Femtocell: Femtostep to the Holy Grail

Ravishankar Borgaonkar, Kévin Redon

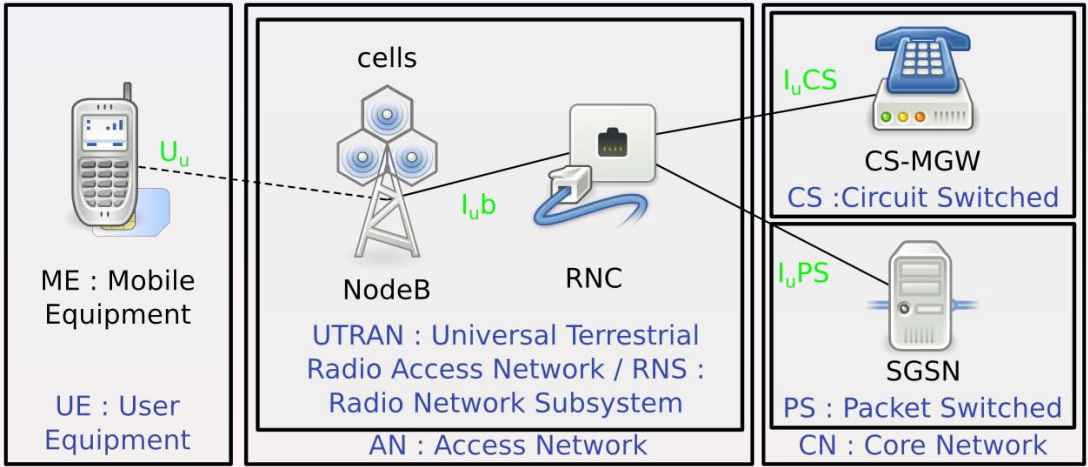
Technische Universität Berlin, SecT
ravii/kredon@sec.t-labs.tu-berlin.de

TROOPERS 2011, 30 March 2011

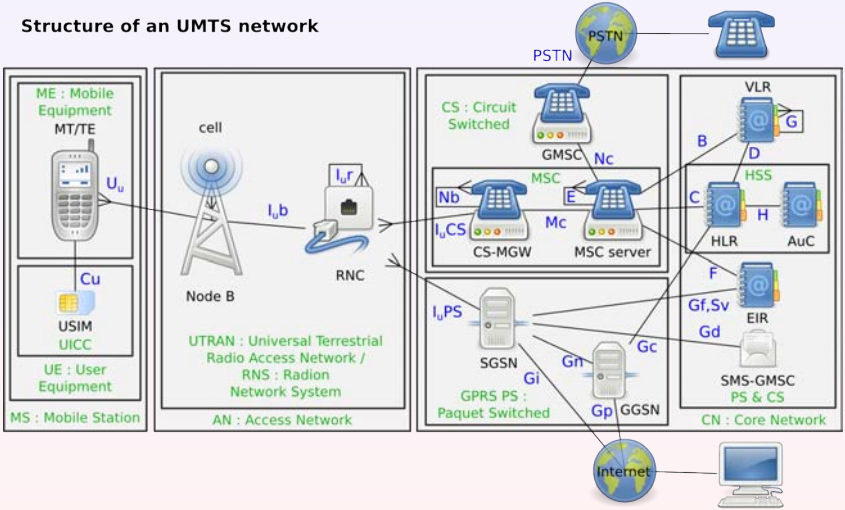
mobile telecommunication history

- 0G - 1950 : not so handy
- 1G - 1980 : similar to 2G, but with analog voice (like in PSTN)
- 2G - 1991 : GSM in Europe, CDMA in the USA. Very successful, ... and now broken
- 2.5G : GPRS. Packet Switching capability
- 3G - 2002 : UMTS in Europe, CDMA 2000 in the USA. Usable mobile Internet
- 3.5G : HSDPA, faster download. 3.75G : HSUPA, faster upload. 3.9G : LTE/WiMAX
- 4G : LTE-Advanced, WiMAX 2 : Higher bandwidth, no Circuit Switching

UMTS architecture (simplified)



UMTS architecture (complex)



cells


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

technology

What is a femtocell :

- it's an access point (sometimes called FAP)
- it connects the mobile phone to the 3G/UMTS network
- compatible with every UMTS capable mobile phone
- small cells, with a coverage of less than 20m
- low power device
- easy to install, you only have provide power and Internet access
- technical name : Home Node B (HNB)

user advantages

advantages provided to the users :

- can be installed at home to provide coverage (if not available)
- provides high bandwidth (not shared with the public)
- can provide location based services (kids arrived at home)

but nothing Wifi can not provide for free, except you don't have to configure the phone.

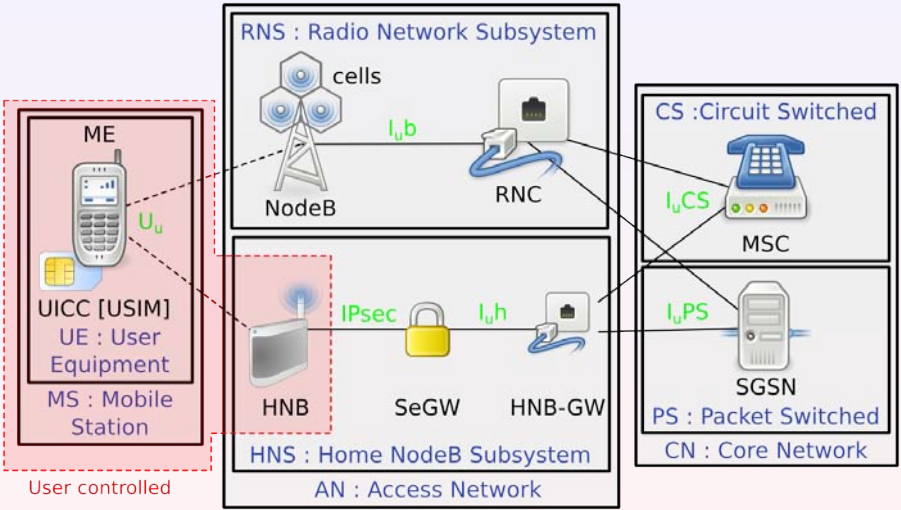
operator advantages

advantages for the operator :

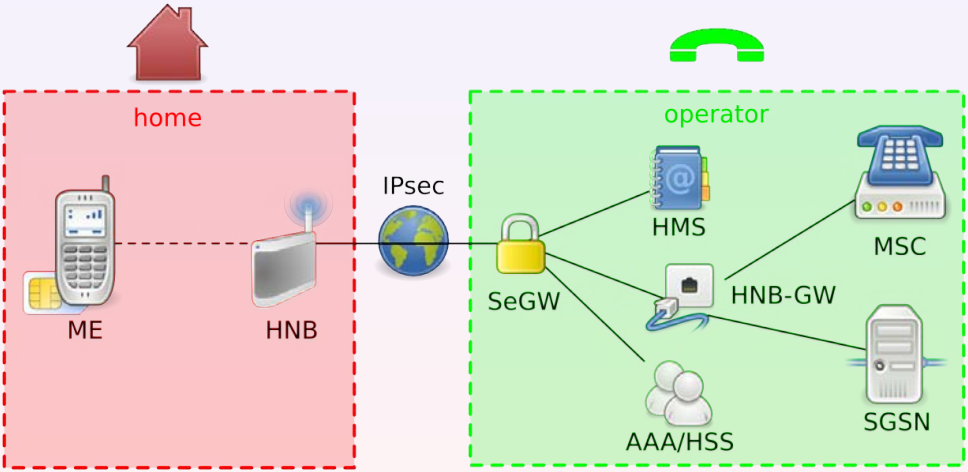
- extended coverage, near to the users
- traffic offloads from their public infrastructure
- cheap hardware, that the user even has to buy
- no installation cost
- no maintenance cost
- new revenue possibilities
- IP connectivity

conclusion : femtocells are a great opportunity for the operators.

HNB in UMTS network



HNB Subsystem



requirements

How to get a femtocell:

- choose a country from the 12 which deploy them
- get an address and IP from this country, because usage in only allowed within the country
- select an operator from the 18 which offer them
- get a mobile phone subscription from this operator, required to get the femtocell service
- gently ask for a femtocell
- get it for free, one time payment, or monthly fee
- enjoy ☺

Location verification

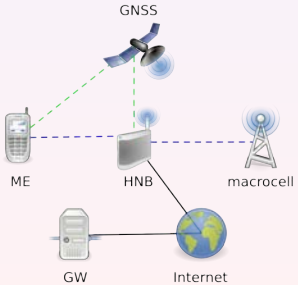
operators have to verify where the femtocell is, for several reasons:

- prevent you to avoid roaming costs in foreign countries
- UMTS uses the 2.1 GHz freq. band, a licensed spectrum band. The operators own the radio licenses for the femtocell only for their country
- location of the users is required for lawful interception

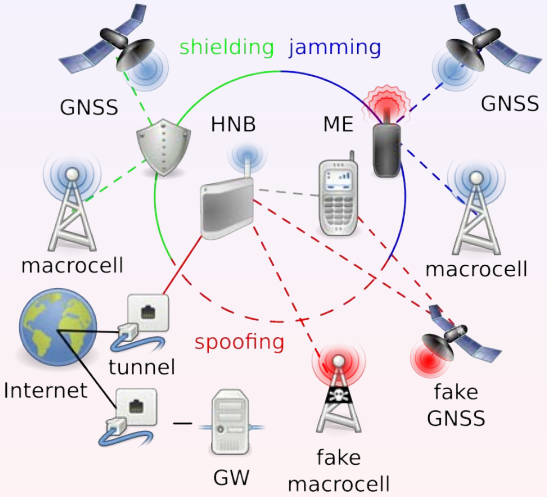
techniques

How to find were the femtocell is located:

- IP : geoIP, even knowing the ISP is enough
- GNSS : GPS
- macrocell : cells bacon county, network, and location information (MCC, MNC, LAC)

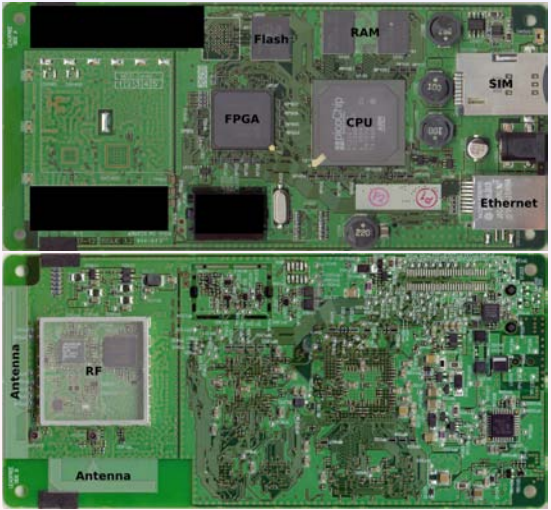


attacks


shielding
jamming
GNSS
HNB
ME
GNSS
macrocell
macrocell
spoofing
tunnel
Internet
fake
GNSS
GW
fake
macrocell


Happy Home
Thursday
25 Mar 2010
Keypad
Phonebook
Menu
SAMSUNG

under the hood



network testing

first approach :

- sniffing
  only DHCP,and NTP. Then everything goes over IPsec
- probing ports (nmap)
  only port 80 is open
  linux has been detected, but the source code is not public
- web interface available
  protected access, no documentation, even the customer service was unaware
- serial port found on PCB
  login prompt not enabled

First impression : the device is secure. ☹
But the first impression is not the last impression. ☺

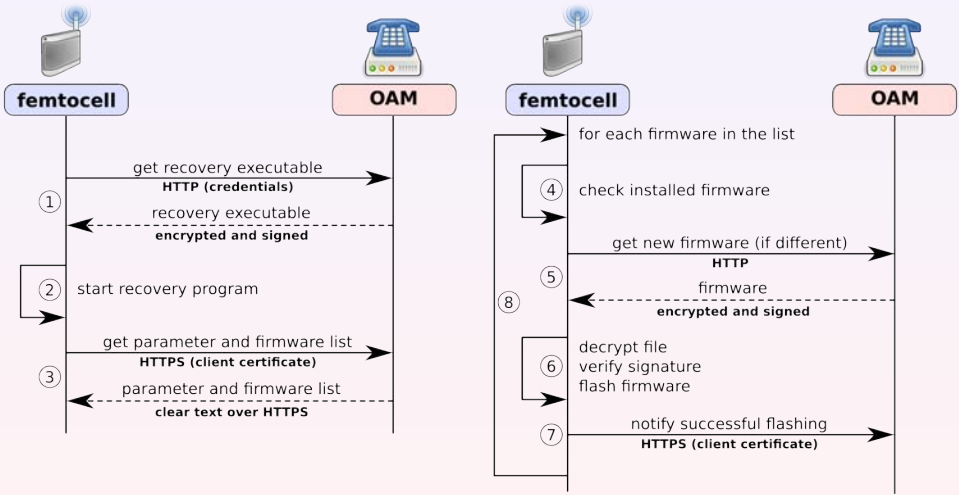
recovery mode and purpose

critical point : the recovery procedure
remember :

- keep femtocells cheap
- no maintenance cost
- no local support

So if something does not work right, do a factory reset. For that, the recovery procedure has been created.

process overview

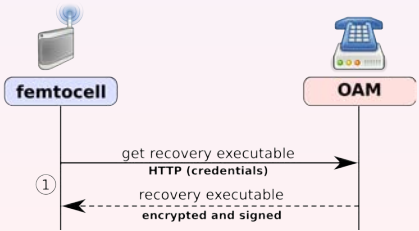


flaws and exploits ①

flaws :

- recovery image is downloaded over HTTP
- credentials are in plain text
- normally the image is encrypted, but modified URL will return unencrypted version
- image is still signed. it can't be altered, but viewed

exploit : the recovery process can be analyzed

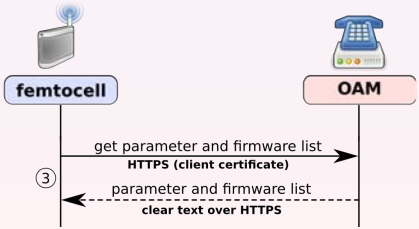


flaws and exploits ③

flaws :

- integrity of parameter and image list relies only on HTTPS
- file is not signed
- HTTPS uses authentication, but not mutual

exploit : you can provide your own lists

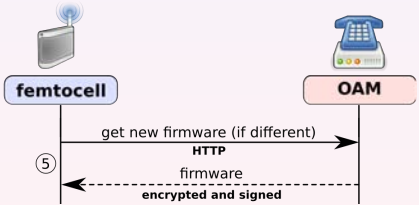


flaws and exploits ⑤

flaws :

- real name of the files are in the image list
- encryption keys are in the image list

exploit : you can get an decrypt the images



reconfigure

the parameter list contains some interesting values :

- the login prompt for the serial port can be enabled
- the root password is the same then in the recovery image, stored in md5
- the public key used to verify the signatures is in there
- it's possible to clone femtocells (except the SIM)

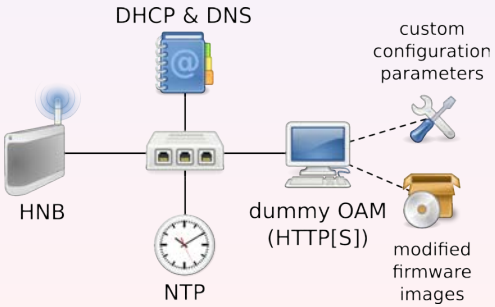
```
[General]
pcbid=P04S...
imei=357539...
mac=00:1B:67:...
hwflag=2
serial=P04S...

[BootSigning]
pubkey=EE:17:C5:F2:...
```

reflash

you can provide your own image list :

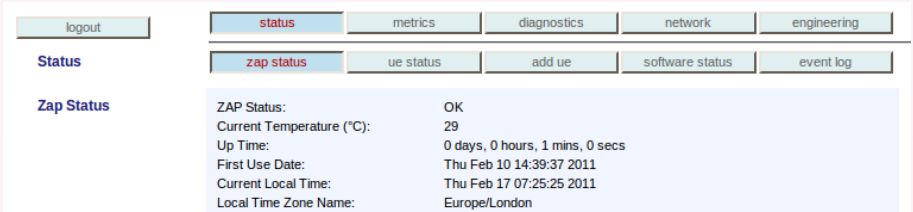
- the URLs, encryption keys and signatures are in there
- your can provide your own images
- your can use the previously obtained images, and modify them
- now it's possible to install anything



web interface

found while analyzing the images :

- credentials for web interface are in a local database
- the previously discovered interface is provided by the operator. it only contains the status and subscriber list
- a hidden web interface is provided by the vendor. it contains the complete configuration
- the hidden web pages can be accessed without authentication



HNS services

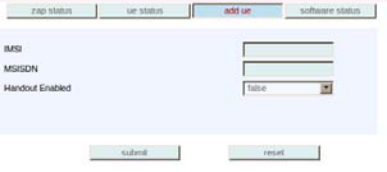
use the femtocell to explore behind the security gateway :

- Performance Measurement server : stores the femtocell activity
- OAM server : used to update the femtocell
- HMS server : used to configure and provision the femtocell

Reconfiguration

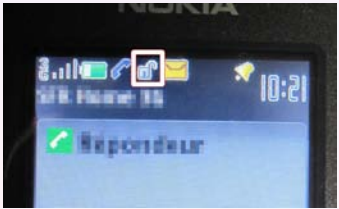
you can change the femtocell settings :

- disable macrocell sniffing
- add phone to the subscriber list
- provide own security gateway
- change cell configuration



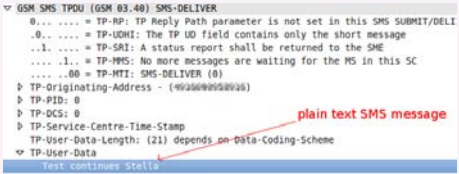
significance of the attacks

- privacy threats - recording phone calls, SMS..



significance of the attacks

- eavesdropping
- accessing infrastructural elements



threat list

Attacks, effects, and impact are documented in the 3GPP femtocell standard (TR 33.820)

group	threat	impact
Compromise of HNB Credentials	Compromise of HNB authentication token by local physical intrusion	Harmful
Physical attacks on a HNB	Booting HNB with fraudulent software ("re-flashing")	up to disastrous
Configuration attacks on a HNB	Fraudulent software update / configuration changes	Extremely harmful
	Mis-configuration of HNB	Irritating to harmful
	Mis-configuration of access control list (ACL) or compromise of the access control list	Irritating to harmful
Protocol attacks on a HNB	Man-in-the-middle attacks on HNB first network access	Very Harmful
	Compromise of an HNB by exploiting weaknesses of active network services	Extremely harmful
	Manipulation of external time source	Harmful
	Threat of HNB network access	Harmful
Attacks on the core network, including HNB location-based attacks	Changing of the HNB location without reporting	Harmful
	Misconfiguration of the firewall in the modem/router	Annoying
	HNB announcing incorrect location to the network	Harmful
User Data and identity privacy attacks	User's network ID revealed to Home (e)NodeB owner	Breaking users privacy

It also includes recommendations and countermeasures

conclusion and opening

- femtocells is an effective technology in terms of offloading the traffic and of new business cases
- but... the operators need to do their homework
- follow the specifications, secure the device and network access
- some serious threats (ongoing work):
  - re-use the telecom infrastructure elements
  - build a MitM, to be used during communications

Thanks

Thanks to :

- Nico Golde, TU Berlin
- Collin Mulliner, TU Berlin
- Prof. Jean-Pierre Seifert, TU Berlin
- Benjamin Michéle, TU Berlin

questions

Danke

Questions ?