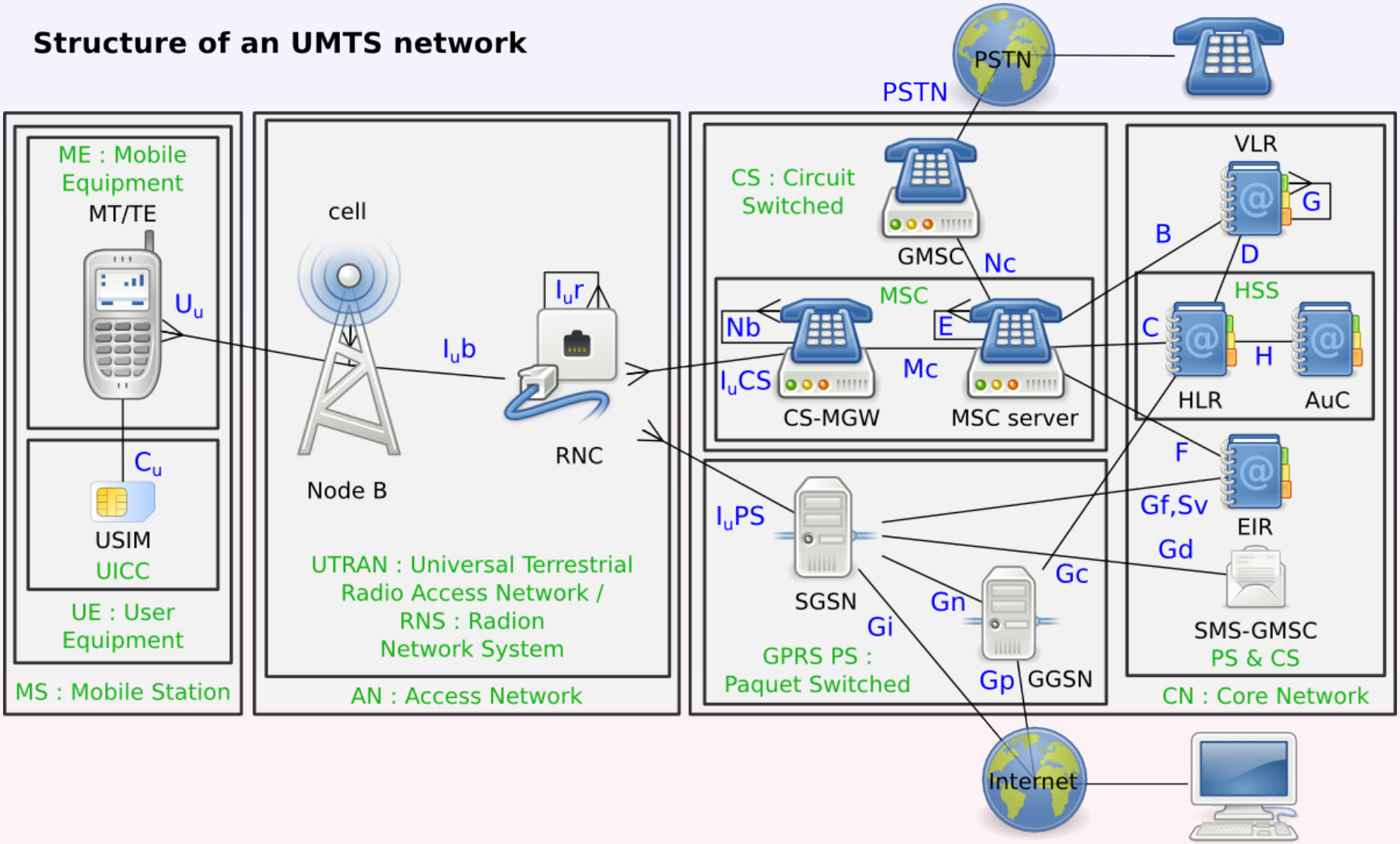
Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunication

Kévin Redon, Nico Golde, Ravishankar Borgaonkar

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

Troopers 2012, Heidelberg, 20th March 2012

messy UMTS architecture

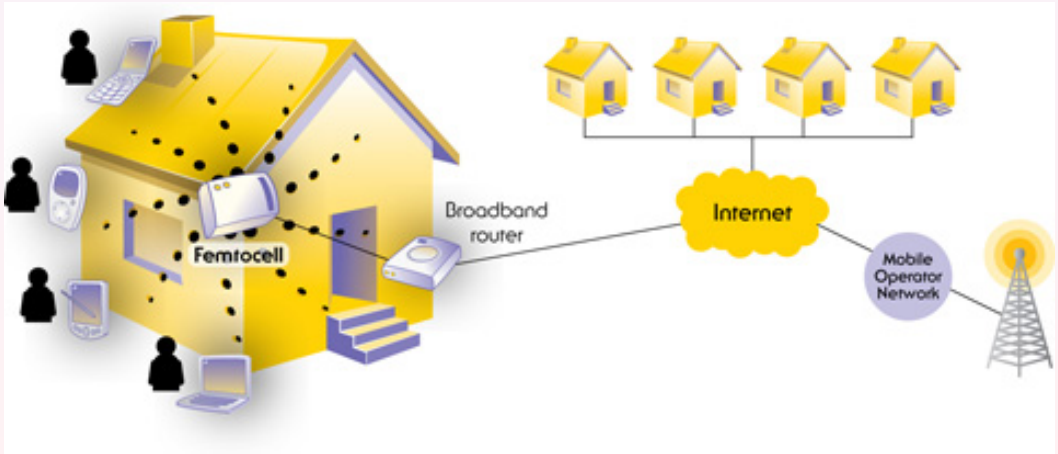


here be dragons

- telecommunication networks are separate and closed networks, not as Internet is
- everything is based on trust and mutual agreement
- there a no evil attacker to defend against
- a critical infrastructure, with millions of users, left unprotected ...

femtocells: offloading technology

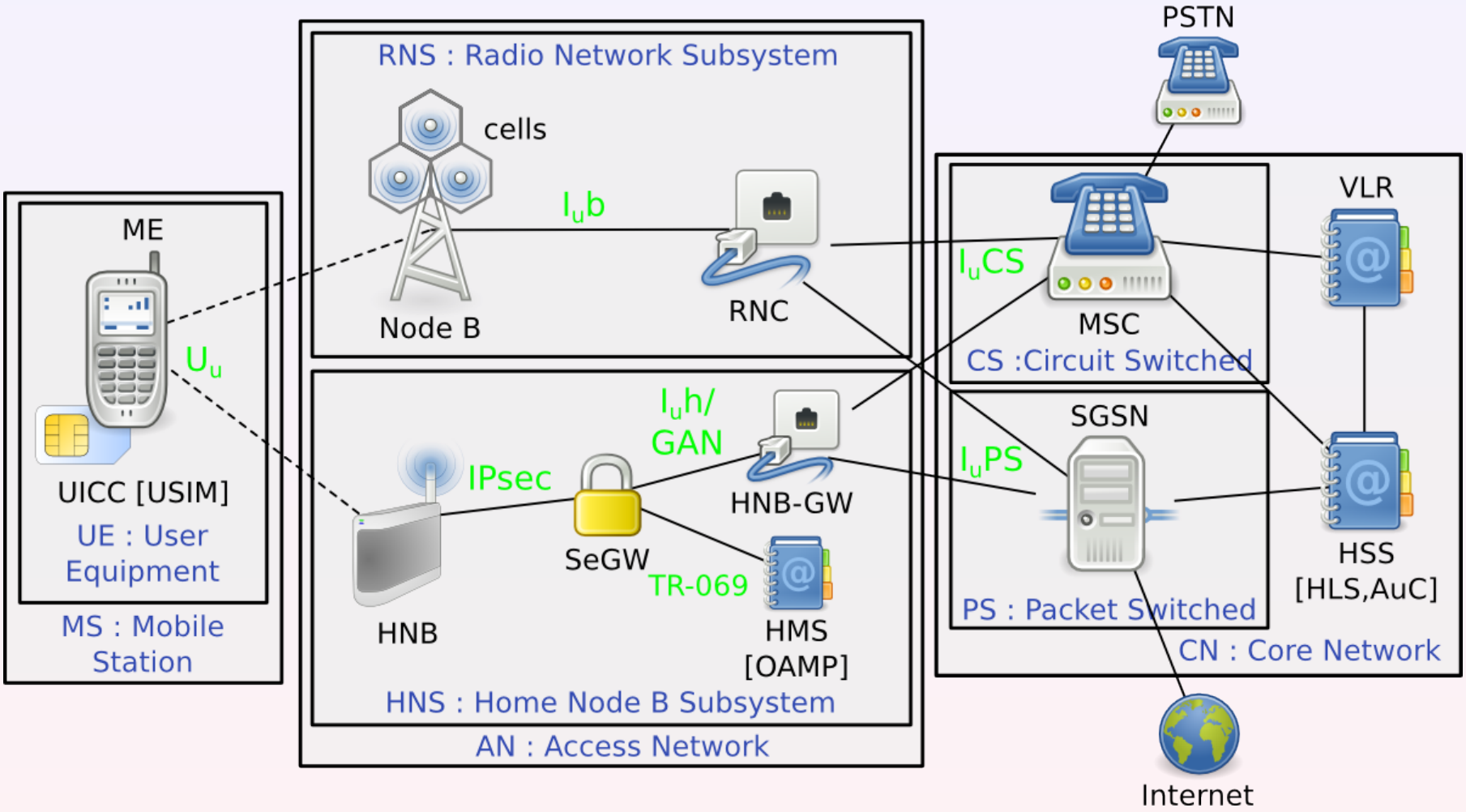
- technical name in 3G: Home Node B (HNB)
- traffic offload from public operator infrastructure
- improve 3G coverage, particularly indoor
- cheap hardware compared to expensive 3G equipment
- the user provides prower, Internet connection, maintenance, and still pays for the communication



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)

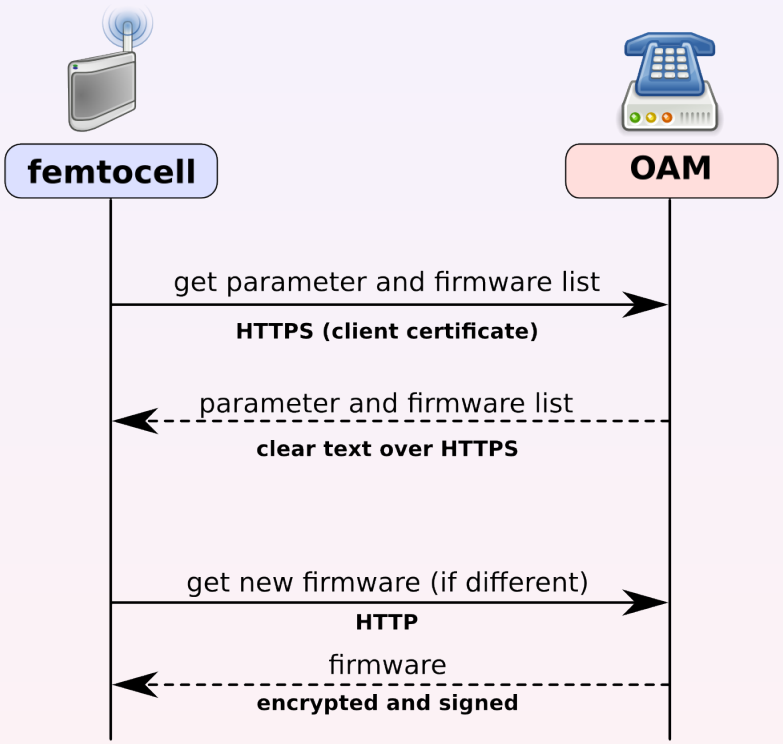


SFR femtocell

- 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

recovery procedure

- femtocells provide a recovery procedure
- similar to a factory reset
- new firmware is flashed, and settings are cleared
- used to "repair" the device without any manual intervention



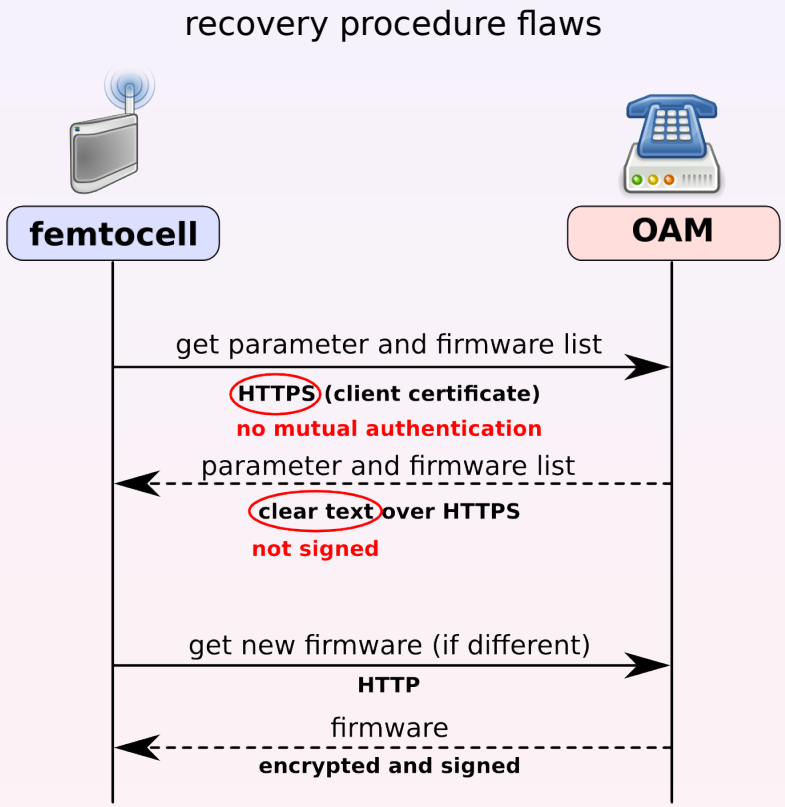
recovery to fail

- firmware server is not authenticated

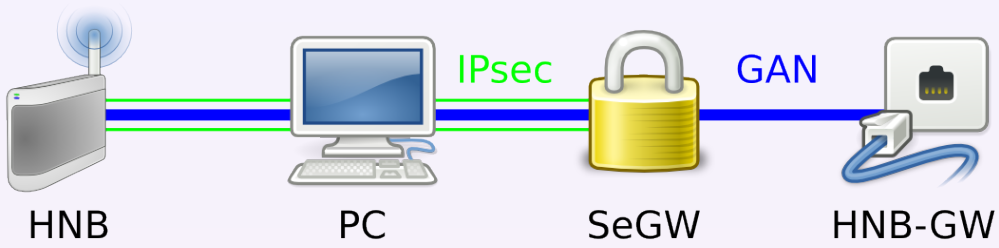
```
408  FULLPRODUCTCODE="$PRODUCTCODE-$PLATFORM$FEATU
409  QUERY="?productcode=$FULLPRODUCTCODE&version=
     $PCBID&flashid=$FLASHID&keyid=$KEYID&boot=$BO
     biqfs=$UBAVERSION"
410  WGETOPTS="--no-check-certificate
     --certificate=/etc/tls/certs/client.crt
     --private-key=/etc/tls/private/client.key
     --ca-certificate=/etc/tls/certs/server.crt"
411
```

- public key is in parameter and firmware list, which is not signed

```
1   ## CUSTOMISATION.INI START
2   [General]
3   pcbid=P04S80005[illegible]
4   imei=35753901038[illegible]
5   mac=00:1B:67:00:98:[illegible]
6   hwflag=2
7   serial=P04S80005[illegible]
8
9   [Hardware]
17  [Recovery]
22  [BootSigning]
23  pubkey=
    BE:73:A2:EE:C0:35:40:4A:9C:1
    4:EA:0A:B8:45:D6:3F:18:3B:95
    :EB:98:76:CF:65:DA:39:D9:D1:
    F0:8C:55:E3:A3:54:5E:28:9B:B
    8:75:05:69:B8:0C:B7:5A:8C:1B
    :3A:4A:48:FC:C1:47
24
25  ## CUSTOMISATION.INI END
```



intercepting traffic

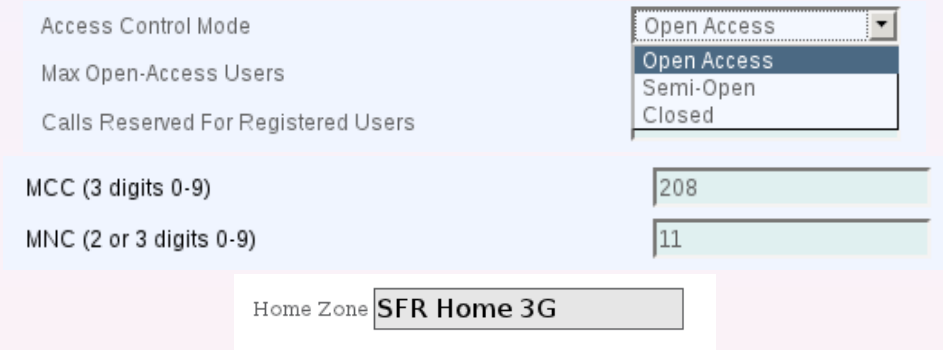


- proprietary IPsec client + kernel module (xpressVPN)
  ⇒ LD_PRELOAD ipsec user-space program to hijack sendto() and extract keys, so to decrypt ESP packets
- voice data encapsulated in unencrypted RTP stream (AMR codec, stream format)
  ⇒ extract RTP stream (rtpbreak), extract AMR and dump to WAV (opencore-based)

getting the fish into the octopus' tentacles

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

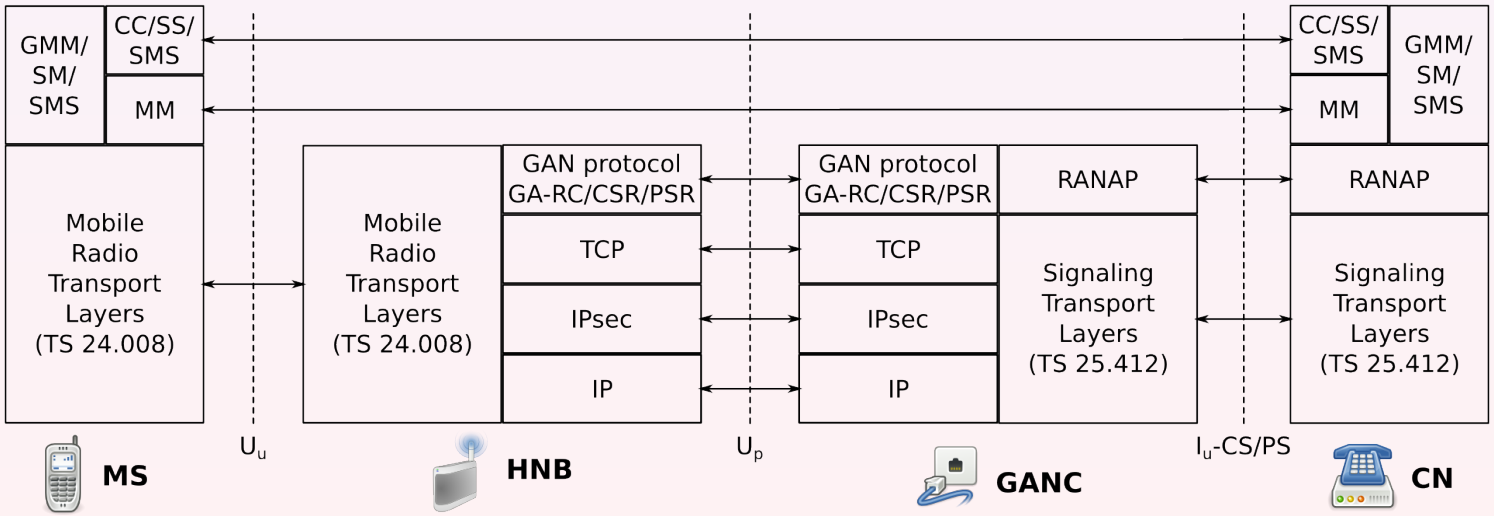
⇒ the femtocell is turned into a full 3G IMSI-Catcher

mutual authentication in the femtocell ecosystem

- 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

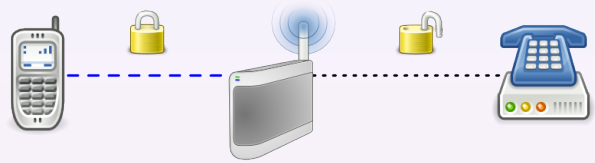
femtocell operator communication: the GAN protocol

- 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



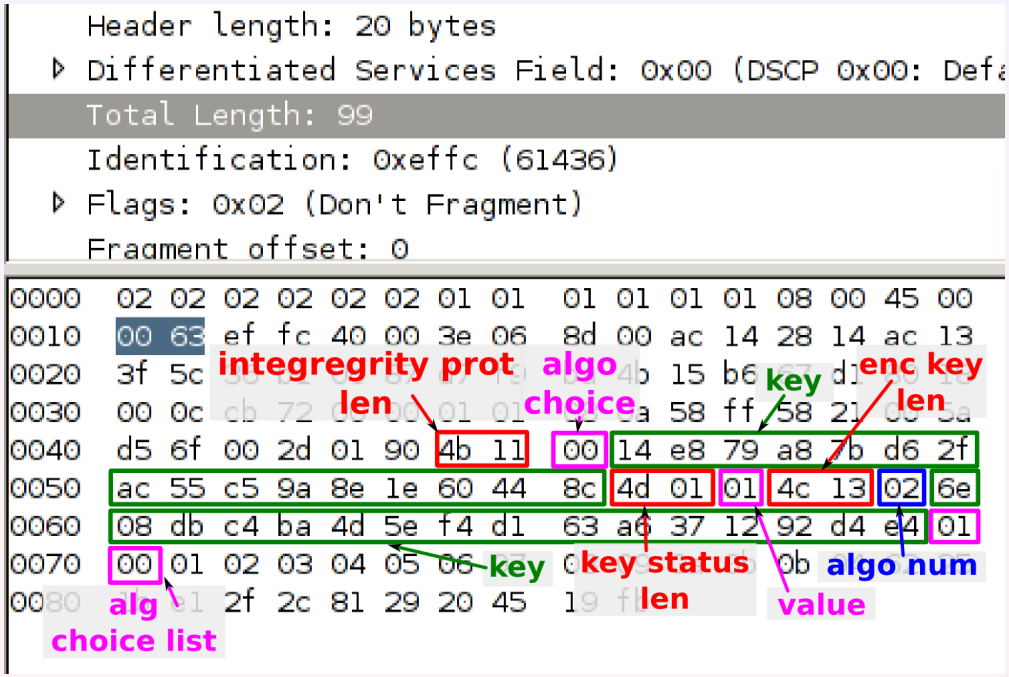
- femtocell acts as a combination of RNC and Node-B: receives cipher key and integrity key from the operator for OTA encryption

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

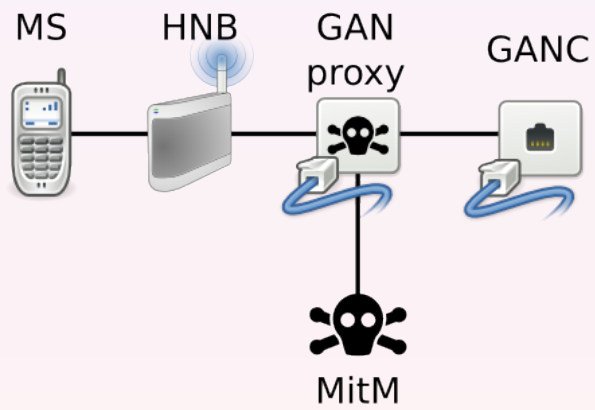
SECURITY MODE COMMAND

- derived from RANAP, but spec unknown



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



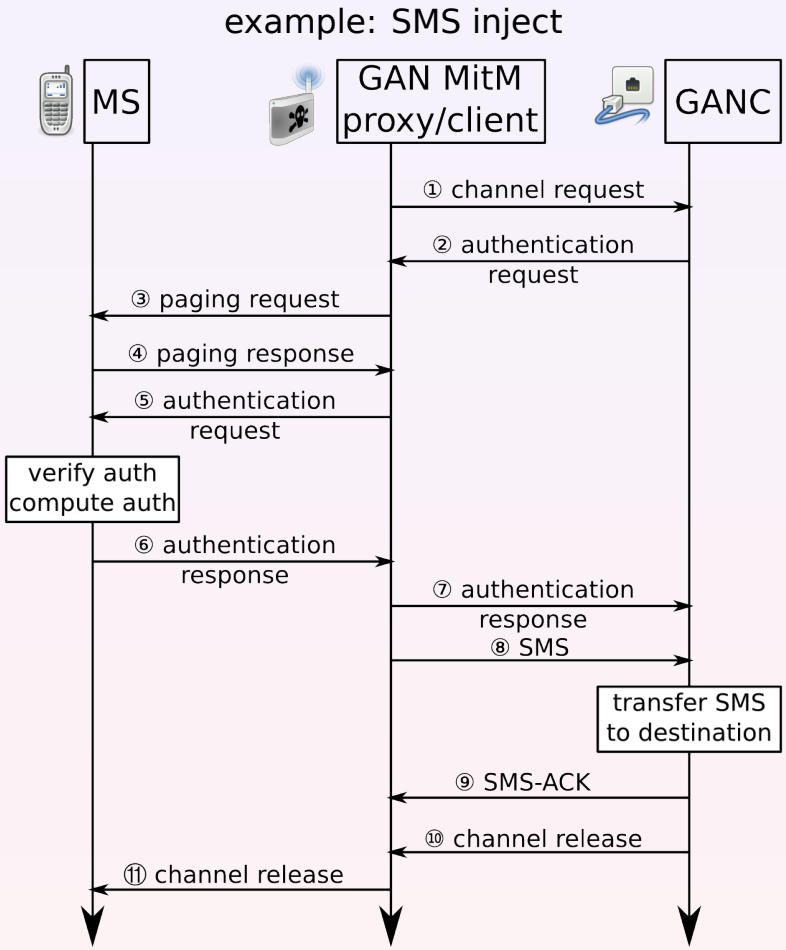
more mitm pls? sms...

- SMS message filtered by GAN proxy
- modified by client
- transfered to real GANC

```
▾ 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: 39011f000100079133060910 93f013151c0f810094712627...
    ▸ 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[redacted])
      ▸ 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
```

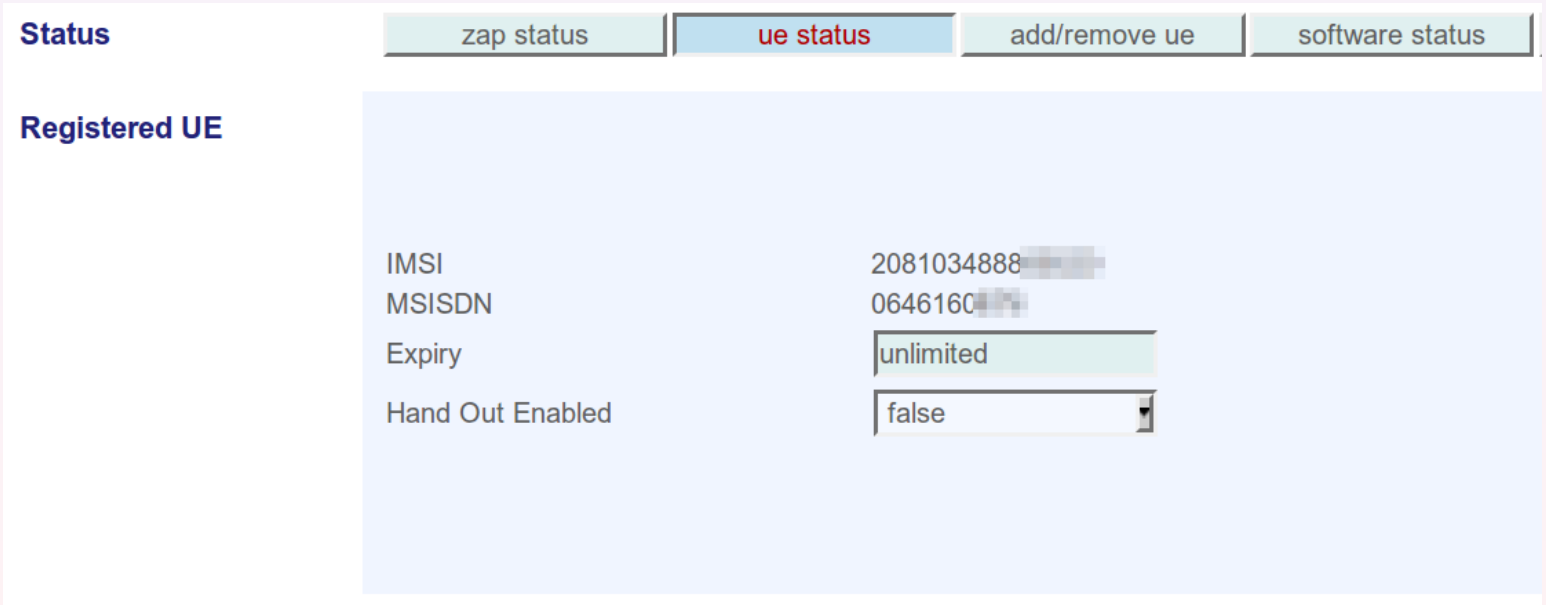
how about impersonating subscribers?

- lets use services for free, billed to a victim
- client requires subscriber information
- proxy additionally caches subscriber info (TMSI/IMSI) for each MS-GANC connection
- phone needed for authentication
- applies to any traffic (SMS,voice,data)
- victim is impersonated



collecting subscriber information

- other femtocell are accessible within the network
- website is also accessible
- leaks **phone number** and IMSI of registered subscriber



locating subscribers

- location verification performed by OAM
- femtocell scan for neighbour cells

Engineering

RRM | General | Neighbour | CellConf | RRCtimers | UEtimers | ComCh | RabPar | RANAP/NAS

UMTSMac | UMTSZAF | GSMMacr

Neighbour GSM Macros List

Cell Id	MCC	MNC	LAC	RAC	Freq	ARFCN	NCC	BCC	UlTxPwr	SniffMd	Meas RSSI (dBm)	Delete
27501	208	10	4301	0	DCS 18(	124	3	6	33	true	-93	false
17536	208	10	1100	0	DCS 18(	108	3	0	33	true	-89	false
10259	208	10	4301	0	DCS 18(	520	1	2	30	true	-82	false
8762	208	10	4301	0	DCS 18(	91	1	0	33	true	-81	false
27535	208	10	18000	0	DCS 18(	70	0	5	33	true	-74	false
8689	208	10	4301	0	DCS 18(	115	2	6	33	true	-93	false
12120	208	10	4301	0	DCS 18(	648	0	7	30	true	-78	false
7535	208	10	18000	0	DCS 18(	66	0	7	33	true	-80	false
17535	208	10	18000	0	DCS 18(	86	3	1	33	true	-85	false
19686	208	10	4301	0	DCS 18(	84	3	3	33	true	-94	false

global control

- web-site/database is not read-only
- OAMP, image and GAN server can also be set
- or using root exploit
- traffic can be redirected to our femtocell (either settings or iptables)
  $\Rightarrow$ any femtocell subscriber communication can be intercepted, modified and impersonated

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 ⇒ 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!

attacking other femtocells

- attack surface limited:
  - network protocols: NTP, DNS spoofing (not tested)
  - services: webserver, TR-069 provisioning (feasible)
- both HTTP. TR-069 is additionally powered by SOAP and XML
- lots of potential parsing fail
- all services run as root

femtocell remote root (CVE-2011-2900, not 7870-8559-1831-2856-1651)

- we went for the web service (wsal)
- based on shttpd/mongoose/yassl embedded webserver
- we found a stack-based buffer overflow in the processing of HTTP PUT requests
- direct communication between femtocells is not filtered by SFR
- exploit allows us to root **any** femtocell within the network

$\Rightarrow$ any femtocell can be flashed
$\Rightarrow$ perfect botnet

advanced access

- SeGW is required to access the network
- authentication is performed via the SIM (removable)
- how about configuring an IPsec client with this SIM?

⇒ no hardware and software limitation
⇒ no femtocell required anymore
⇒ femtocells don't act as a great wall to protect the operator network anymore :D
⇒ it also works with normal phone SIMs

meeting the usual suspects

HNS servers run typical Open Source software, not especially secured, e.g:

- MySQL, SSH, NFS, Apache (with directory indexing), ... available
- FTP used to submit performance measurement reports, including femtocell identity and activity
- all devices share the same FTP account
- vsftpd users are system users, SSH is open :D

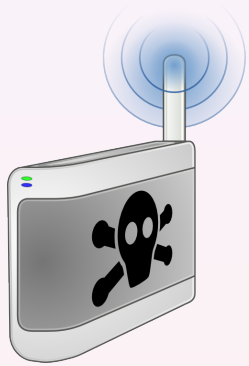
stairways to heaven

- attacks on operator network
- signaling attacks (not blocked)
- free HLR queries
- leveraging access to:
  - other Access Networks
  - Core Network
- ...

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