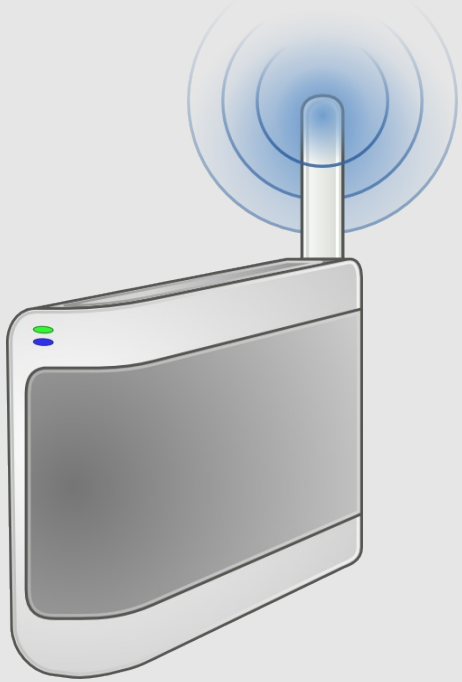
Hacking Femtocells

a femtostep to the holy grail



Ravishankar Borgaonkar

ravii@sec.t-labs.tu-berlin.de

Kevin Redon

kredon@sec.t-labs.tu-berlin.de

Security in Telecommunication

Technical University of Berlin

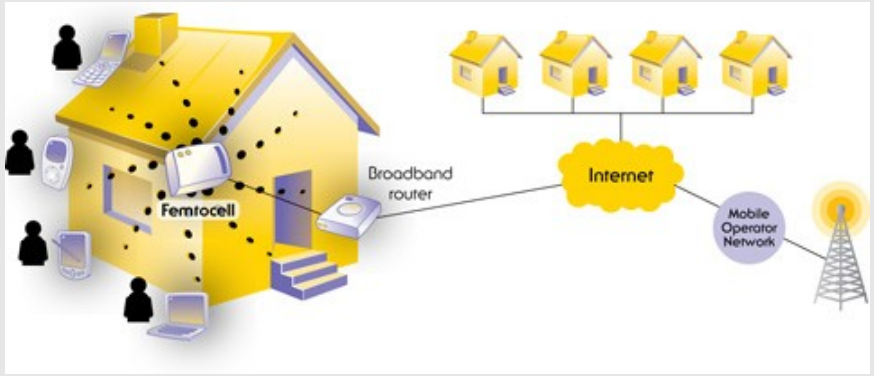
Introduction

- Ravishankar Borgaonkar
  - PhD student at TU Berlin
  - Area: M2M Security, Mobile Networking Security
- Kevin Redon
  - Master Student at TU Berlin
  - Area: Network Security
- Special thanks to:
  - Collin Mulliner, TU Berlin
  - Prof. Jean-Pierre Seifert, TU Berlin
  - Benjamin Michéle, TU Berlin
  - Monty Python

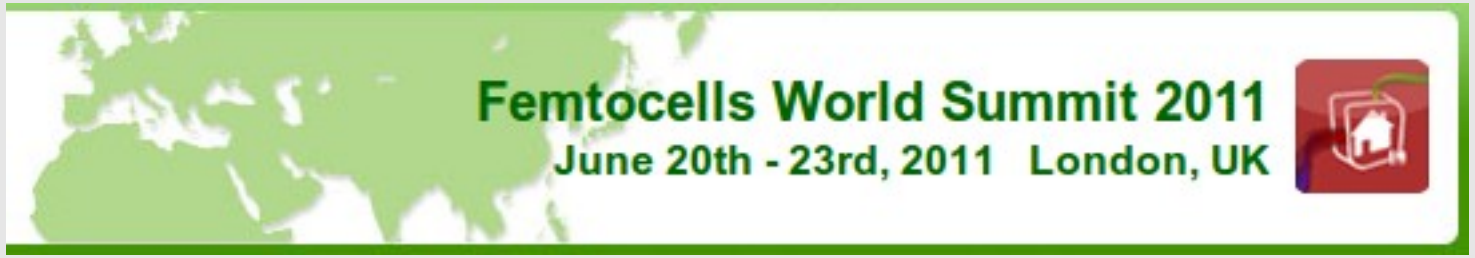
Contents

Femtocell Technology

- low power wireless device
- supports any 3G mobile device
- provide 3G coverage for places where macrocells can not
- offloads traffic from the macrocell layer, and improve macrocell capacity
- IP connection to the core network
- higher data rates with power saving option to the mobile devices



Femtocell Future



Someday, all Basestations will be Made Like This
Nigel Toon - CEO, picoChip

Femtocells - Playing A Pivotal Role In 4G Networks
Timo Hyppola - Head of Indoor Radio, Nokia Siemens Networks

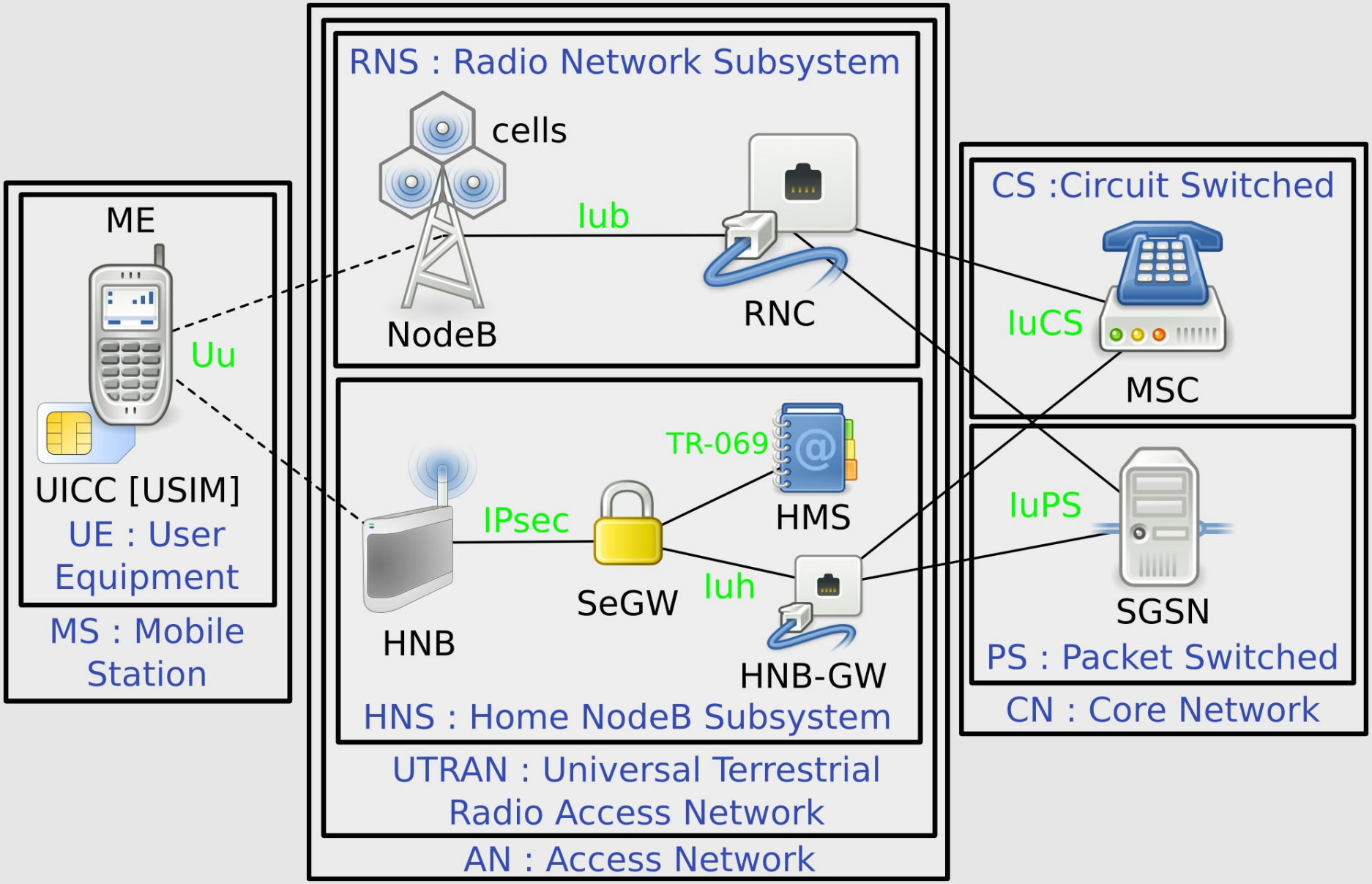
How and where ?

- currently in the 9 countries (soon in other places)
- you can buy easily
- you need to provide right address to provision since they lock the device to a particular location
- if you change the address, it will not work (as they say so)
- costs < 100 euro + normal phone subscription
- **No Roaming** is allowed on the Femtocells

Small base station?

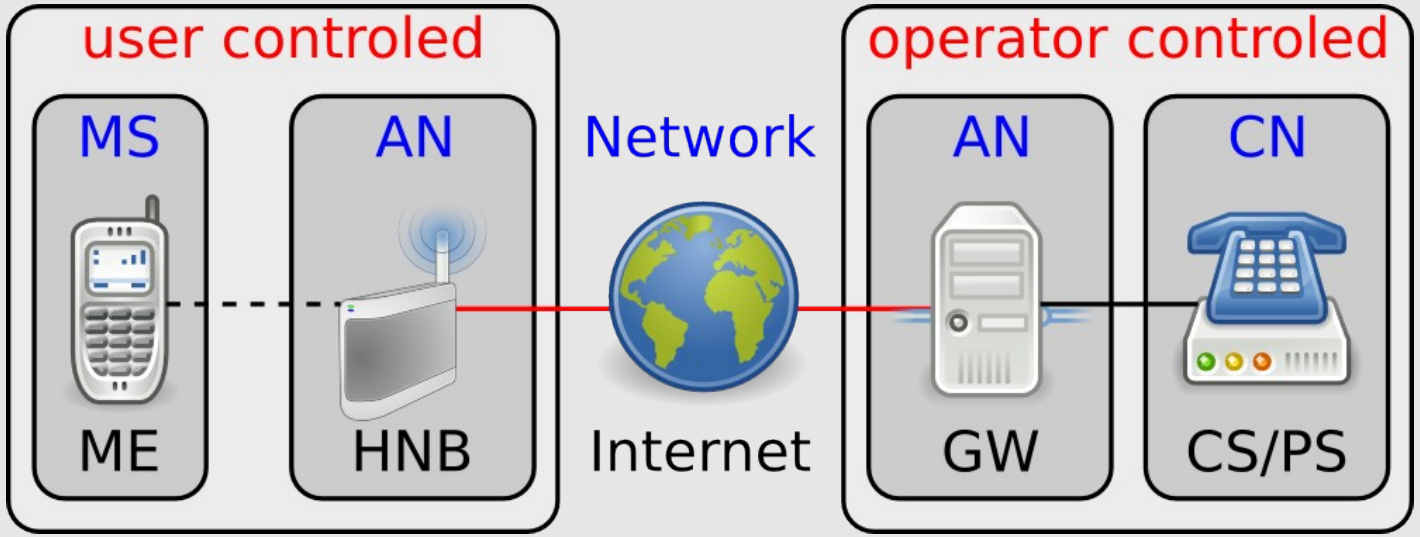
Country	Operator	Vendor
USA	AT & T, Verizon	ip.access, Samsung
Japan	KDDI, NTT Docomo	Airvana, Mitsubishi
Portugal	Optimus	Huawei
France	SFR	Ubiquisys
Singapore	Singtel, Starhub	Huawei
Japan	Softbank	Ubiquisys
Spain	Telefonica	Huawei
UK	Vodafone	Alcatel-Lucent
Greece	Vodafone	Huawei

Difference : Femtocell and NodeB



Femtocell Architecture

- femtocell Device aka HNB (Home NodeB)
- Security Gateway (SeGW)
- Operation, Administration & Management server (OAM)
- User Equipment (UE)

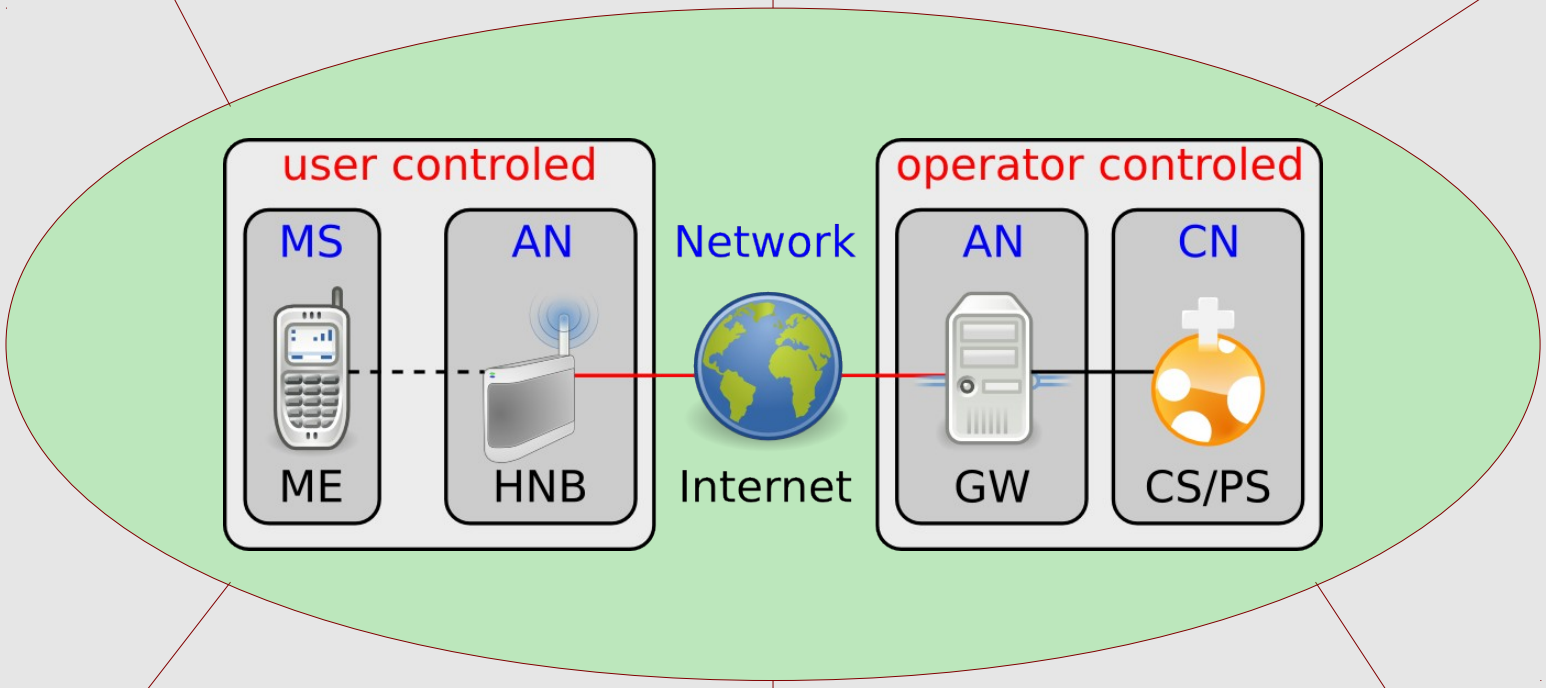


Femtocell Security

Only registered SIMs are allowed

3G AKA procedure

Secure phone calls (over-the-air)



Remote controlled HNB

Location verification

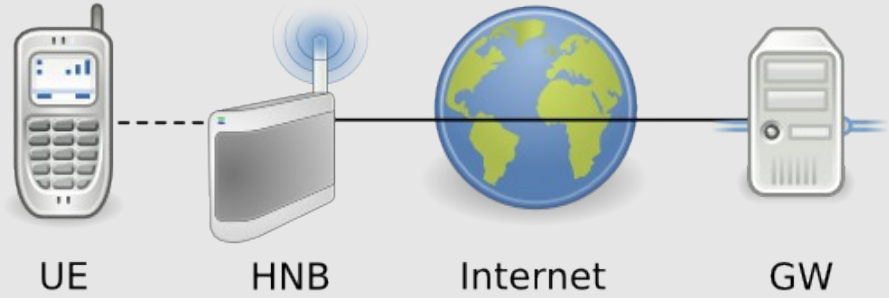
IPsec tunnel over boradband

Femtocell Security Requirements

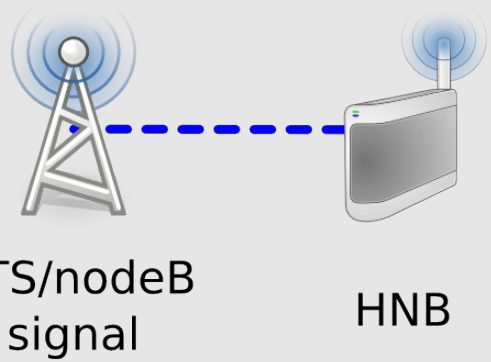
- femtocell should be locked to a specific geographical location to avoid misuse (roaming is good) and to respect radio license
- booting process of the femtocell should be secured by cryptographic means (e.g. no ROOT access)
- device should not reveal any secret information such as IMSI, stored keys etc.(e.g. public keys, IPsec keys)
- …
- Security of H(e)NB, TR 33.820

Location Locking Methods

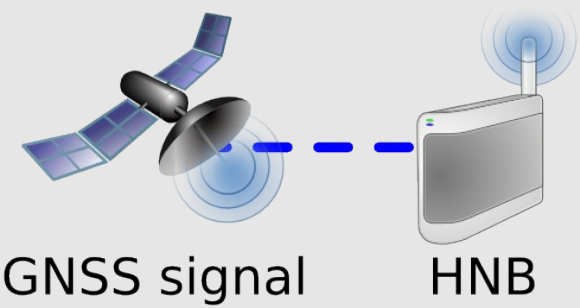
geoIP



macrocells

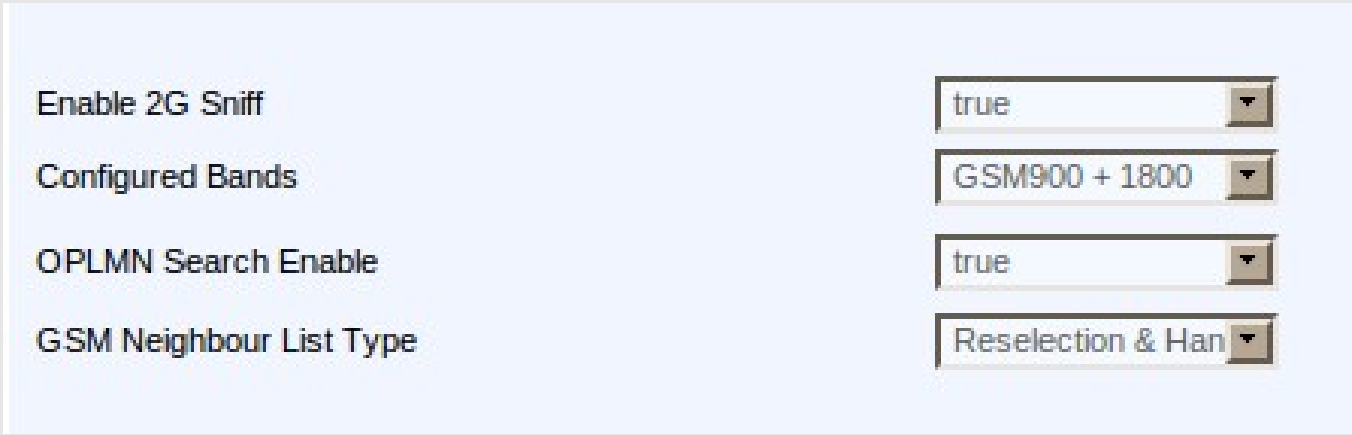


GNSS



UE reports

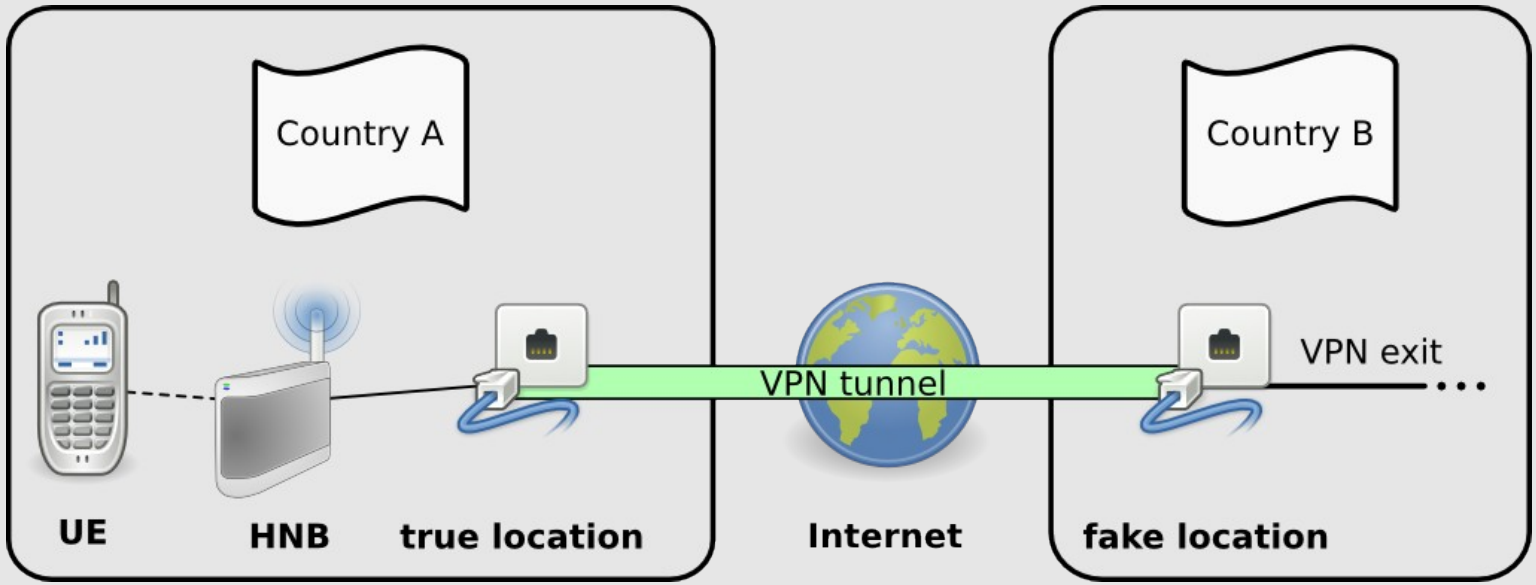
On the Device



Alarm	Activation time
CannotSelectRFProfile:	INACTIVE
SoftwareFault:	INACTIVE
PMReportFailure:	INACTIVE
LocationChanged:	INACTIVE
PoorRFQos:	INACTIVE
PoorBackHaulQoS:	INACTIVE
OverTemperature:	INACTIVE
UpgradeFailure:	INACTIVE
FilesystemFailure:	INACTIVE
HotSpotIndication:	INACTIVE
NoNtpServer:	INACTIVE
InvalidCountry:	INACTIVE
GatewayChanged:	INACTIVE
AllTimingServerConnectivityLost:	INACTIVE
NoTimingSource:	INACTIVE

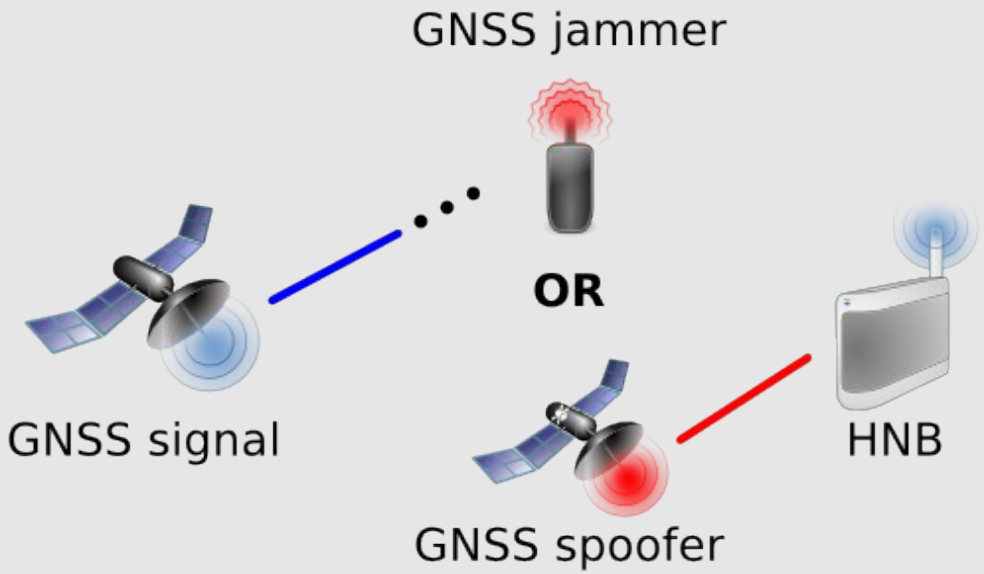
Breaking locks - IP address

- use VPN (Virtual Private Network)
- only need to show that you are at home :-)



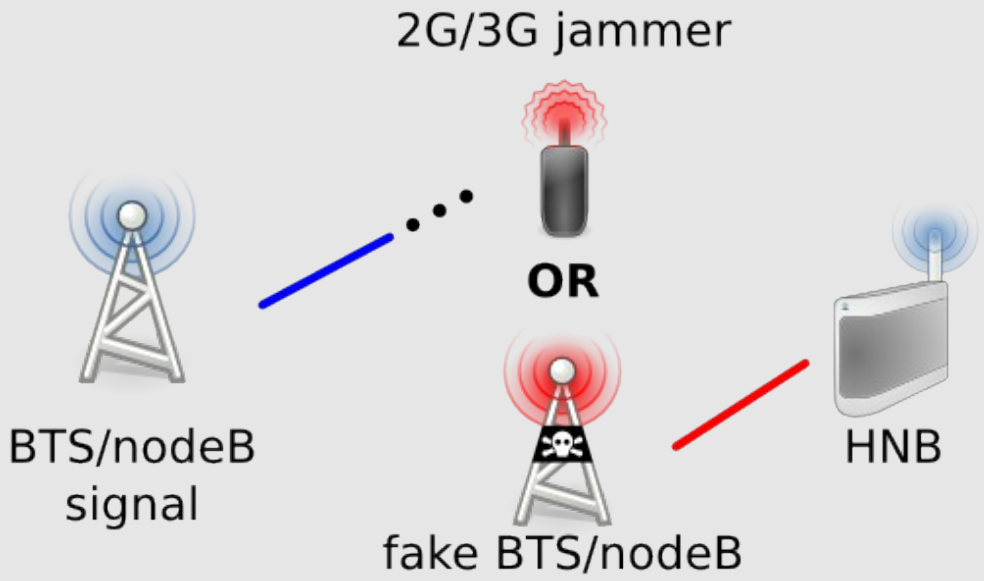
Breaking locks – GNSS (GPS)

- tools you need: GPS jammer or GPS spoofer
- go indoor (low GPS signal)
- not all devices have GPS



Breaking locks - macrocells

- tools you need: GSM jammer, fake BTS, or elevator
- LAC and MCC can be faked using fake BTS
- block the signal (jamming, Faraday cage)



Result

what could go wrong? **lawful interception**


device security analysis

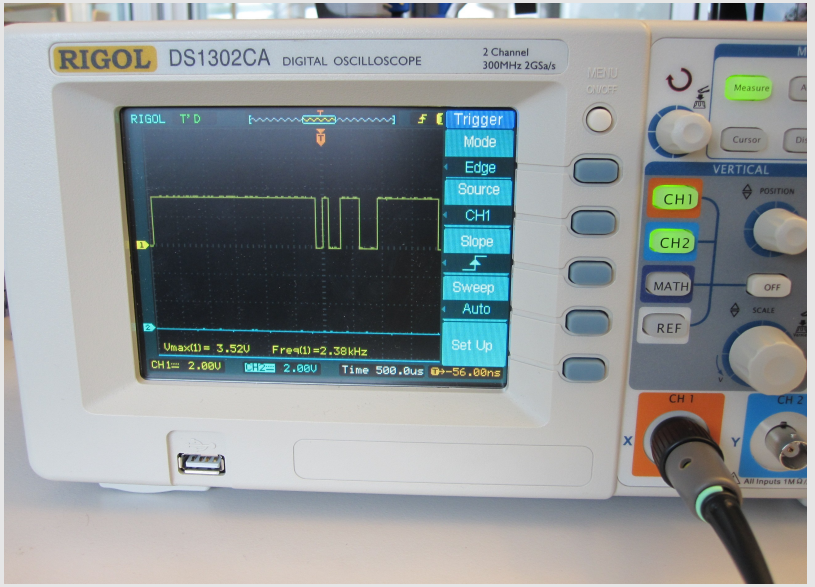
Rooting the device

different approaches to own an access point:

- scan the network
- finding a serial port
- sniffing the communication

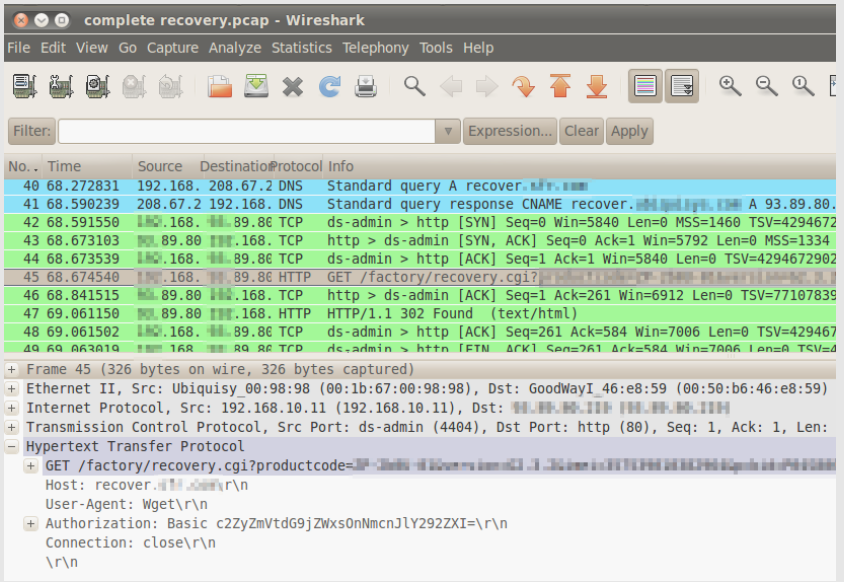
Secured device

- no port open apart http
- serial port found, but no login prompt
- all communication is over IPsec



Recovery procedure

- image download over http
- using hashes in the url
- encrypted and signed
- one small https request
- some https notifications



1. small loader getting a recovery file system
2. recovery image downloads and flashes all other images

Recovery to failure

0. recovery file system in also available unencrypted

   you cannot modify it (signed), but at least analyze (tivo)

1. no mutual authentication over HTTPS

2. given public key is not signed

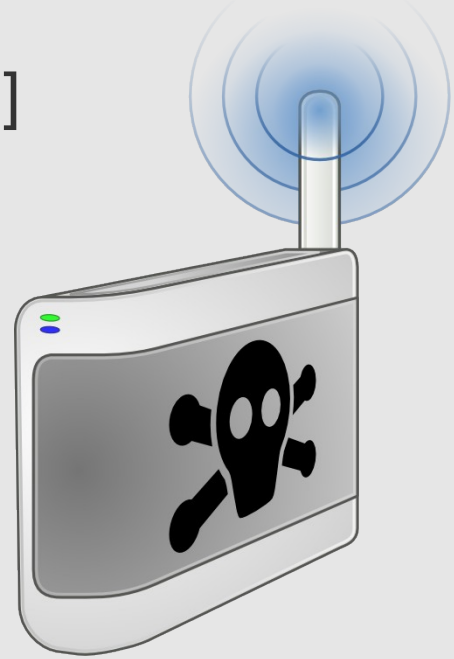
3. all images can now be decrypted and analyzed

Your mine: pwnd

- setup a fake recovery server

  services : DHCP, DNS, NTP, and HTTP[S]

- re-activate login prompt
- flash modified images



- threat 6 of 29 :

  Booting H(e)NB with fraudulent software (“re-flashing”)

  Impact: up to disastrous. Possibility to use any software can mean any violation of the security

Doors to heaven

a small eye drop behind the SeGW

Analysis of the Research

- effective technology in terms of offloading the traffic and of new business cases
- provides higher data rates to the user … **but ....**
- the device security can become a breach
- some serious threats :
  - could open gates to the Telecom infrastructure elements (like HLR)
  - a very cheap IMSI catcher device
  - might used as MiTM device while calling

References

- 3GPP ," Security of Home Node B (HNB) / Home evolved Node B (HeNB) ", TS 33.320, V9.1.0, April 2010. http://www.3gpp.org
- 3GPP Technical Specification Group Service and System Aspect, " Security of H(e)NB", TR 33.820, V8.3.0, December 2009
- 3GPP TR 33.820 Release 8 : 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Security of H(e)NB
- The nanoBTS: small GSM basestations. http://www.ipaccess.com/picocells/nanoBTS picocells.php

Demo

Questions?

Thank U