LTE vs. Darwin

Hendrik Schmidt <hschmidt@ernw.de>
Brian Butterly <bbutterly@ernw.de>

ERNW
providing security.

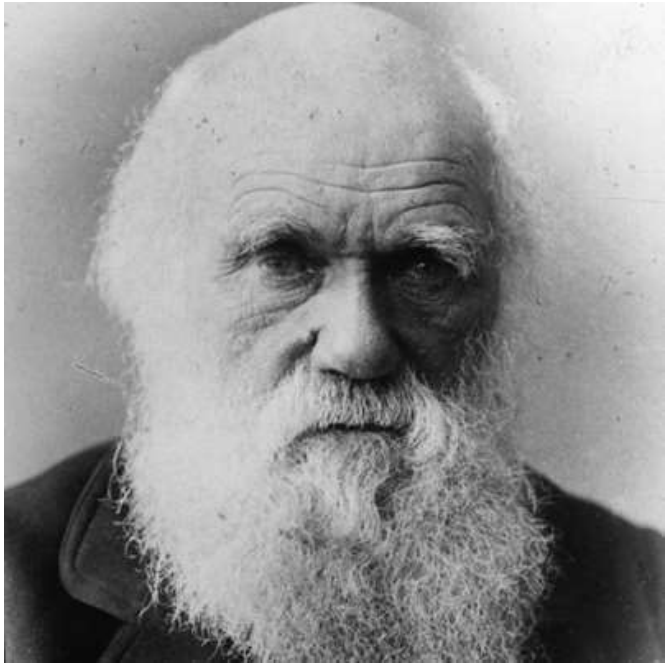
Who we are

- Old-school network geeks,
  working as security researchers for
- Germany based ERNW GmbH
  - Independent
  - Deep technical knowledge
  - Structured (assessment) approach
  - Business reasonable recommendations
  - We understand corporate
- Blog: *www.insinuator.net*
- Conference: *www.troopers.de*
- Telco research project: *www.asmonia.de*

Motivation - Long Term Evolution (LTE)

- 4G wireless technology for mobile communication
- The 4G standard introduces a lot of new technologies providing modern services to the customer.
  - This includes features as *SON*, ...Trust and optional controls

Charles Darwin and the Darwin Award



From: biography.com

- "Taking oneself out of the gene pool by their own (unnecessarily foolish) actions."
- First on Usenet group discussions as early as 1985
- 1993 on a website and collection of books by University of California, Berkeley
- www.darwinawards.com

One Example

"(2003, Australia) Parents often warn that firecrackers can blow your hand off, but as a 26-year-old Australian learned, they can also remove your gonads from the gene pool. An ambulance rushed to an Illawarra park after receiving reports that a man was hemorrhaging from his behind. The mercifully unidentified man had placed a lit firecracker between the cheeks of his buttocks, stumbled, and fell upon it."

http://darwinawards.com/darwin/darwin2003-19.html

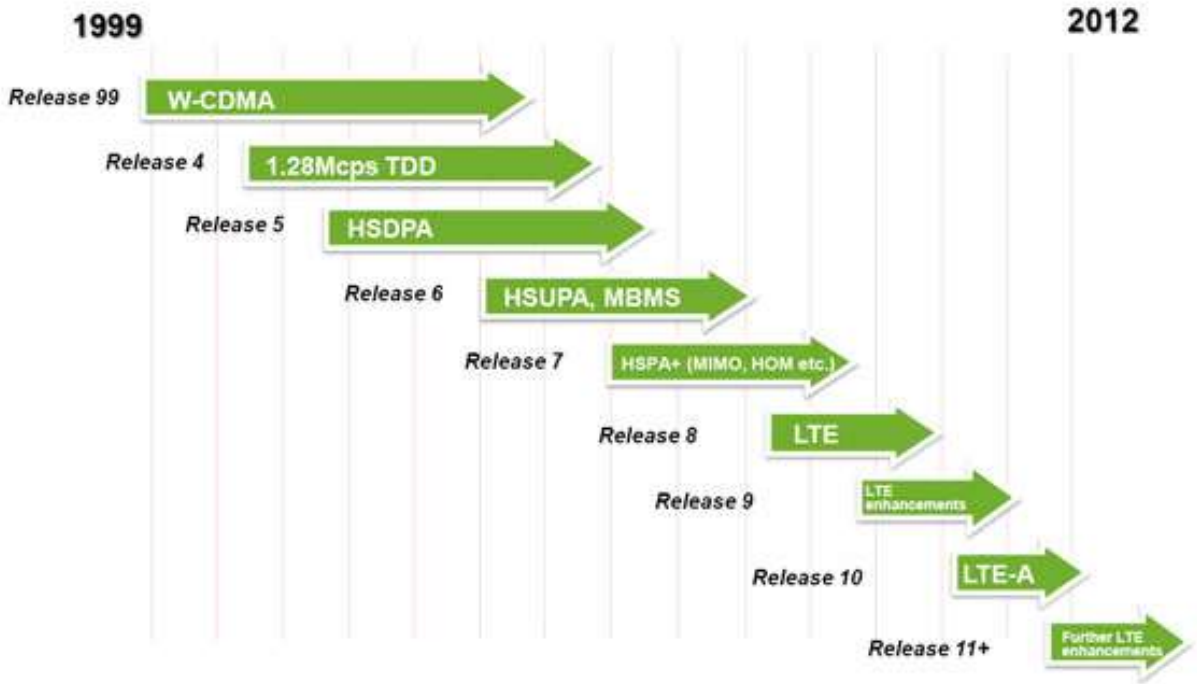
Rly? ☺

From: youtube.com

We‘ll start with some basics…

Standards - Overview

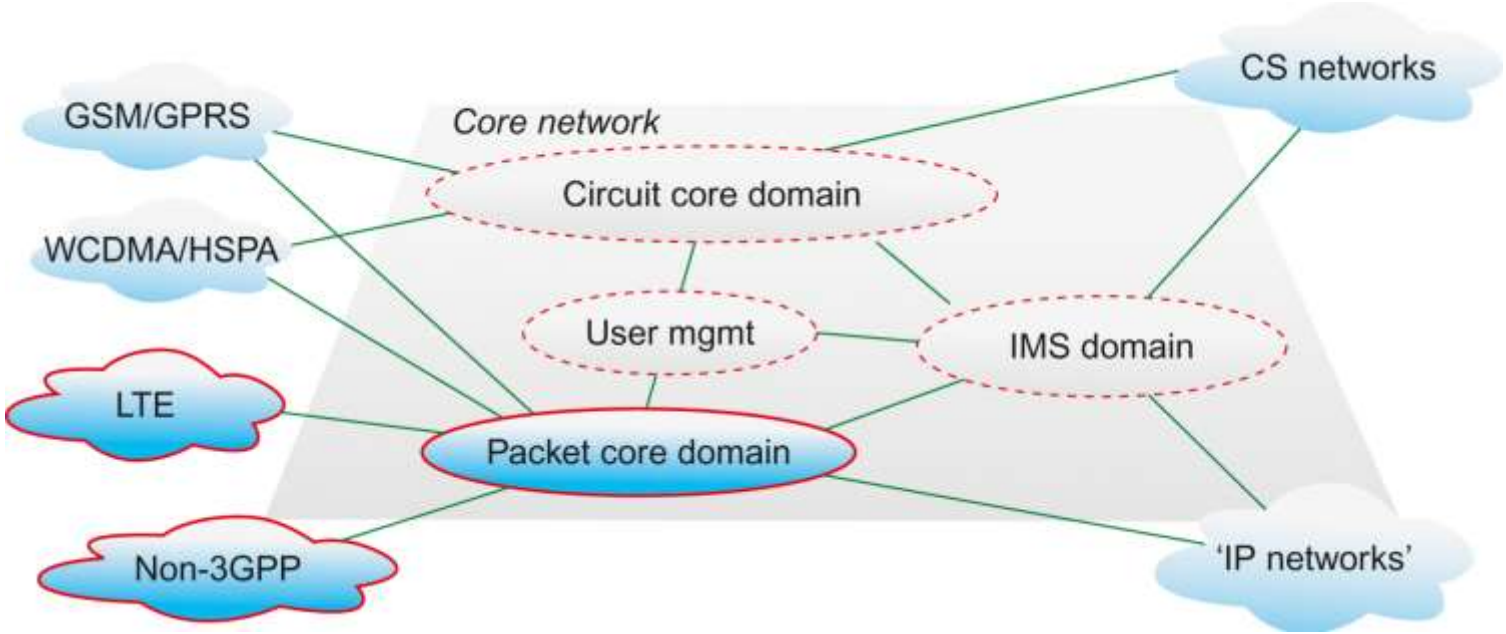
- International Telecommunication Union (ITU)
  - http://www.itu.int/
- 3rd Generation Partnership Project (3GPP)
  - www.3gpp.org
- Europäisches Institut für Telekommunikationsnormen (ETSI)



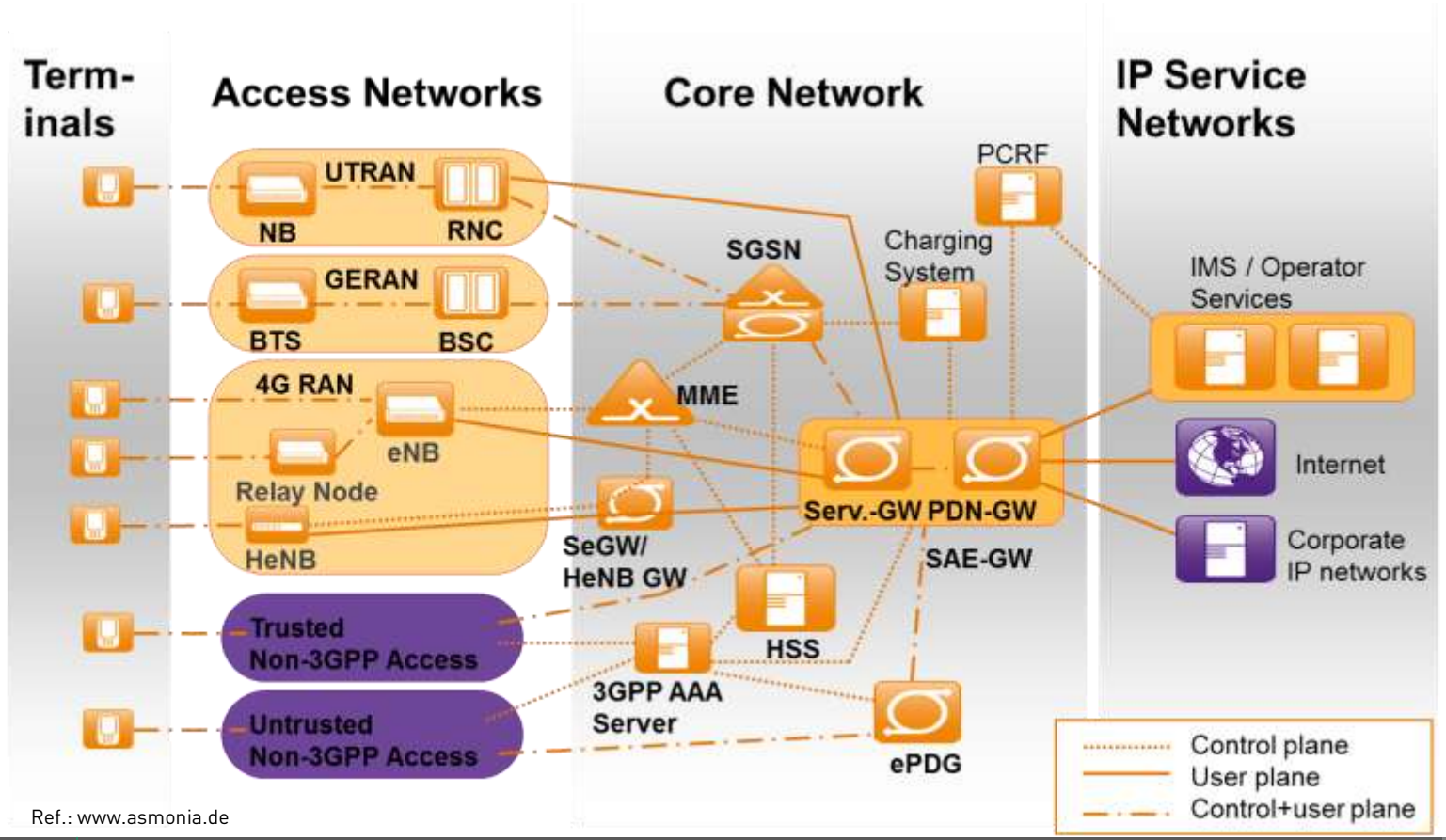
3GPP Milestones...

Ref.e: www.3gpp.org

(Evolved) Packet System - Architecture



Ref.: 3gpp.org



Ref.: www.asmonia.de

LTE in the Field

What we see

eNodeB

- The actual air interface.
- Come in different shapes and sizes.
  - Rack, “Small-Boxes“, Portable
- Different types for different size cells.
  - Macro (>100m), Micro (100m), Pico (20-50m), HeNB (10-20m)
  - (WiFi/WiMax)
- Termination Point for Encryption
  - RF channel encryption
  - Backend channel encryption

This results in..... Het-Nets

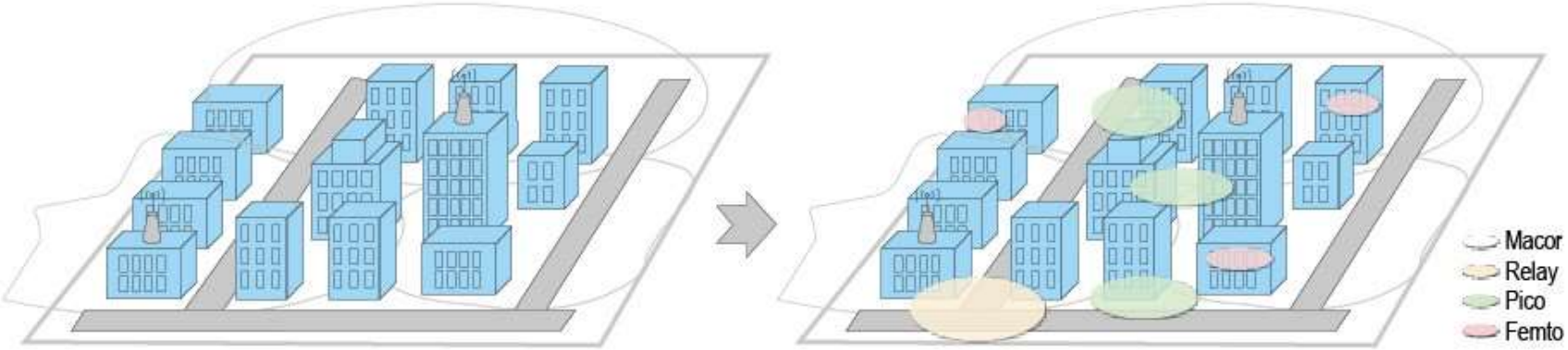


Figure 2. Evolution from homogeneous to heterogeneous networks.

Source: http://wwwen.zte.com.cn/endata/magazine/ztetechnologies/2012/no1/articles/201202/t20120206_283266.html

An actual Runcom eNodeB

Source: runcom.com

eNodeB

- Ports for various amounts of “directional“ antennas.
  - Single eNodeB, multiple Cells.
  - Cellmast “between“ two cells
- Placed “close to antenna“
  - On the mast or down below.
- Connected via LAN
  - “Self Configuring“
    - More on that later on

And now...? => Starting with the phone!

Part 1: UE Awareness

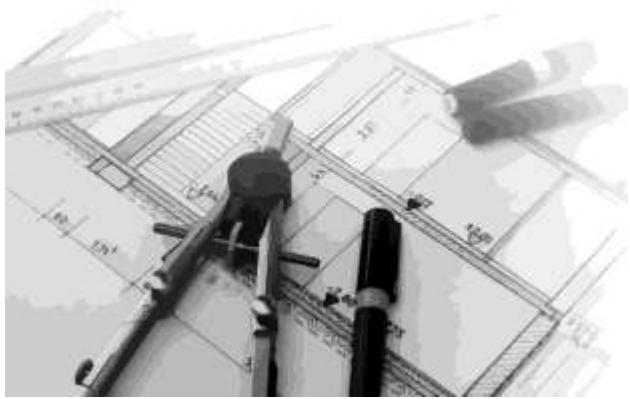
Phone means...

- Usually, it has to do phone calls ☺
  - or Internet; or some other stuff as we will see...
  - ...or everything merged together
- We've got
  - $Tablets/Slates
  - $USB-Sticks/-Modems
  - $4G Cards
  - $Mobile Hotspots
  - Relay Nodes ;-)

Our Scope

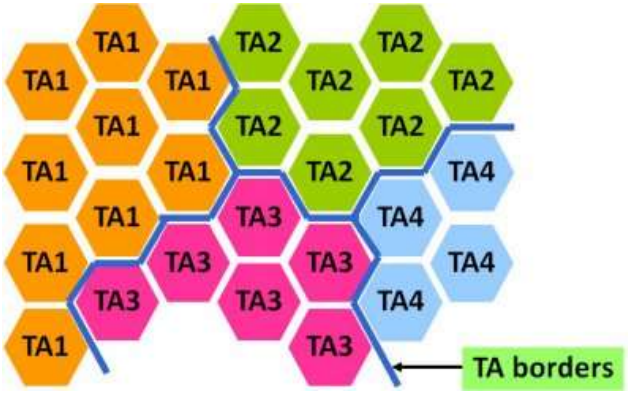
- When talking phone security you usually see the OS and its applications.
  - We'll check out some background functionality

UE: Look, Feel, Ask



- (Physical) Cell ID
- Tracking Area Code
- “Signal Strength“
- Position

PCI & TAC



- Physical Cell-ID
  - As known from "old" networks
  - Regionally unique identifier
  - 504 different IDs
  - Configured automatically
- Tracking Area Code
  - Contains multiple cells.
  - Paging area
  - UE's current "location"

Source: http://www.3gpp.org/technologies/keywords-acronyms/96-nas

Signal Strength & Location

Enhanced Serving Mobile Location Center (E-SMLC)

- Backend part for positioning
- Accepts requests from MME and organizes the actual process of positioning

- Signal Strength
  - Measured by device
  - Output in different formats
- Location
  - Positioning request
    - Use of OTDA (Observed Time Difference of Arrival)
    - Use differences in arrival times of packets from certain eNodeBs
  - GPS…GALILEO…GLONASS

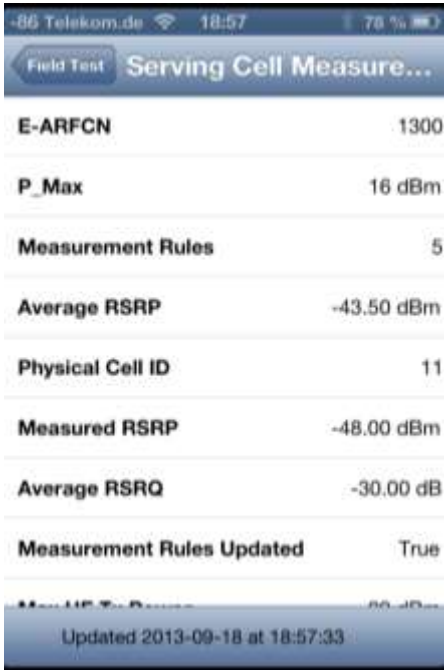
Accessing Data

- Rather easy
  - Use of magic numbers
  - Apps
  - AT Commands

Hackers do „Information Gathering“

3001#12345#

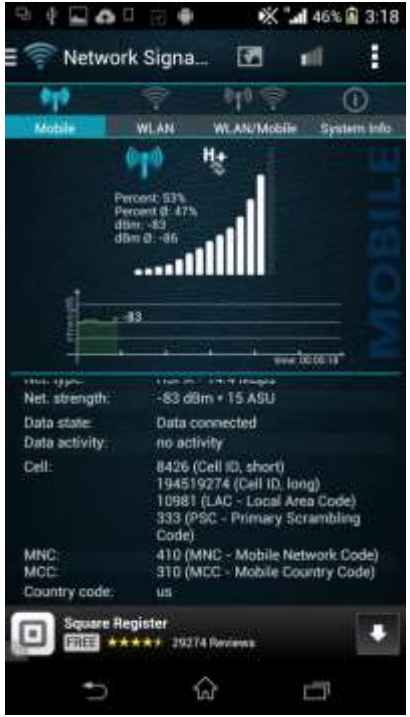
- The magic number for IPhones



And on Android...

Network Signal Info

https://play.google.com/store/apps/details?id=de.android.telnet&hl=de



But why…?

From: youtube.com

- Knowledge! Understanding LTE!
- Collect and Log Data
- Answer a few questions
  - How large are Cells?
  - How large are Tracking Areas?

“Simple“ Approach

- Writing an App on Android
- Use of onboard functionality & dump data into xml file

```
tm =
(TelephonyManager)this.getSystemService(Context
.TELEPHONY_SERVICE);
CellIdentityLte cell =
((CellInfoLte)a).getCellIdentity();
pci=cell.getPci());
tac=cell.getTac());
mnc=cell.getMnc());//Network Code
mcc=cell.getMcc());//Country Code
```

Or do it manually

```
*EMRDY: 1
AT+COPS?
+COPS: 0,0,"T-Mobile",0

OK
AT+cops=?
+COPS: (1,"T-Mobile","T-Mobile","310260",0),(1,"AT&T","AT&T","310410",2),(1,"AT&T","AT&T","310410",0),(1,"T-Mobile","T-Mobile","310260",2)

OK
```

3rd Party Awareness

Am I being watchted?

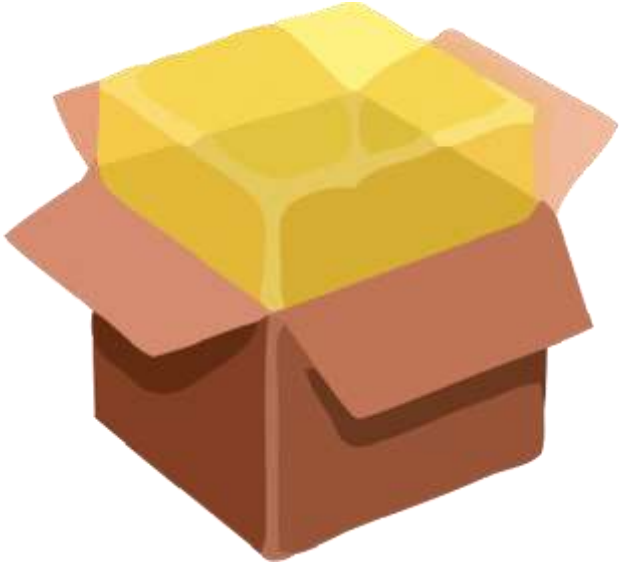
Can you see me??

- LTE is an IP Network
  - Scanning can be possible
- Exemplary Data
  - Attach Process
  - Paging Process

The Attach Procedure

Initial Bearer Setup

Involved components



- SIM Card
- UE
- eNB
- MME – Mobility Management Entity
- SGW – Serving Gateway
- PGW - PDN (Packet Data Network) Gateway
- HSS – Home Subscriber Server

ERNW
providing security.

#1

UE powers on

Sends RRC Connection Request to eNB.
(including S-TMSI/Random)

IMSI transfered to eNB in Connection Completed Message

eNB contacts MME and passes on ID

Communication relayed from eNB to MME in NAS Messages is >>always<< encrypted ☺

Always Encrypted?

- Yes!
- You may choose from three ciphering algorithms
- EEA2 - AES
- EEA1 – SNOW 3g
- EEA0 - Null ciphering algorithm

#2

MME fetches all neccessary keys and subscriber data from HSS

Authentication request, containing AUTN, is sent to UE and passed on to SIM

Authentication process is started and encrypted channel between UE and eNB established

#3

- Final steps of attach procedure are processed
  - Establishment of IP connection etc.

- ...But, the connection is encrypted and we as a third party can't see it anymore....

Paging

What is Paging

- " Wake up call"
  - UE is usually in a connected standby mode to save energy
- Paging wakes the UE and informs it of incoming messages and calls
- UE checks for Paging Messages periodically on certain channel

How to reach a certain UE ?

- Paging frames are sent out in a certain tracking area periodically
- Certain " flags" can be set in these frames
  - Actually in certain sub-frames
- UE knows which " flag" to react to

Where to look?

SFN mod T= (T div N) * (UE_id mod N)

Find the Frame

eNB and UE are synchronized during attachment process!!

- SFN mod T=
  (T div N) * (UE_id mod N)

- SFN: System Frame Number
- T: DRX cycle of the UE
  - UEs wake up cycle (32, 64, 128, 256)
- nB: Number of paging occasions per DRX cycle
  - 4T, 2T, T, T/2, T/4, T/8, T/16, T/32
- N: min(T,nB)
- UE_id: IMSI mod 1024

Find the Occasion

- i_s = floor(UE_ID/N) mod Ns
- Ns: max(1,nB/T)
- Paging Occasion from lookup table

Ns	PO i_s=0	PO i_s=1	PO i_s=1	PO i_s=1
1	9	N/a	N/A	N/A
2	4	9	N/A	N/A
3	0	4	5	9

And now?

We need:

SFN mod T=
(T div N) * (UE_id mod N)

- Closer look at (UE_id mod N)
  - N <= 256
  - So (...) can be 255 max
- Closer look at (T div N)
  - T <= 256
  - N >= T/32 → N >= 8
  - So (...) can be 32 max
- Whole term can be max 8160

So....

- We've got 8160 possible paging frames
- And 4 possible paging locations

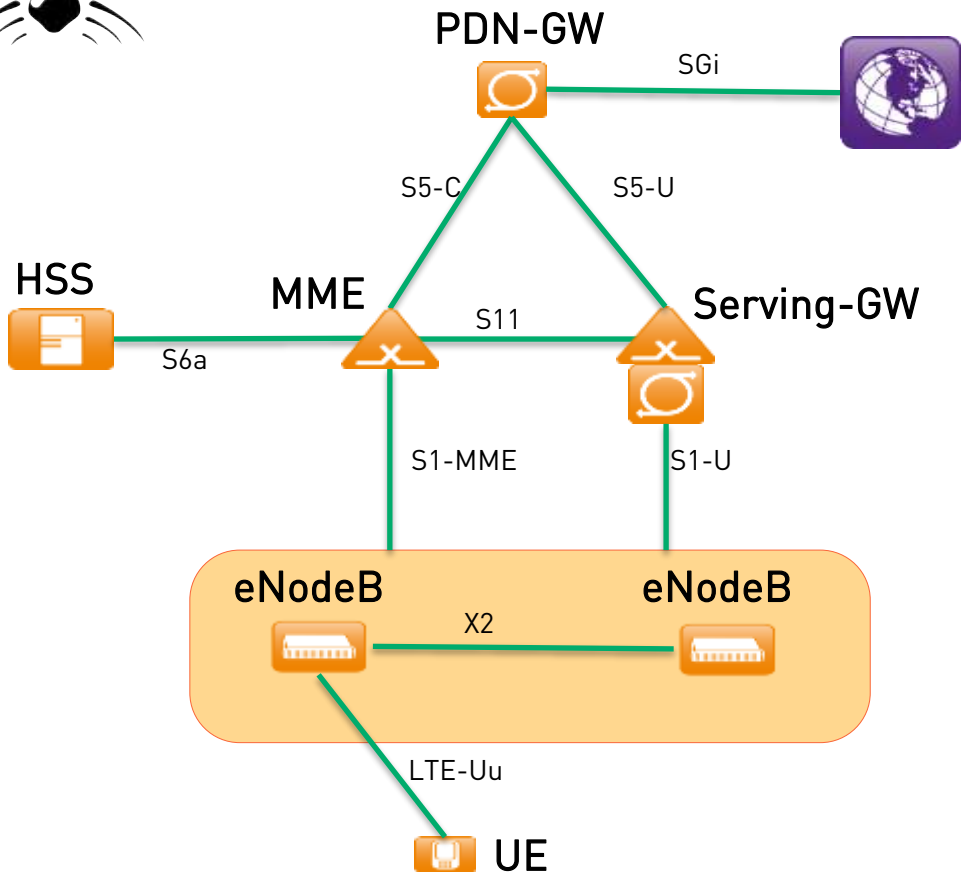
- So we can page up to 32640 different devices
- Or...well...page a few different ones at the same time

Impact?

- You might loose some extra battery power
- Rather hard to actually track a mobile phone, due to different constansts on different eNBs

The other side...

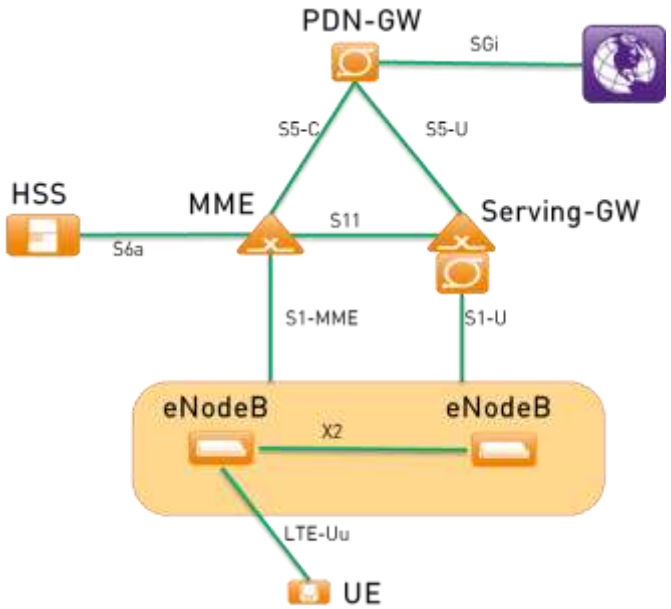
Backend Structure



Remember...?

The 4G LTE Basic

Control Structure



- GTP Interfaces
  - ShmooCon 2011: Attacking 3G and 4G mobile telecommunications networks.
- S1 Interface
  - S1-MME: control interface between eNB and MME
  - S1-U: user plane
  - IPSec Encryption

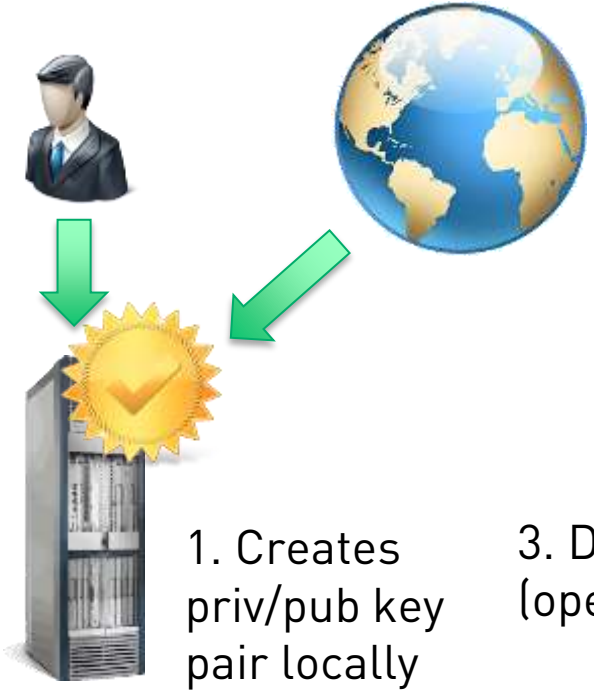
Some quotes from 3GPP TS 33.403

- "Setting up and configuring eNBs **shall be authenticated and authorized** so that attackers shall not be able to modify the eNB settings and software configurations via local or remote access."

Access to the eNodeB?

Source: worldlte.blogspot.com

Certificates on Devices (e.g. eNB)



2. Signs pub key with factory cert

4. Stores it in its CA pool as a high level certificate

5. Has a signing certificate of operator.

1. Creates priv/pub key pair locally

3. Delivers factory cert to customer (operator) “in a secure way“

Specs about IPSec

- But this doesn't matter, 4G security is mostly based on Security-Gateways
- 3GPP TS 33.401
  - "In order to protect the S1 and X2 control plane [...], it is *required to* implement IPsec [...]. For both S1-MME and X2-C, IKEv2 certificates based authentication [...] *shall be* implemented."
  - "In order to protect the S1 and X2 user [...], it is *required to* implement IPsec [...] with confidentiality, integrity and replay protection."
  - "... transport mode IPsec is *optional* for implementation"

Specs about IPSec…

"NOTE 1: In case control plane interfaces are trusted (e.g. physically protected), there is no need to use protection […]."

"NOTE 2: In case S1 and X2 user plane interfaces are trusted (e.g. physically protected), the use of IPsec/IKEv2 based protection is not needed."

You remember...?

Source: worldlte.blogspot.com

Some words on security…

- In reality you will find…
  - Clients with process controls, DHCP, certificates, auto-connection/configuration
  - Servers with DHCP, CMDB, CA, Gateway, QoS
- And you know how this works, or?
  - Management Interfaces?
  - Complexity?
  - Common (IP) network problems/vulns?

Security on $telco_equipment?

- Ever scanned your providers IP address range?

```
:~/tools/nmap$ ./nmap -sP .

Starting Nmap 6.40 ( http://nmap.org ) at 20
Note: Host seems down. If it is really up, b
Nmap done: 1 IP address (0 hosts up) scanned
```

```
hschmidt@hslpt:~$ telnet
Trying .
Connected to .
Escape character is '^]'.
--------------------------------
-----Welcome to ATP Cli------
--------------------------------

Login:
```

```
hschmidt@ :~/ERNW/temp$ nmap -sP .

Starting Nmap 6.41SVN ( http://nmap.org ) at 2014-01-07 15:05 CET
Nmap scan report for .100.70)
Host is up (0.032s latency).
Nmap done: 1 IP address (1 host up) scanned in 2.57 seconds
```

Access Point Names (APN)

- Access List often depends on the chosen APN.

- APNs are well-known, or?
- Ever heard of APNBF?
  - www.c0decafe.de

3GPP Security Assurance Methodology (SECAM)

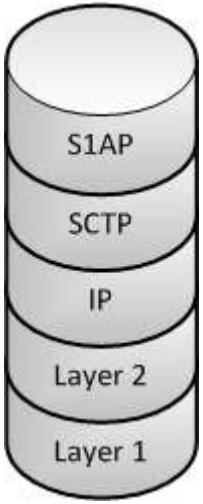
- Defined in 3GPP TR 33.805 (year 2013)
  - "Each 3GPP network product class [...] can have vulnerabilities which, if exploited, can damage the MNO and/or end-users."

SECAM evaluation will cover the following four tasks:

- Vendor network product development and network product lifecycle management process assurance compliance (assessing if the method used to develop the products is compliant with the Security Assurance Process)
- Security Compliance Testing (assessing if requested security requirements are correctly implemented in a network product)
- Basic Vulnerability Testing (running of a set of FOSS/COTS tools on external interfaces of the Network product)
- Enhanced Vulnerability Analysis (holistic approach to analyse risk and impact of Vulnerabilities found in the Network Product))

Back to S1 Interface

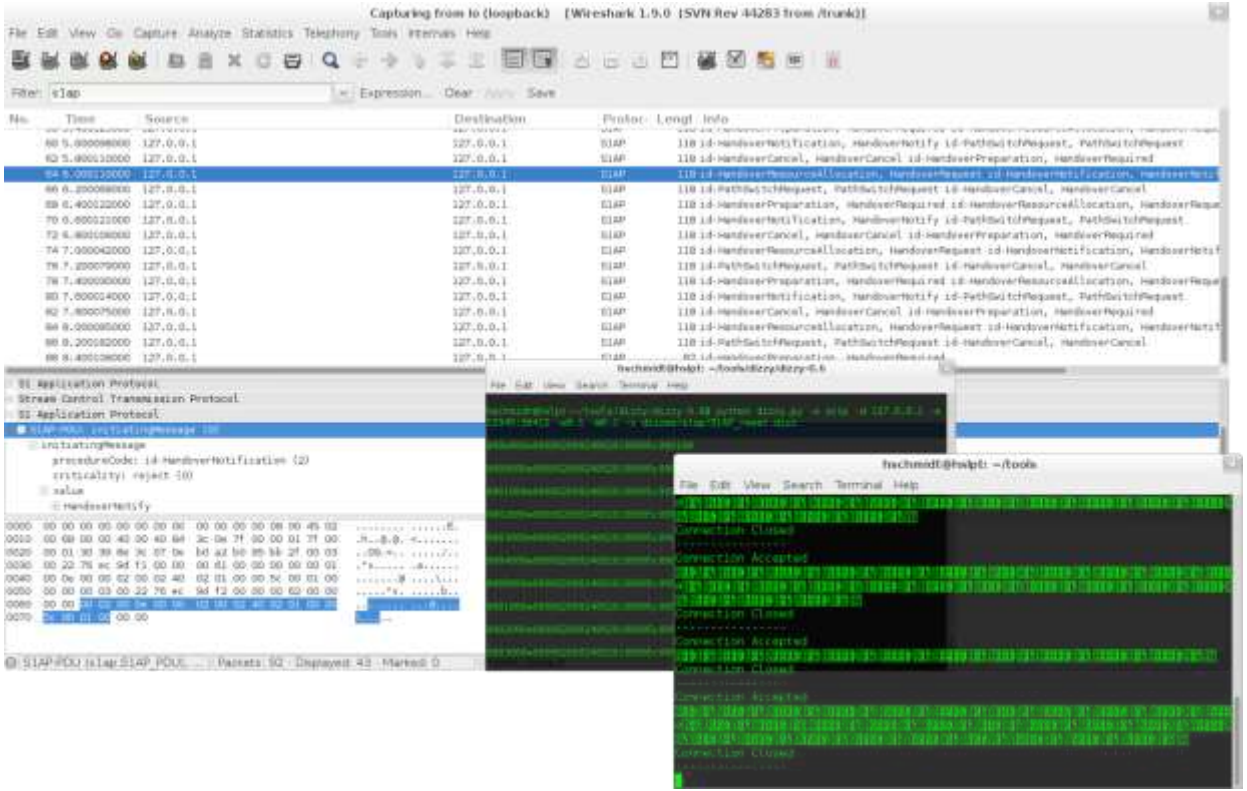
S1AP Protocol Stack



- S1 Application Protocol (S1AP), designed by 3GPP for the S1 interface
- Specified in 3GPP TS 36.413

- Necessary for several procedures between MME and eNodeB
- Also supports transparent transport procedures from MME to the user equipment

- SCTP Destination Port 36412



S1AP with Dizzy

www.insinuator.net

www.c0decafe.de

Technology in Perfection?

From: youtube.com

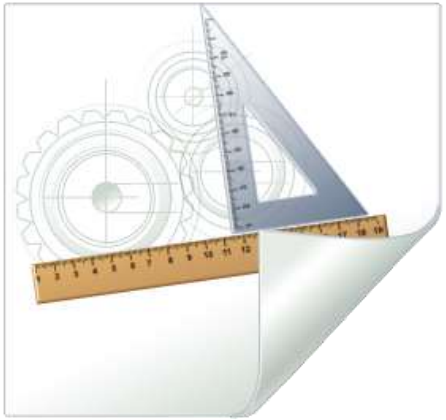
Self Organizing Networks

SON

Self Configuration

Big style " Plug & Play"

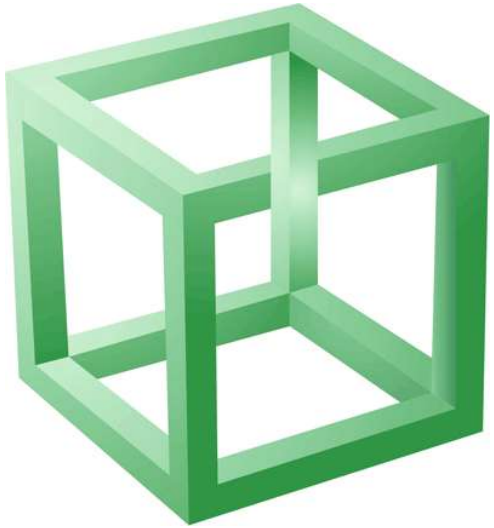
Why?



- Reduce on-site activities by installer
  - Reduce work to:
    - Connect to Antenna
    - Connect to LAN-Cable
    - Connect to Power
- Reduce installation costs
- Increase flexibility

How?

Base firmware is installed in factory



- eNB gets IP via DHCP
- Config gets pushed depending on HW-ID
- Installer configures positioning data or device uses internal GPS receiver
- (Work out PID and maybe new PID for surrounding cells)

Relay Nodes

Selective repeaters

Repeat data for certain eNodeBs

- Install and switch on
- Relay Node acts as UE
  - Connects to “Configurator eNB“
  - Fetches config from backend
- Relay Node relays data from “Donor eNB“

Self-Optimization

Optimized!

From: youtube.com

Self-Optimization

- "Automatically avoiding overlap"
- eNBs are aware of neighboring eNBs/cells
- Automated communication between adjacent eNBs
  - Band sharing both in time and frequency domains
  - Adapting of signal strength

ANR

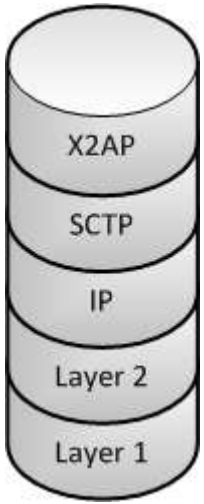
Automatic Neighbour Relation

- eNB checks for other cells in it‘s range.
  - Either itself or by asking an UE for the cells it can see
- If a cell is found, a channel is established via backend.
- Communication via X2 channel
  - Both eNBs communicate directly

HeNBs

- Home-eNodeBs are able to take part in SON process
  - The ones you might have at home
  - The ones you might have hacked and rooted
- Protocol was adapted to support communication with HeNBs
  - Addition of extra security gateway

X2 Interface



- Similar to S1AP ☺
- X2 Application Protocol (X2AP) is defined in 3GPP TS 36.423
- Interconnecting two eNodeBs within E-UTRAN architecture
  - Providing signaling information across the X2 interface
- SCTP Destination port 36422

→ Demo

Just a few thoughts

- Can I get my phone to actually make 2 eNBs think that they‘re closer than the actually re?
- Can I use my HeNB and tell a macro cell eNB, that I‘m actually covering all it‘s area and that I‘m so much better in doing so?

- → Future research

Will Darwin strike again?

Conclusions

- Overall, it is a good concept, but there is high complexity!
- Some things are a bit shocking…
- But you see: they have learned!

Random Darwin Award

(5 Feb 2013, São Paulo, Brazil)

http://darwinawards.com/darwin/darwin2013-01.html

- Mechanic Sérgio A. Rosa, 49, was welding a gas tanker that, curiously, exploded, sending his remains flying 400 meters through the air.

There's never enough time...

THANK YOU...

...for yours!

Stay in touch

- Visit our blog and join the discussion: INSINUATOR.NET
- Join us at TROOPERS.de conference!
- Ping us at Twitter: @WEareTROOPERS @Insinuator
- Drop us a mail.

Random Darwin Award

(July 2011, New York)

http://darwinawards.com/darwin/darwin2011-03.html

- Protesting motorcycle helmet laws, an Onondaga, NY man was participating in a bare-noggin protest ride when he was killed via flipping over the handlebars.

Random Darwin Award

(10 January 2007, Germany)

http://darwinawards.com/darwin/darwin2007-01.html

- A 63-year-old man's extraordinary effort to eradicate moles from his property resulted in a victory for the moles. The man pounded several metal rods into the ground and connected them [...] to a high-voltage power line, intending to render the subterranean realm uninhabitable. Incidentally, the maneuver electrified the very ground on which he stood.

Random Darwin Award

(1995)

http://darwinawards.com/darwin/darwin1996-07.html

- Azninski, 30, had been drinking with friends when it was suggested they strip naked and play some "men's games". Initially they hit each other over the head with frozen turnips, but then one man upped the ante by seizing a chainsaw and cutting off the end of his foot. Not to be outdone, Azninski grabbed the saw and, shouting "Watch this then," he swung at his own head and chopped it off.

Random Darwin Award

(27 February 2012, North Carolina)

http://darwinawards.com/darwin/darwin2012-03.html

- Gary was at a friend's apartment when he spotted a salsa jar containing a mystery fluid. Thinking that it was an alcoholic beverage, he helped himself to a sizeable swig of gasoline! Naturally enough, he immediately spit out the offending liquid onto his clothes. Then, to recover from the shock, Gary lit a cigarette.

Random Darwin Award

(5 Feb 2013, São Paulo, Brazil)

http://darwinawards.com/darwin/darwin2013-01.html

- Mechanic Sérgio A. Rosa, 49, was welding a gas tanker that, curiously, exploded, sending his remains flying 400 meters through the air.