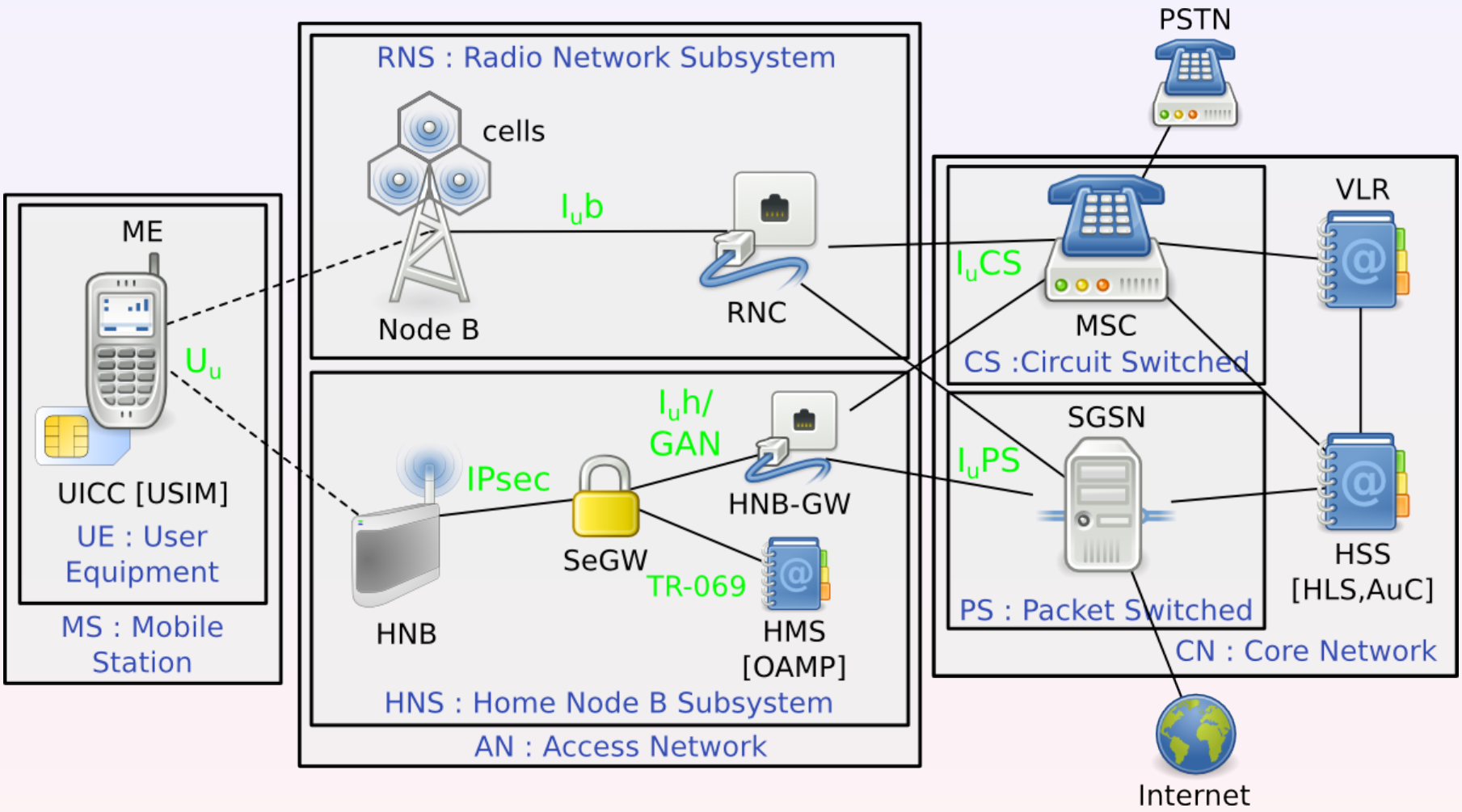
- technical name in 3G: Home Node B (HNB)
- technical name in 4G: Home evolved Node B (HeNB)
- traffic offload from public operator infrastructure
- improve 3G coverage, particularly indoor
- cheap hardware compared to expensive 3G equipment
- the user provides prower, Internet connection, maintenance,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



small cells


macrocells
cell
10^{0}
mini
10^{-3}
micro
10^{-6}
nano
10^{-9}
pico
10^{-12}
femto
10^{-15}
atto
10^{-18}

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

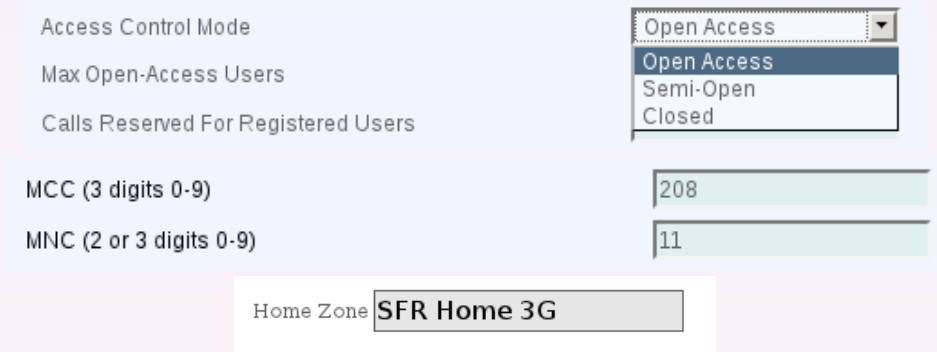
Command and Control

- 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 ⇒ 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

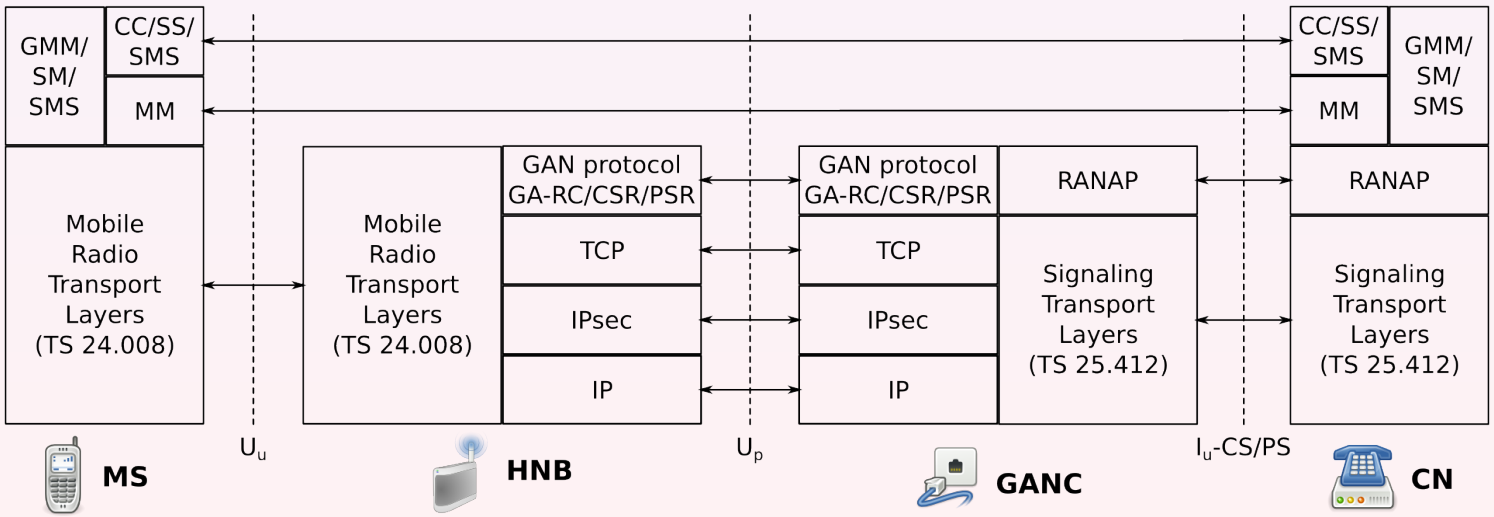
- classical approach in GSM: IMSI-Catcher
  - fake operator BTS (MCC/MNC)
  - acts as MitM between operator and victim
  - phone usually can't detect
  - used to track and intercept communication
- UMTS standard requires mutual authentication
  - mutual authentication is done with the **home operator**, not with the actual cell
  - the femtocell forwards the authentication tokens
  - mutual authentication is performed even with a rogue device

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

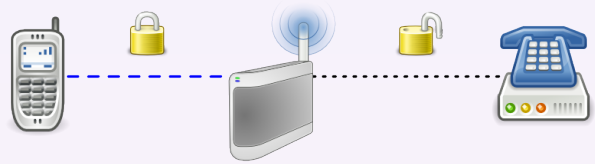
Generic Access Network (GAN)

- 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



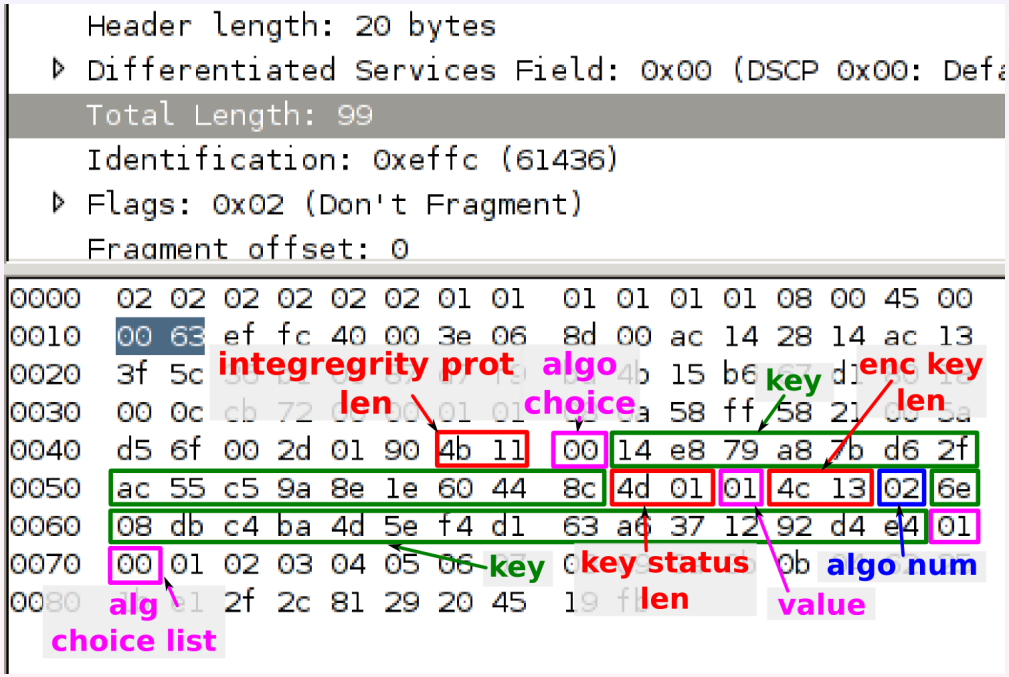
- femtocell acts as a combination of RNC and Node-B: receives cipher key and integrity key from the operator for OTA encryption

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

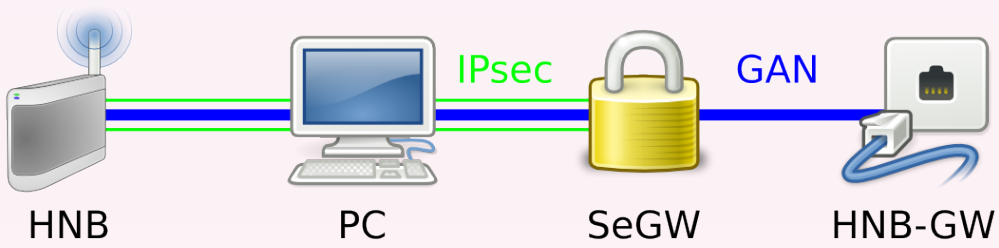
SECURITY MODE COMMAND

- derived from RANAP, but spec unknown



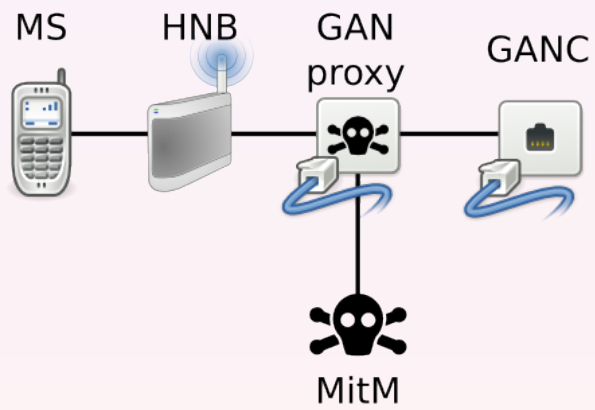
plain text

- 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)



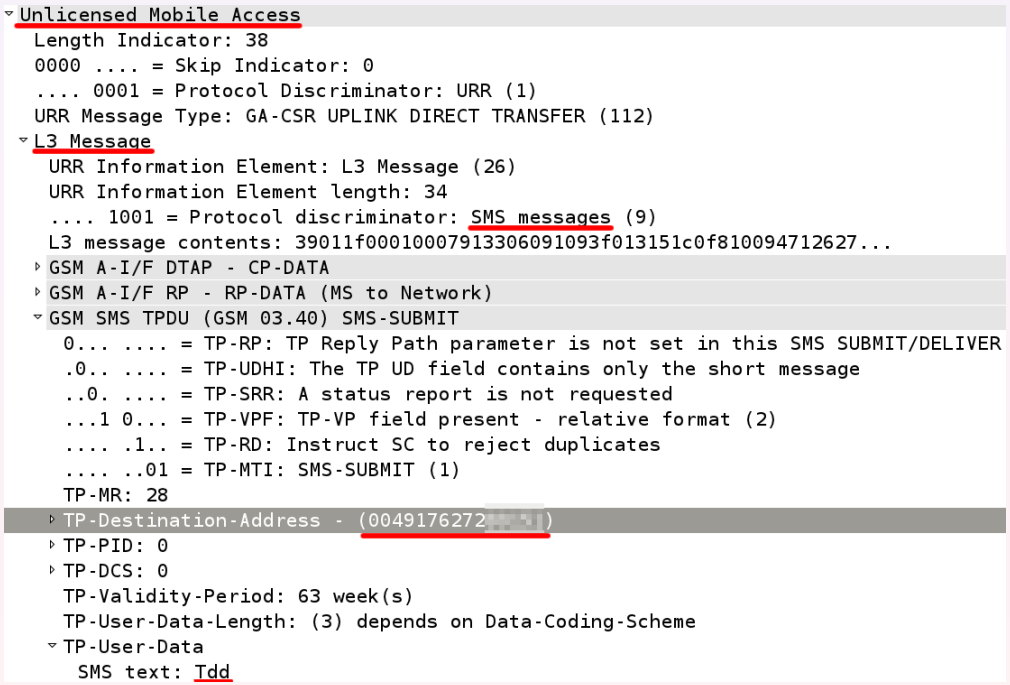
GAN proxy/client

- 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



MitM

- interception (SMS in GAN, voice over RTP)
- modification (because of the point to point design)
- injection (need the phone for authentication)



return of the IMSI detach

- IMSI detach DoS discovered by Sylvaint Munaut in 2010 [1]
  $\Rightarrow$ results in discontinued delivery of MT services (call, sms,...)
  $\Rightarrow$ 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

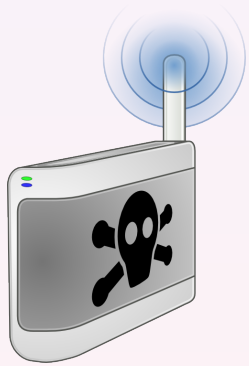
- proximity constraint not existent in femtocell network
- devices reside in various geographical areas
- but all subscribers meet in one back-end system $\Rightarrow$ and they are all handled by one femtocell VLR (at least for SFR) ☺

- 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?



contact us

- 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