Femtocells: a Poisonous Needle in the Operator's Hay Stack

Ravishankar Borgaonkar, Nico Golde, Kévin Redon

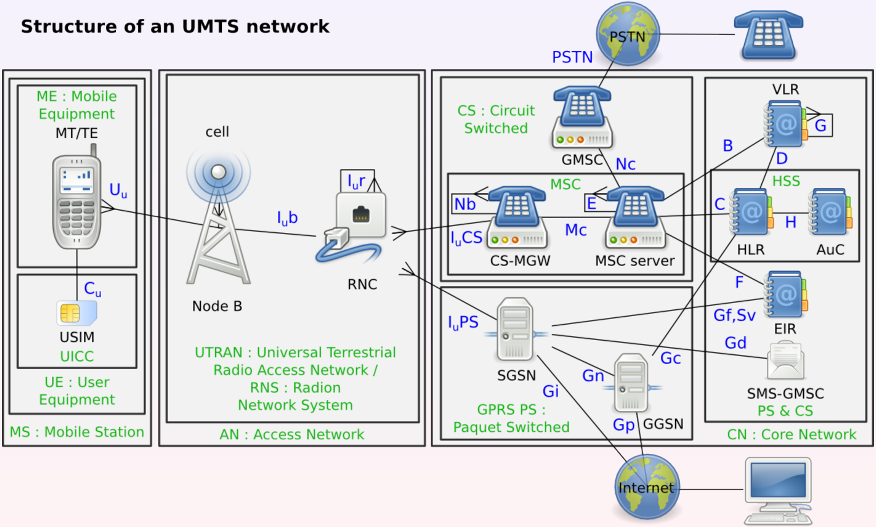
Technische Universität Berlin, Security in Telecommunications
femtocell@sec.t-labs.tu-berlin.de

HITB 2011, Kuala Lampur, 13th October 2011

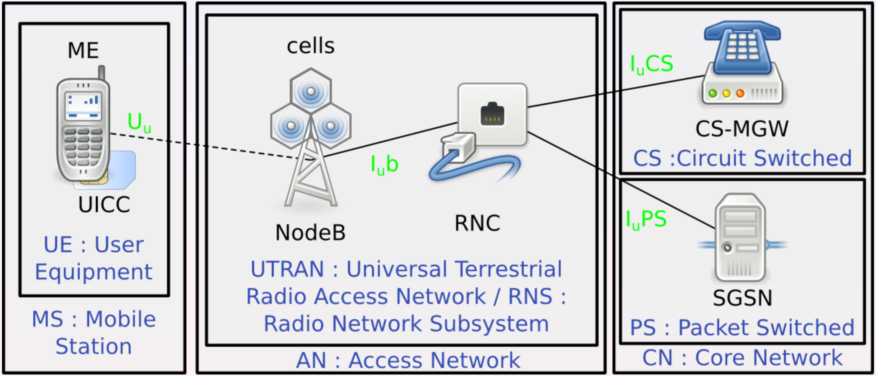
Agenda

- mobile telecommunication
- end-user attacks
- network attacks

UMTS architecture (complex)



UMTS architecture (simplified)



technology - femtocell context?!

What is a femtocell?

- a small access point
- connects the mobile phone to the 3G/UMTS network
- compatible with every UMTS enabled mobile phone
- small cell, with a coverage of less than 50m
- low power device
- easy to install: you only have to provide power and Internet access
- technical name in 3G: Home Node B (HNB)

customer advantages

advantages provided to users:

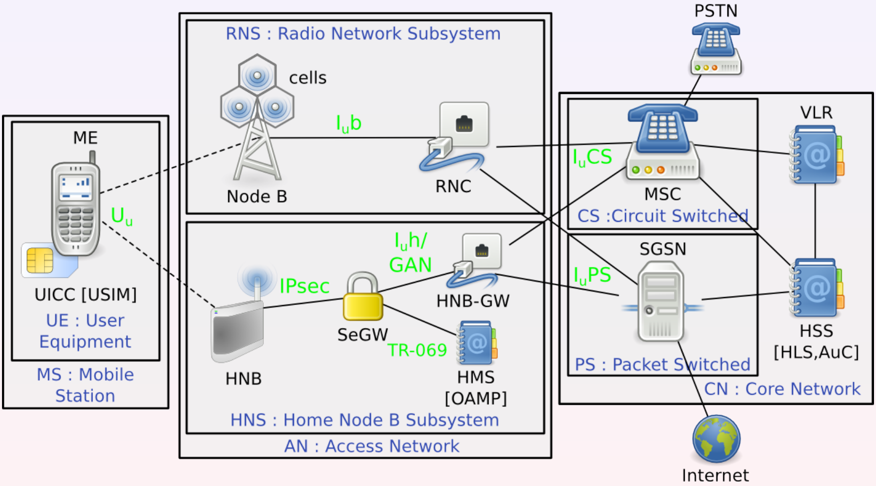
- can be installed at home to improve 3G coverage
- high bandwidth, and high voice quality
- location based services

operator advantages

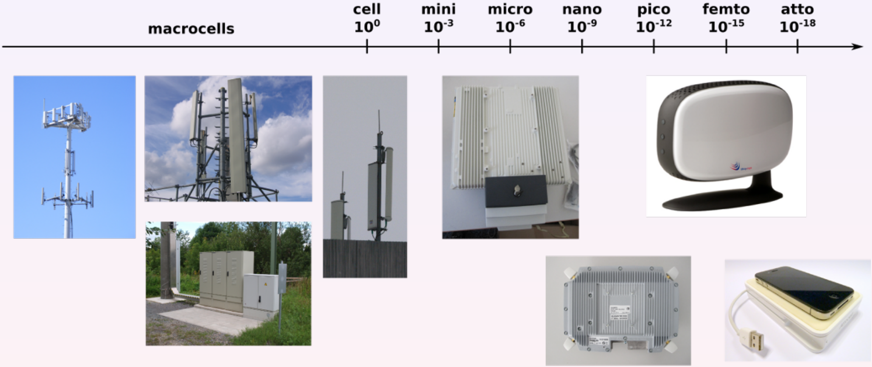
advantages for mobile operators:

- traffic offload from public operator infrastructure ⇒ reduce expenditure
- cheap hardware compared to expensive 3G equipment
- no installation and maintenance cost
- IP connectivity

Home Node B Subsystem (HNS)



small cells



macrocells

cell 10^{0}

mini 10^{-3}

micro 10^{-6}

nano 10^{-9}

pico 10^{-12}

femto 10^{-15}

atto 10^{-18}

femtocell threats (as defined by 3GPP)

HNB threats listed by the 3GPP

group	#	threat	impact
Compromise of H(e)NB Credentials	1	Compromise of H(e)NB authentication token by a brute force attack via a weak authentication algorithm	harmful
	2	Compromise of H(e)NB authentication token by local physical intrusion	harmful
	4	User cloning the H(e)NB authentication Token. User cloning the H(e)NB authentication Token	very harmful
Physical attacks on a H(e)NB	3	Inserting valid authentication token into a manipulated H(e)NB	harmful
	6	Booting H(e)NB with fraudulent software (“re-flashing”)	up to disastrous
	8	Physical tampering with H(e)NB	harmful
	26	Environmental/side channel attacks against H(e)NB	harmful
Attacks on Radio resources and management	21	Radio resource management tampering	harmful
Protocol attacks on a H(e)NB	5	Man-in-the-middle attacks on H(e)NB first network access	very harmful
	15	Denial of service attacks against H(e)NB	annoying
	17	Compromise of an H(e)NB by exploiting weaknesses of active network services	extremely harmful
	25	Manipulation of external time source	harmful
	27	Attack on OAM and its traffic	very harmful
	28	Threat of H(e)NB network access	harmful

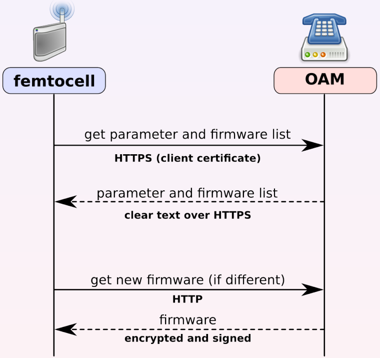
group	#	threat	impact
Attacks on the core network, including H(e)NB location-based attacks	11	Changing of the H(e)NB location without reporting	harmful
	12	Software simulation of H(e)NB	very harmful
	13	Traffic tunnelling between H(e)NBs	very harmful
	14	Misconfiguration of the firewall in the modem/router	annoying
	16	Denial of service attacks against core network	annoying
	24	H(e)NB announcing incorrect location to the network	harmful
User Data and identity privacy attacks	9	Eavesdropping of the other user’s UTRAN or E-UTRAN user data	very harmful
	10	Masquerade as other users	very harmful
	18	User’s network ID revealed to Home (e)NodeB owner	breaking users privacy
	22	Masquerade as a valid H(e)NB	very harmful
	23	Provide radio access service over a CSG	very harmful
Configuration attacks on a H(e)NB	7	Fraudulent software update / configuration changes	extremely harmful
	19	Mis-configuration of H(e)NB	irritating to harmful
	20	Mis-configuration of access control list (ACL) or compromise of the access control list	irritating to harmful

SFR femtocell

- sold by SFR (2nd biggest operator in France)
- cost: 99€ + 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

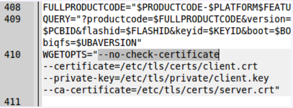
recovery procedure

- 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


femtocell
OAM
get parameter and firmware list
HTTPS (client certificate)
parameter and firmware list
clear text over HTTPS
get new firmware (if different)
HTTP
firmware
encrypted and signed

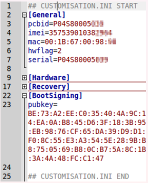
recovery to fail

- firmware server is not authenticated



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

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

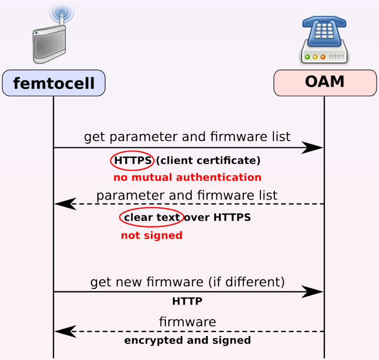


```
## CUSTOMISATION.INI START
[General]
pcbid=P04S80005[redacted]
imei=35753901038[redacted]
mac=00:1B:67:00:98:[redacted]
hwflag=2
serial=P04S80005[redacted]

[Hardware]
[Recovery]
[BootSigning]
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

## CUSTOMISATION.INI END
```

recovery procedure flaws



femtocell

OAM

get parameter and firmware list

HTTPS (client certificate)

no mutual authentication

parameter and firmware list

clear text over HTTPS

not signed

get new firmware (if different)

HTTP

firmware

encrypted and signed

any attacks hmm?

WHAT NOW?

requirements

- classical approach in GSM: IMSI-Catcher
  - fake operator BTS (MCC/MNC)
  - acts as MitM between operator and victim
  - phone usually can't detect
  - usually used to track and intercept communication
- UMTS standard requires mutual authentication $\Rightarrow$ GSM approach not working [1]
- no devices acting as UMTS base station + code is available

[1] some attacks by using protocol downgrades are known

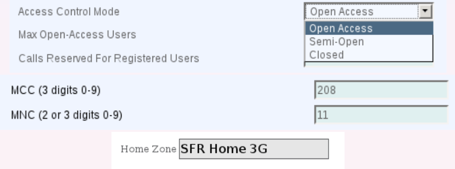
mutual authentication in the femtocell ecosystem

- in case of femtocell: mutual authentication also provided
  ⇒ but it's useless ☺
- 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

getting the fish into the octopus' tentacles

Howto build a 3G IMSI-Catcher:

- cell configuration is kindly provided as a feature of femtocells
- local cell settings stored in a proprietary database format
- some comfort provided ⇒ web interface



Access Control Mode: Open Access

Max Open-Access Users
Calls Reserved For Registered Users

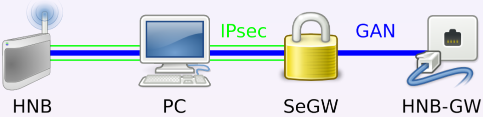
MCC (3 digits 0-9): 208
MNC (2 or 3 digits 0-9): 11

Home Zone: SFR Home 3G

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

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

intercepting traffic



- proprietary IPsec client + kernel module (xpressVPN)
- multiple ways to decrypt IPsec traffic: NETLINK, ip xfrm state (not available on SFR box)
- we decided to hijack/parse ISAKMP messages passed via sendto(2) glibc wrapper
- voice data encapsulated in unencrypted RTP stream (AMR codec, stream format)

extracting voice

- LD_PRELOAD ipsec user-space program to hijack sendto() and extract keys
- pass key material to host running tcpdump
- decrypt ESP packets
- extract RTP stream (rtpbreak)
- opencore-based (nb) utility to extract AMR and dump to WAV

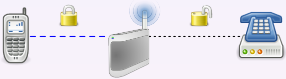
demo time

DEMONSTRATION

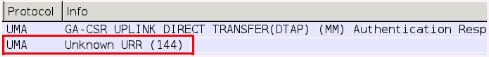
interception

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

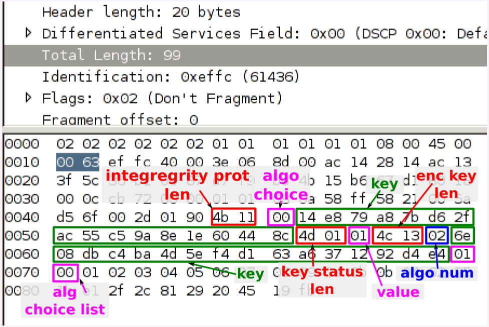


Protocol	Info
UMA	GA-CSR UPLINK DIRECT TRANSFER(DTAP) (MM) Authentication Resp
UMA	Unknown URR (144)

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

SECURITY MODE COMMAND

- derived from RANAP, but spec unknown

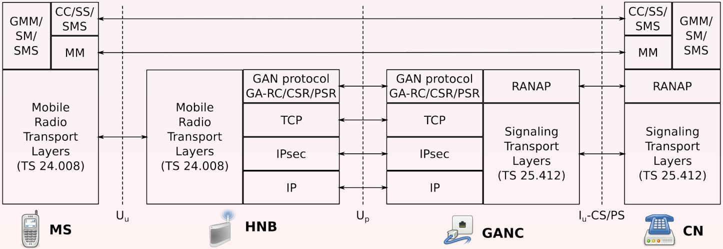


```
    Header length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Defa
    Total Length: 99
    Identification: 0xeffc (61436)
  ▷ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
```

```
0000  02 02 02 02 02 02 01 01  01 01 01 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                     b 15 b6    d1
0030  00 0c cb 72    00 01 01     a 58 ff 58 21 00 5a
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     0                 0b
0080     e1 2f 2c 81 29 20 45  19 f
```

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



GMM/ SM/ SMS

CC/SS/ SMS

MM

Mobile Radio Transport Layers (TS 24.008)

U_u

Mobile Radio Transport Layers (TS 24.008)

GAN protocol GA-RC/CSR/PSR

TCP

IPsec

IP

U_p

GAN protocol GA-RC/CSR/PSR

TCP

IPsec

IP

RANAP

Signaling Transport Layers (TS 25.412)

I_u-CS/PS

CC/SS/ SMS

MM

GMM/ SM/ SMS

RANAP

Signaling Transport Layers (TS 25.412)

MS

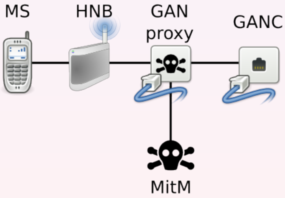
HNB

GANC

CN

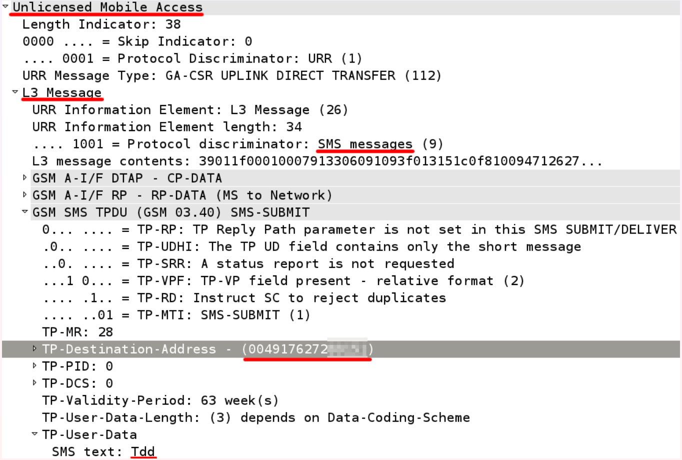
GAN proxy/client

- 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: 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[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
```

demo time

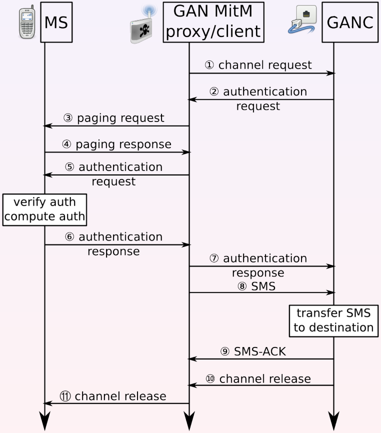
DEMONSTRATION

SMS modification

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

example: SMS inject



demo time

DEMONSTRATION

SMS injection

return of the IMSI detach

- IMSI detach DoS discovered by Sylvaint Munaut in 2010 [2]
  ⇒ 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

[2] 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!

demo time

DEMONSTRATION

IMSI detach

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)

- we went for the web service (wsal)
- based on shttpd [3]/mongoose [4]/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
- `http://www.sec.t-labs.tu-berlin.de/~nico/wsal_root.py`
- fixed in V2.0.24.1 firmware

[3] http://docs.huihoo.com/shttpd/

[4] http://code.google.com/p/mongoose/

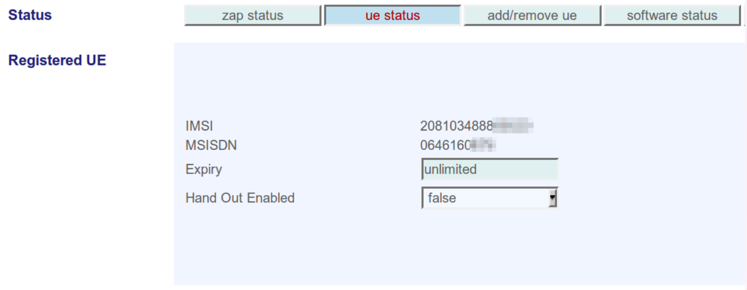
demo time

DEMONSTRATION

remote root

collecting subscribers

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

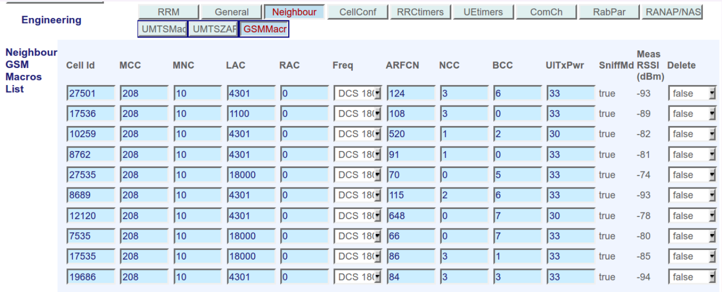


Registered UE

IMSI 2081034888[redacted]
MSISDN 0646160[redacted]
Expiry unlimited
Hand Out Enabled false

locating subscribers

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



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)

⇒ any femtocell can be flashed
⇒ any femtocell subscriber communication can be intercepted, modified and impersonated

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

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

stairways to heaven

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

other femtocell research

- THC vodafone `http://wiki.thc.org/vodafone`, rooted in 2009, unfortunately bug fixed since 2 years
- Samsung femtocell `http://code.google.com/p/samsung-femtocell/`
- clearly shows that this is no single operator problem and might cause some pain
- femtocell architecture is defective by design, security wise

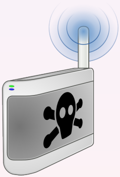
thanks (in no particular order)

- Jean-Pierre Seifert
- Collin Mulliner
- Benjamin Michéle
- Dieter Spaar
- K2

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
- Finally all material from this talk (including tools) will be available one week after the HITB KL at: `http://tinyurl.com/sectfemtocellhacks`

extended coverage

- femtocells have a small coverage (by definition, 25-50m)
- signal range can be increased using amplifier and external antenna