Dumbster Driving 16: 4G LTE BaseStations

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

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*

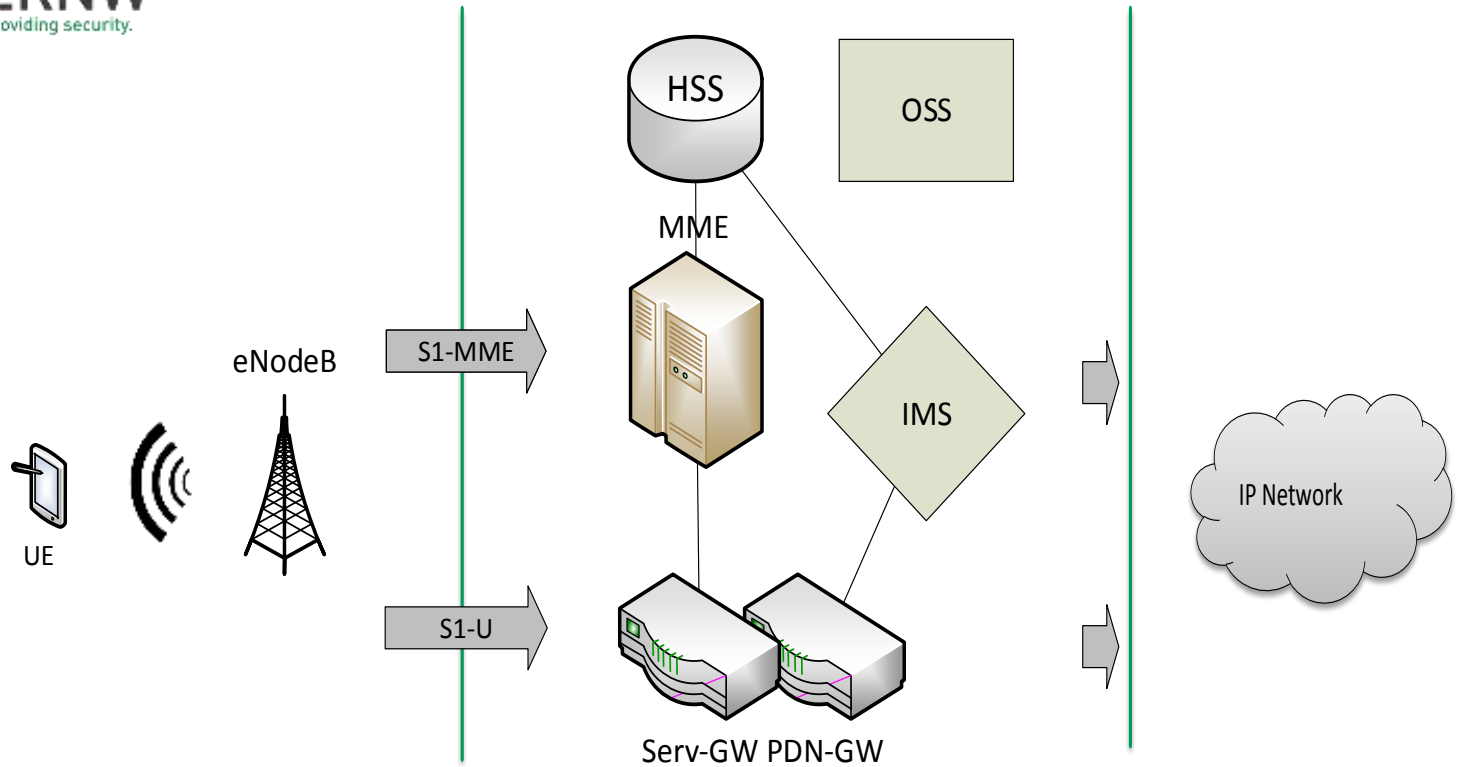
- Conference: *www.troopers.de*

TROOPERS
MAKE THE WORLD A SAFER PLACE


NO
TRESPASSING
NRS 207.200
INFORMATION
AT&T Mobility operates telecommunications antennas at this location. Remain at least 3 feet away from any antenna and obey all posted signs.
Contact the owner(s) of the antenna(s) before working closer than 3 feet from the antenna(s).
Contact AT&T Mobility at 800-638-2822 prior to performing any maintenance or repairs near AT&T Mobility antennas.
This is Site USID # L128
Contact the management office if this door/hatch/gate is found unlocked.

Introduction

A 4G/LTE Telecommunication Network



eUTRAN

4G Core

ERNW
providing security.

Typical Environment?

Source:
worldlte.blogspot.com

ERNW
providing security.

Typical Environment?

ERNW
providing security.

The Idea

1. **Understand** BaseStation Setup
2. **Purchase** an old BaseStation out of the field
3. Get BS running in an **emulated environment**
4. Perform an evaluation of **configuration & security**

What we need:
Basestation Physical Setup

- Base Band Unit (BBU)
  - Usually standing on the ground
  - Including Power Distribution Unit (PDU) and Power Supply Unit (PSU)
- Remote Radio Head/Unit (RRH/RRU)
  - May be placed on the cell mast or on the ground
- Antenna
  - Come in various shapes and sizes
  - Nowadays often vector antennas

- All active parts are interconnected
  - BBU, RRU, sensors, power supply, vents

Power Supply

- Components run on -48V
  - Not +-48V (96V differential)
  - Basically just 48V connected the other way round

RRU

- Basically receives raw RF signals via Fiber and sends them out via Copper
  - Towards the antenna
- Usually capable of serving a specific frequency band

Most important Unit: the BBU

- Frame for holding power unit and **functional blades**
- Sometimes have a backplane for interconnection between components
  - Arbitrary PCB connectors
  - Multiple interfaces (LAN, UART, Arbitrary, CAN)
- Functional blades decide the network type
  - Ericsson: DUL/DUW/DUG -> Digitial Unit LTE/WCDMA/GSM
- Slots for multiple blades
  - Single BBU could serve GSM and WCDMA
  - Depends highly on specific BBU and blade combination
- Single blade can serve multiple cells
  - Using sector antennas a single mast could i.e. serve 4 cells in 4 different directions

ERNW
providing security.

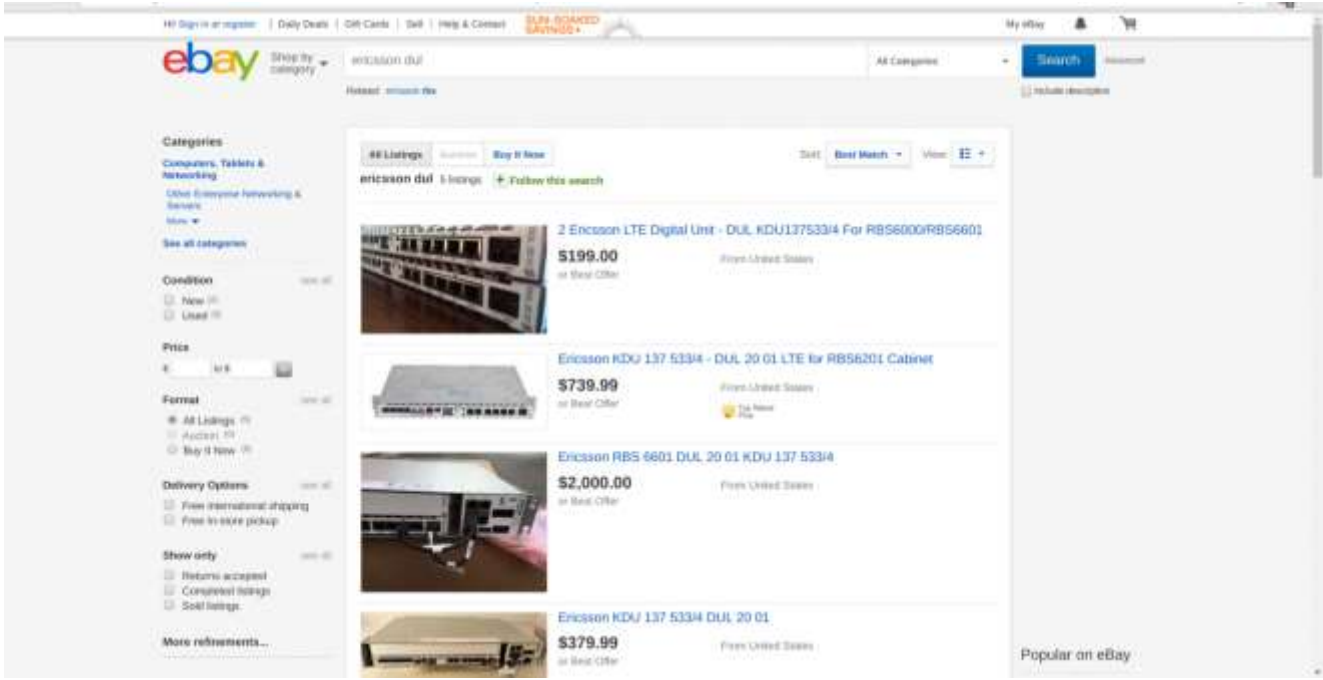
Variants of an eNodeB

- 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

Implementing a Lab

Just a Quick HowTo

ERNW
providing security.



Ebay ☺

Some helpful words:

- Nokia - FlexiBTS
- Huawei – BBU + LMPT/UMPT
- Ericsson – RBS + DUL
- ALU – MBS

Lab Setup – What You Need

- A Basestation
  - The RRU is optional if you just want to play with the BTS itself
- Power Supply
  - -48V ~ 5A will be sufficient
- Power Connectors
  - Good luck ;-)
  - The devices sometimes have strange plugs, so you might need some time to find or make them
- Stack of network cables

ERNW
providing security.

Our Lab ☺

Let‘s start reconnaissance!

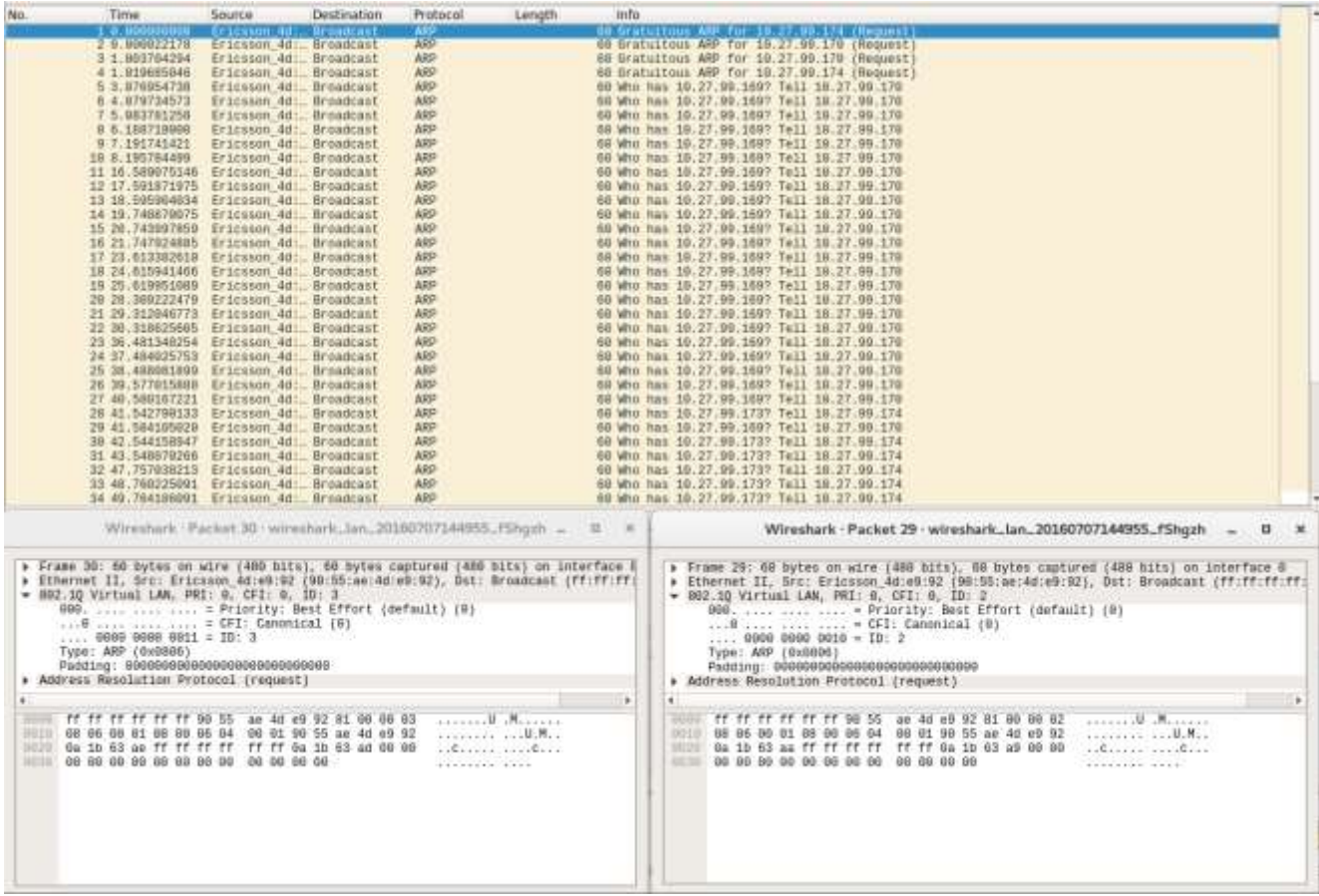
Ericsson RBS6601 - DUL
RJ-45 & Gbic Interfaces

- GPS
  - For timing or positioning (during setup)
- EC
  - Equipment Control
- AUX
  - Auxiliary Bus
- LMT A
  - Local maintenance terminal A
- LMT B
  - Local maintenance terminal B
- TN A
  - Backhaul Access – S1

- IDL
  - Inter-DUL-Link
- TN B
  - Backhaul Access – S1
- A, B, C, D, E, F
  - Interfaces towards RRU

ERNW
providing security.

The First Sniff ☺

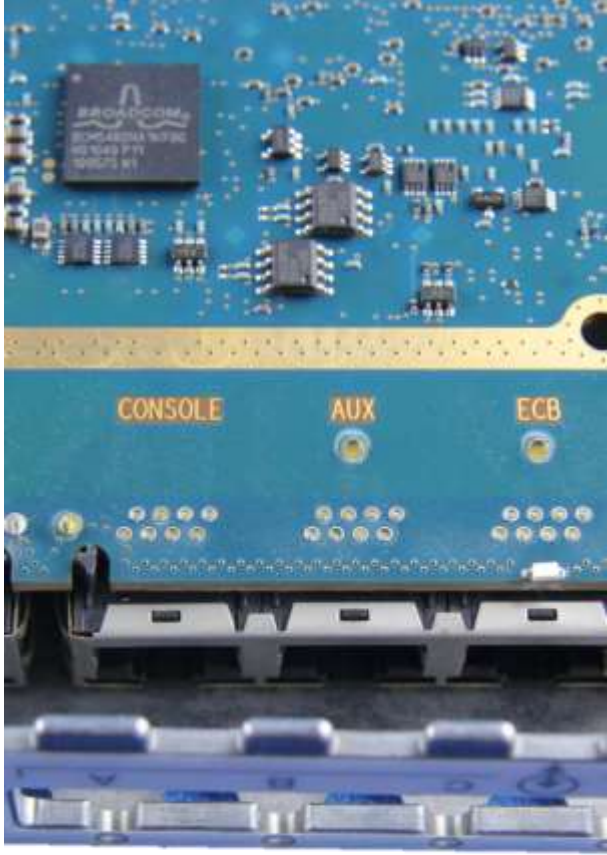


Let‘s get Started!

- The most important interfaces of our setup:
  - Vlan 3: Signalling
  - Vlan 2: O&M

- You see a lot of traffic, the eNB is designed to operate almost as standalone

  → Not that many modifications needed



ERNW
providing security.

The Second Sniff

68	13.836203560	10.27.99.170	10.168.128.12	SCTP	86	INIT
69	13.842477789	CadmusCo_d8:…	Broadcast	ARP	64	Who has 10.168.128.12? Tell 10.168.108.108
70	13.842485807	CadmusCo_d8:…	Broadcast	ARP	64	Who has 10.168.128.12? Tell 10.168.108.108
71	14.076199230	10.27.99.170	10.168.114.1…	SCTP	86	INIT
72	14.236141691	10.27.99.170	10.168.128.12	SCTP	86	INIT
73	14.282938815	CadmusCo_d8:…	Broadcast	ARP	64	Who has 10.168.114.108? Tell 10.168.108.108
74	14.282943478	CadmusCo_d8:…	Broadcast	ARP	64	Who has 10.168.114.108? Tell 10.168.108.108
75	14.476198764	10.27.99.170	10.168.114.1…	SCTP	86	INIT
76	14.636181847	10.27.99.170	10.168.128.12	SCTP	86	INIT
77	14.842608735	CadmusCo_d8:…	Broadcast	ARP	64	Who has 10.168.128.12? Tell 10.168.108.108
78	14.842614868	CadmusCo_d8:…	Broadcast	ARP	64	Who has 10.168.128.12? Tell 10.168.108.108
79	14.876198705	10.27.99.170	10.168.114.1…	SCTP	86	INIT
80	15.036202389	10.27.99.170	10.168.128.12	SCTP	86	INIT
81	15.276205130	10.27.99.170	10.168.114.1…	SCTP	86	INIT
82	15.436208968	10.27.99.170	10.168.128.12	SCTP	86	INIT
83	15.836449869	10.27.99.170	10.168.128.12	SCTP	86	INIT
84	18.849426175	Ericsson_4d:…	Broadcast	ARP	60	Who has 10.27.99.173? Tell 10.27.99.174
85	18.849620550	CadmusCo_d8:…	Ericsson_4d:…	ARP	64	10.27.99.173 is at 08:00:27:d8:80:9d
86	18.849624174	CadmusCo_d8:…	Ericsson_4d:…	ARP	64	10.27.99.173 is at 08:00:27:d8:80:9d
87	18.850380180	10.27.99.174	5.211.14.4	TCP	82	65529→50073 [SYN] Seq=0 Win=32768 Len=0 MSS=1
88	24.400646654	10.27.99.170	10.168.108.1…	SCTP	86	INIT

```
▶ Frame 87: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
▶ Ethernet II, Src: Ericsson_4d:e9:92 (90:55:ae:4d:e9:92), Dst: CadmusCo_d8:80:9d (08:00:27:d8:80:9d)
▼ 802.1Q Virtual LAN, PRI: 1, CFI: 0, ID: 3
    001. .... .... .... = Priority: Background (1)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 0000 0011 = ID: 3
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.27.99.174, Dst: 5.211.14.4
▶ Transmission Control Protocol, Src Port: 65529, Dst Port: 50073, Seq: 0, Len: 0
```

```
0000  08 00 27 d8 80 9d 90 55  ae 4d e9 92 81 00 20 03   ..'....U .M.... .
0010  08 00 45 30 00 40 00 1d  40 00 40 06 b8 cb 0a 1b   ..E0.@.. @.@.....
0020  63 ae 05 d3 0e 04 ff f9  c3 99 59 90 59 c1 00 00   c....... ..Y.Y...
0030  00 00 b0 02 80 00 bd 7a  00 00 02 04 05 b4 01 03   .......z ........
0040  03 00 04 02 01 01 01 01  08 0a 00 00 00 01 00 00   ........ ........
0050  00 00                                              ..
```

Attacking the BS

- Signalling Traffic
- Local Maintenance Interface
- Remote OAM Interface
- Physically

- Our goals: Understanding the device, configuration access and finally – getting root

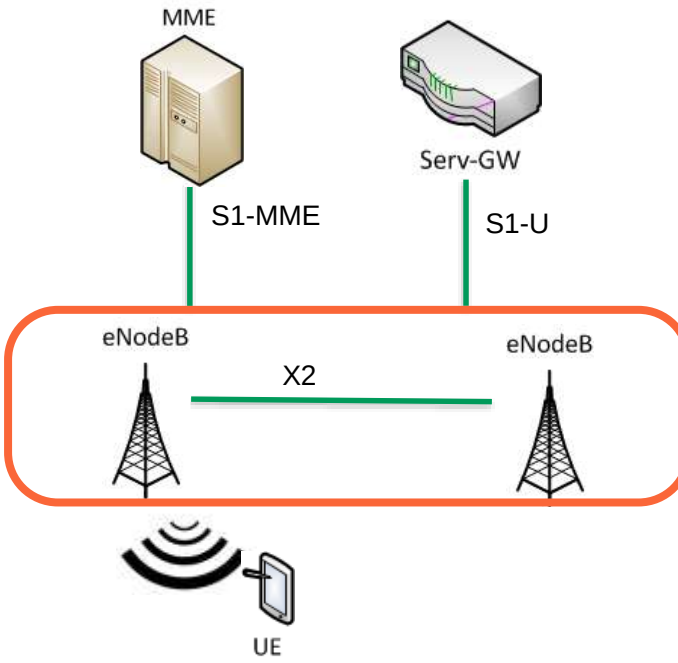
→ Keep in mind: this is a real BTS like out in the field

The Transport Interface

Access to, or How to Build Your Own Provider Network

S1-Interface

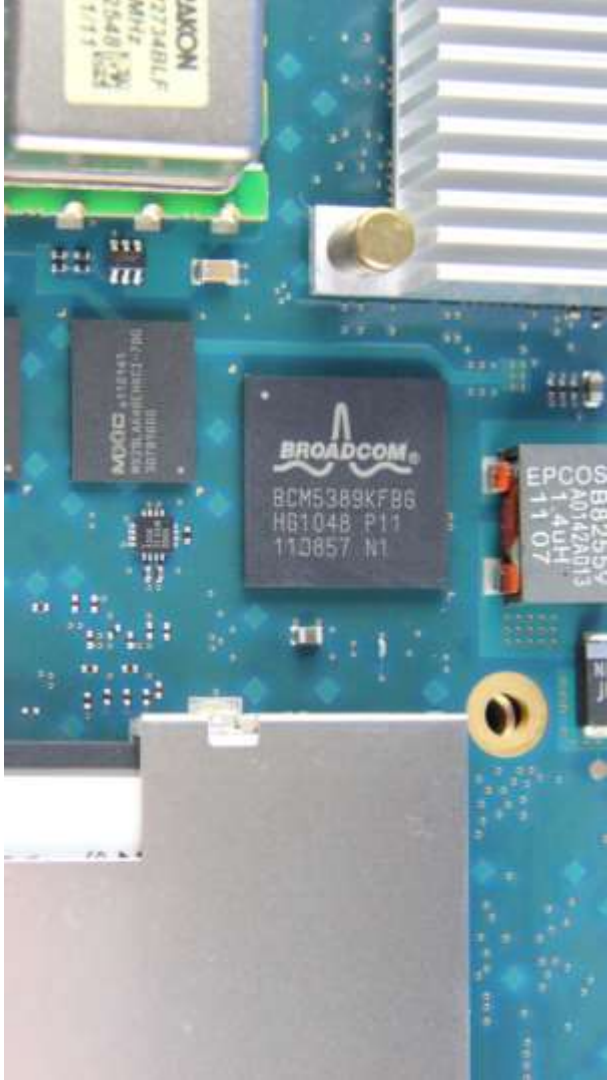
- S1 interface is divided into two parts
  - S1-MME (Control Plane)
    - Carries signalling messages between base station and MME
  - S1-U (User Plane)
    - Carries user data between base station and Serving GW



ERNW
providing security.

From 3GPP TS 33.401

- "In order to protect **the S1 and X2 control plane** as required by clause 5.3.4a, it is **required to implement IPsec** ESP according to RFC 4303 [7] as specified by TS 33.210 [5]. For both **S1-MME and X2-C**, IKEv2 certificates based authentication according to TS 33.310 [6] shall be implemented"
  - "NOTE 1: In case control plane **interfaces are trusted** (e.g. physically protected), there is **no need to use protection** according to TS 33.210 [5] and TS 33.310 [6]."
- "In order to protect the **S1 and X2 user plane** as required by clause 5.3.4, it is **required to implement IPsec** ESP according to RFC 4303 [7] as profiled by TS 33.210 [5], with confidentiality, integrity and replay 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**."
- "In order to achieve such protection, IPsec ESP according to RFC 4303 [7] as profiled by TS 33.210 [5] **shall be implemented for all O&M related traffic**, i.e. the management plane, with confidentiality, integrity and replay protection."
  - "NOTE 2: In case the S1 management plane **interfaces are trusted** (e.g. physically protected), the use of protection based on IPsec/IKEv2 or equivalent mechanisms is **not needed**."



S1-Interface

- After the host 10.27.99.169 on VLAN 2 becomes available the eNodeB activates communication over the S1-Interface

- Using SCTP it tried to reach 7 different hosts by SCTP INIT request to establish a connection

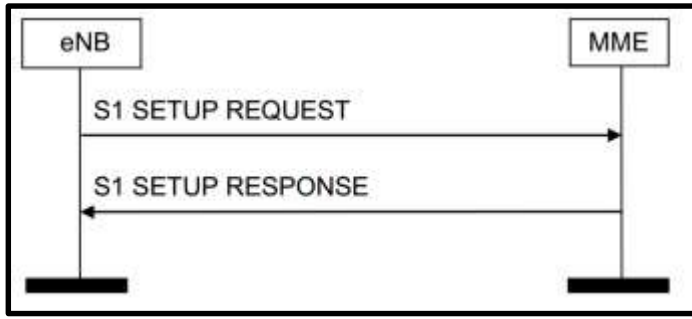
→ S1 Application Protocol (S1AP)

1	0.000000000	10.27.99.170	10.168.113.12	SCTP	86	INIT
4	0.400078216	10.27.99.170	10.168.113.12	SCTP	86	INIT
5	0.800055018	10.27.99.170	10.168.113.12	SCTP	86	INIT
6	1.200068064	10.27.99.170	10.168.113.12	SCTP	86	INIT
9	1.600097273	10.27.99.170	10.168.113.12	SCTP	86	INIT
10	2.000097083	10.27.99.170	10.168.113.12	SCTP	86	INIT
11	2.400088190	10.27.99.170	10.168.113.12	SCTP	86	INIT
22	4.104433920	10.27.99.170	10.168.105.108	SCTP	86	INIT
23	4.104592561	10.27.99.170	10.168.111.12	SCTP	86	INIT
28	4.296097420	10.27.99.170	10.168.105.108	SCTP	86	INIT
29	4.296108916	10.27.99.170	10.168.111.12	SCTP	86	INIT
32	4.696156330	10.27.99.170	10.168.105.108	SCTP	86	INIT
33	4.696169402	10.27.99.170	10.168.111.12	SCTP	86	INIT
34	5.096153686	10.27.99.170	10.168.105.108	SCTP	86	INIT
35	5.096166153	10.27.99.170	10.168.111.12	SCTP	86	INIT
40	5.496140257	10.27.99.170	10.168.105.108	SCTP	86	INIT
41	5.496153582	10.27.99.170	10.168.111.12	SCTP	86	INIT
42	5.896177502	10.27.99.170	10.168.105.108	SCTP	86	INIT
43	5.896190156	10.27.99.170	10.168.111.12	SCTP	86	INIT
48	6.296157138	10.27.99.170	10.168.105.108	SCTP	86	INIT
49	6.296170488	10.27.99.170	10.168.111.12	SCTP	86	INIT
50	6.696177961	10.27.99.170	10.168.105.108	SCTP	86	INIT
51	6.696200706	10.27.99.170	10.168.111.12	SCTP	86	INIT
52	7.096135747	10.27.99.170	10.168.105.108	SCTP	86	INIT
53	7.096146406	10.27.99.170	10.168.111.12	SCTP	86	INIT
54	12.284666659	10.27.99.170	10.168.114.108	SCTP	86	INIT
57	12.476111702	10.27.99.170	10.168.114.108	SCTP	86	INIT
58	12.844428930	10.27.99.170	10.168.128.12	SCTP	86	INIT
61	12.876174719	10.27.99.170	10.168.114.108	SCTP	86	INIT
62	13.036120357	10.27.99.170	10.168.128.12	SCTP	86	INIT
63	13.276192880	10.27.99.170	10.168.114.108	SCTP	86	INIT
66	13.436199062	10.27.99.170	10.168.128.12	SCTP	86	INIT
67	13.676148344	10.27.99.170	10.168.114.108	SCTP	86	INIT
68	13.836203560	10.27.99.170	10.168.128.12	SCTP	86	INIT
71	14.076199230	10.27.99.170	10.168.114.108	SCTP	86	INIT
72	14.236141691	10.27.99.170	10.168.128.12	SCTP	86	INIT
75	14.476198764	10.27.99.170	10.168.114.108	SCTP	86	INIT
76	14.636181847	10.27.99.170	10.168.128.12	SCTP	86	INIT
79	14.876198705	10.27.99.170	10.168.114.108	SCTP	86	INIT
80	15.036202389	10.27.99.170	10.168.128.12	SCTP	86	INIT
81	15.276205130	10.27.99.170	10.168.114.108	SCTP	86	INIT
82	15.436208968	10.27.99.170	10.168.128.12	SCTP	86	INIT
83	15.836449869	10.27.99.170	10.168.128.12	SCTP	86	INIT
88	24.400646654	10.27.99.170	10.168.108.108	SCTP	86	INIT

Let‘s get Started!

- S1-MME: Basically, only the S1 Setup Request is needed.
  - fake_mme.py
  - S1AP_enum (c0decafe.de)
  - S1AP Dizzy Scripts (insinuator.net)

- Now we can start with further attacks, like
  - UE Tracing/Tracking
  - RAN Configuration
  - E-RAB Management
  - NAS Transport



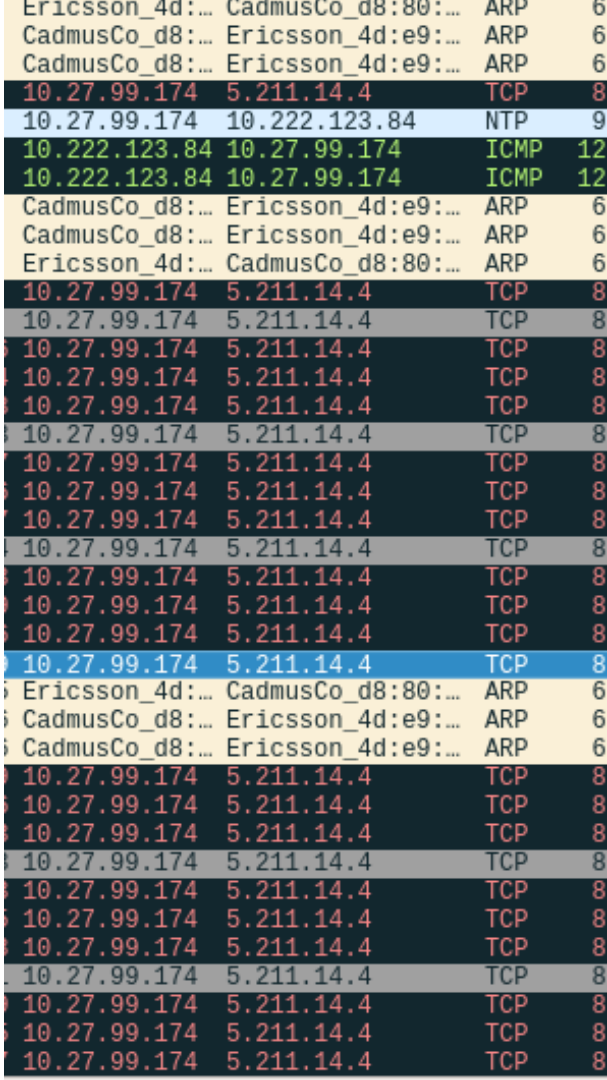
Operations & Maintenance Network

Attacking the Local and Remote Maintenance Interface

ERNW
providing security.

OAM Network

- After the host 10.27.99.173 on VLAN 3 becomes available the eNodeB starts searching for an NTP
- It also tries to establish a TCP session to some management system



Nmap Results

```
Increasing send delay for 10.27.99.174 from 0 to 5 due to 45 out of 149 dropped probes since last increase.
Nmap scan report for 10.27.99.174
Host is up, received arp-response (0.00042s latency).
Scanned at 2015-12-28 19:16:02 CET for 842s
Not shown: 65529 closed ports
Reason: 65529 resets
PORT     STATE SERVICE    REASON        VERSION
21/tcp   open  ftp        syn-ack ttl 64
22/tcp   open  ssh        syn-ack ttl 64 (protocol 2.0)
| ssh-hostkey:
|   1024 39:6b:50:b5:68:ea:cf:f9:1b:85:48:dc:cb:5f:9c:dc (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAKjBoRJD3xs/PDF7i8Zh6VVNlnykkT0aZ/OJoZM0Qb/2Zm1SruM5bYkwAczqstUWXygtgSTmP4
Dv5VHNkmR5Gb5KIe2e5GXNp4HACdAVjThkpBzK27ai+Pj+CXIHQxHcZIMgJyQDA29oCg5KFk9lbtdDkiocabW/KyuAQmxB0
mIVAAAAFQCPdjPIB+E7/0QKPKXG0pcRgIibLQAAAIBLD689UE2fmlufS53dHWsgxm9SsGD4GgP4bnRfV+G494PNfimiVv0W
oqAeDFtVqQLIxZHU2pJ275kgRyDHcp4fTaPssxZpIjyVNiZkjLjDVeZb8D562E4PnG3BVFy2VcMrq4klbO02wKwE5zQrLQfGf7O
o1rv81+1OdpZzU3N48wAAAIEAhj3FTj4i2s8vKEVXzUtdK081YHhyvOJO77niYmJ+jG2IOtt4tJpuNfvdc19ab2wtrqerQ1R6KTA9
2InhktEZvS2e4peeVho0htYoDlDQTybpw5v/LaX8c0/7vtcKJt7On+A0rZwCAd2ScQxNKpcyJAqNf9J+esFJXo9KONWkpms=
|   1024 e8:c6:48:a5:f8:7b:ed:c3:6b:30:86:a6:42:c6:04:a6 (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAz4L21u3pCegfIuLO+iz8te/XmrNhNSeCFf9SCwd8GYL7D1yktvdhn3kFPb+4gwM2B+sIn
hs0TM6+bt7HfW7AU0cPTMy3kgLxvOKU9V+Sm8QzvZSJkkKmbfnwRHY7IVvFSHNZPghWupcDUb7h7z+h3Q3BlcZP7ZQIFPd
3zXEyxIM=
23/tcp   open  telnet     syn-ack ttl 64
80/tcp   open  http       syn-ack ttl 64 WEBS - OSE web server
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: WEBS - OSE web server
|_http-title: 404 URL Not Found
8443/tcp open  tcpwrapped syn-ack ttl 64
|_xmlrpc-methods: ERROR: Script execution failed (use -d to debug)
56834/tcp open  unknown    syn-ack ttl 64
```

Maintenance Terminals

- The workflow
  1. Fault-State of BaseStation (NoService)
  2. Engineer moves on-site
  3. Engineer connects to BTS with $tool
  4. Engineer accesses debug information
  5. Engineer adjusts configuration

ERNW
providing security.

RBS Element Management Applications

Available Installer

Platform	without Java VM	Instructions
Windows	Download (2.6M)	View

Windows Instructions:

Instructions

- After downloading, double-click `em_install.exe`

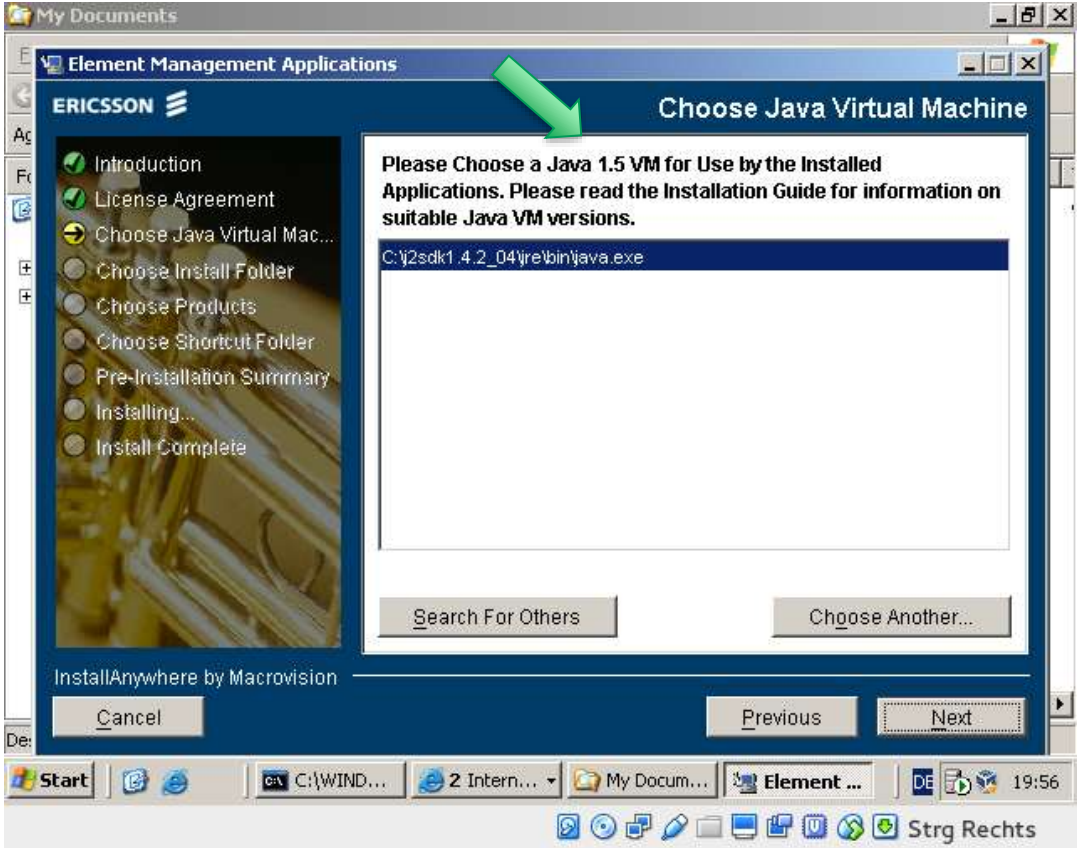
Notes

- You may need to install a Java Runtime Environment (JRE) 5.0 of the latest update. You can download one from Oracle's Java web site.

InstallAnywhere is a registered trademark of Macrovision Corporation

LMT Software Installation

... and Windows XP ...



10.27.99.174 - PHLe0760889 - RBS Element Manager

File View MO Alarm Tools Help

Radio Network | View Descriptions

MO Tree

- ENodeBFunction=1
  - Radio Network Configuration
    - EUtraNetwork=1
    - EUtranCellFDD=PHLe07608891
      - reservedBy
      - EUtranFreqRelation=2300
      - EUtranFreqRelation=_2215
      - SectorEquipmentFunction=1
      - UeMeasControl=1
    - EUtranCellFDD=PHLe07608892
    - EUtranCellFDD=PHLe07608893
    - EUtranCellFDD=PHLe07608894
    - EUtranCellFDD=PHLe07608895
    - EUtranCellFDD=PHLe07608896
  - External Connection and Interfaces
  - Radio Bearers and QoS
  - eNodeB Functionality
  - Sctp=1

Refresh Tree | Stop

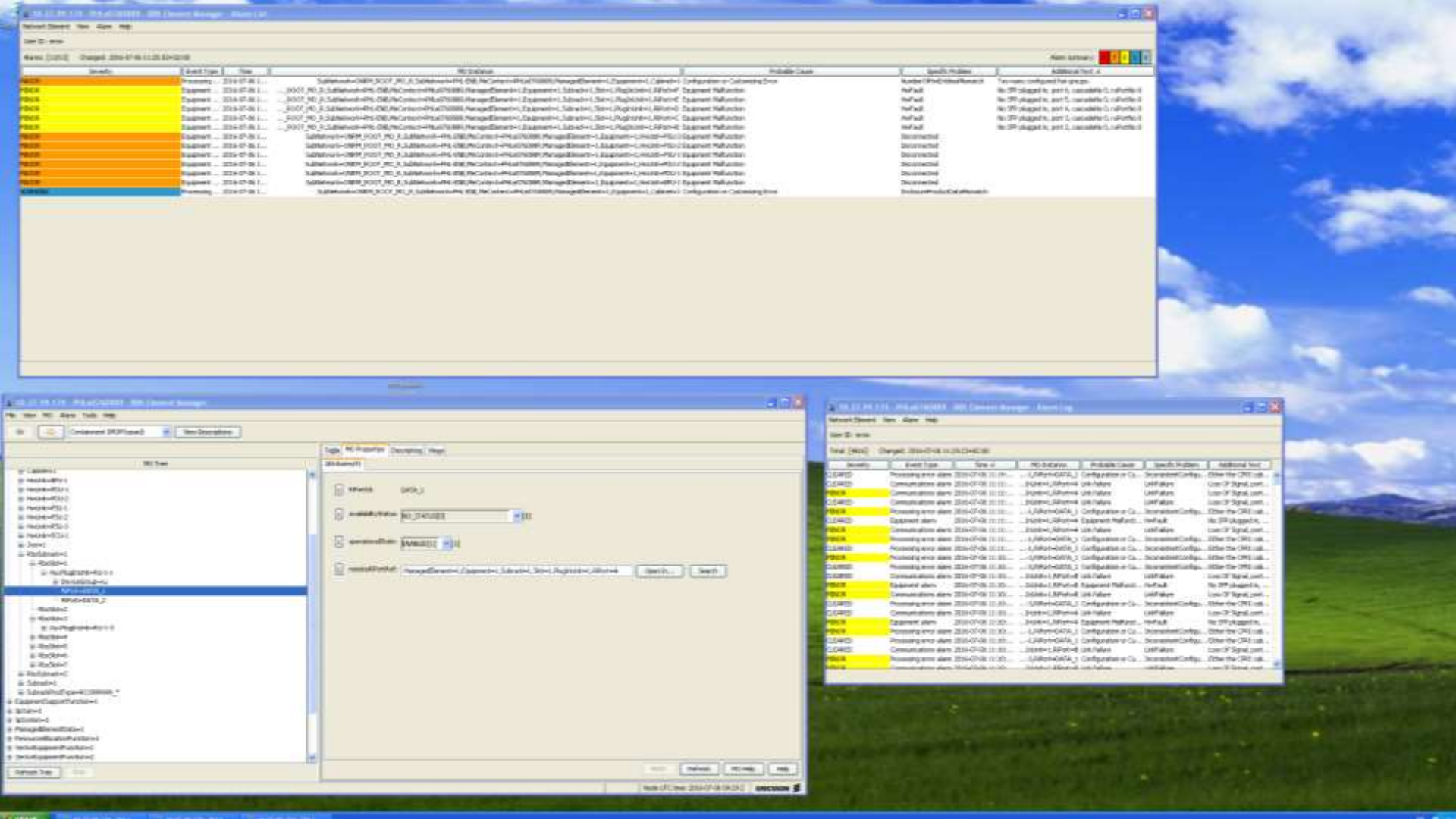
Table | MO Properties | Description | Views

Attributes(687) | Actions(3)

cellSubscriptionCapacity:	1000
cfraEnable:	true
changeNotification:	+ (8)
confidence:	100
configurableFrequencyStart:	0
covTriggerdBlindHoAllowed:	true
dlChannelBandwidth:	3000
dlConfigurableFrequencyStart:	0
dlFrequencyAllocationProportion:	100
dlInterferenceManagementActive:	false
drxActive:	true
earfcndl:	5120
earfcnul:	23120
emergencyAreaId:	+ (4)
eutranCellCoverage:	+ (3)
eutranCellPolygon:	+ (15)

Apply | Refresh

Node UTC time: 2016-0



More on eNB Security

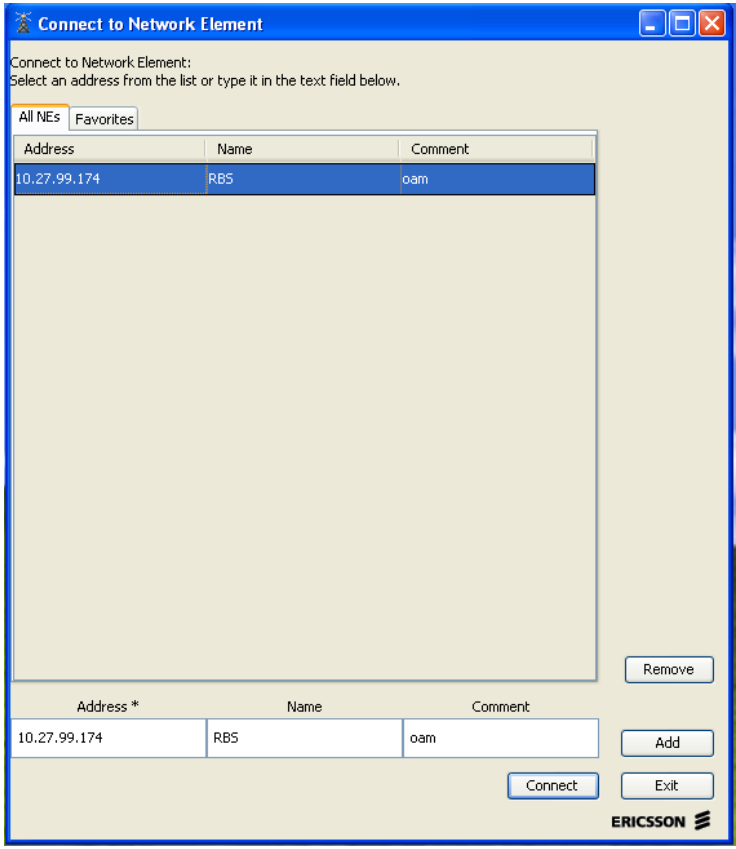
> "Setting up and configuring eNBs **shall be authenticated and authorized** so that attackers shall not be able to modify the eNB settings and software configurations via local or remote access. "

- But, anyhow: 4G BaseStations are *yet another Network Device with IP connection*.

From 3GPP TS 33.401

What we see

- FTP, Telnet, and SSH
- EM with totally outdated Java
- EM is not asking for a password
- EM is based on HTTP and GIOP
  - Transmits current configuration data of the BTS
  - Configuration changes can be made
  - Unauthorized!



Well...

```
[hschmidt@hslaptop ~]$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 rbs@10.27.99.174
rbs@10.27.99.174's password:
PTY allocation request failed on channel 0
Welcome to OSE Shell OSE5.5.
$
```

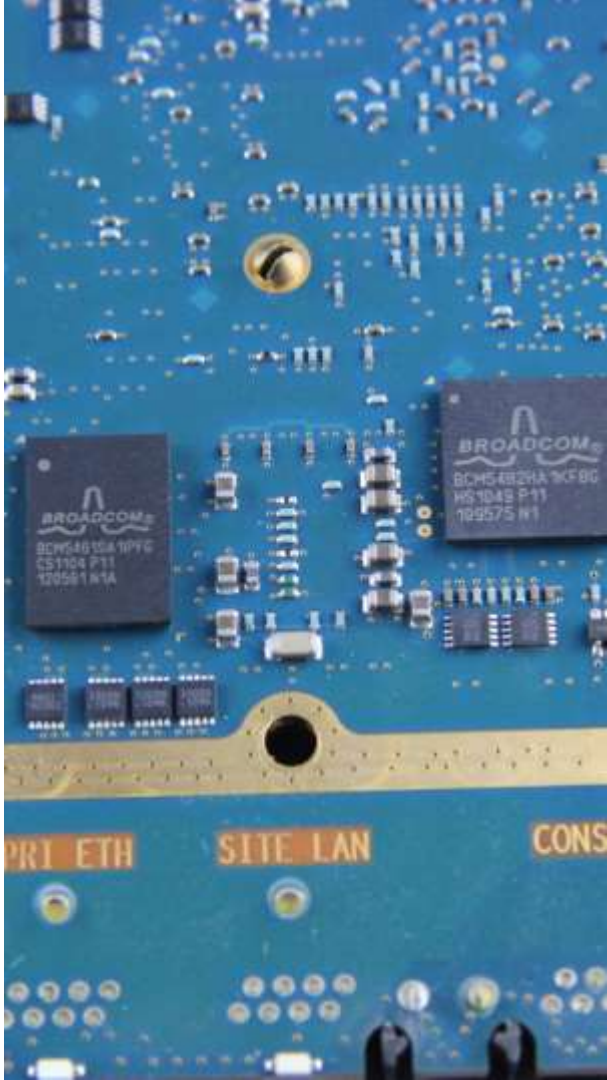
- Username: rbs / cellouser
  - Password: rbs

```
[hschmidt@hslaptop security]$ ls -al
insgesamt 48
drwxr-xr-x  4 hschmidt users 4096 14. Okt 18:43 .
drwxr-xr-x 19 hschmidt users 4096 14. Okt 18:46 ..
-rw-r--r--  1 hschmidt users 1498 14. Okt 18:43 SecurityManagement.prp
-rw-r--r--  1 hschmidt users   70 14. Okt 18:43 banner.fc
-rw-r--r--  1 hschmidt users    0 14. Okt 18:43 banner.txt
-rw-r--r--  1 hschmidt users   17 14. Okt 18:43 corbasecurity
drwxr-xr-x  2 hschmidt users 4096 14. Okt 18:41 esa
drwxr-xr-x  2 hschmidt users 4096 14. Okt 18:41 ipsec
-rw-r--r--  1 hschmidt users   52 14. Okt 18:43 iptransmode.cfg
-rw-r--r--  1 hschmidt users   65 14. Okt 18:43 passwd
-rw-r--r--  1 hschmidt users  958 14. Okt 18:43 security.cfg
-rw-r--r--  1 hschmidt users  668 14. Okt 18:43 ssh_host_dsa_key
-rw-r--r--  1 hschmidt users  534 14. Okt 18:43 ssh_host_rsa_key
[hschmidt@hslaptop security]$ cat passwd
cellouser:xxxelzYE09bDM:1234:1234:Cello User:/home/dir:/bin/tcsh
```

ERNW
providing security.

Webserver

- Running *WEBS - OSE web server*
  - EM Download
  - XML Configuration
- Java JDK (1.1.6, 1.2.1, 1.3.1, 1.4.2, 1.5.0, 1.6.0)
- Somehow, not very load resistant
  → Leading to a DoS of the whole machine



Insights

“No magic behind”

ERNW
providing security.

What We've Seen so far

- The device was obviously not wiped
- No IPSEC on S1 interface
- Hardcoded & default credentials
  - rbs – rbs
  - cellouser - rbs
- Telnet in use
- Unencrypted maintenance interface

ERNW
providing security.

Well…

- RTOS OSE 5.5
  - Running on a Motorola MPC 85xx
  - Assisted by FPGA + ARM
- GZIP Volumes and Files
  - Starting with 1F 8B
- Holding the OS on a Flashdisk

```
.....................................
.............! #"%$'&)(+*-,/.10325476
98;:=<?>A@CBEDGFIHKJMLONQPSRUTWVYX[Z
]\_^a`cbedgfihkjmlonqpsrutwvyx{z}|.~
```

The Disk

- Image must be flipped first
- PPC Binaries have format of *.ppc.elf.strip.pl.conf
- Files are gziped

→ Enables us to extract configuration data (e.g. IPSec keys) and to do reverse engineering

```
Datei   Bearbeiten   Ansicht   Suchen   Terminal   Hilfe
02420C00   1F 8B 08 08   8A D9 31 4E   02 03 68 74   74 70 5F 73   ......1N..http_s
02420C10   65 72 76 65   72 2E 70 70   63 2E 65 6C   66 2E 73 74   erver.ppc.elf.st
02420C20   72 69 70 2E   70 6C 2E 63   6F 6E 66 00   EC DA 79 70   rip.pl.conf...yp
02420C30   97 E5 B5 07   F0 BC A0 4C   A5 62 45 2B   73 5D AA 88   .......L.bE+s]..
02420C40   2D 52 88 21   09 24 21 81   28 01 03 06   B2 B0 84 A0   -R.!.$!.(.......
02420C50   B4 1A B6 B0   24 F9 25 21   1B 01 D9 A4   41 20 20 20   ....$.%!....A
02420C60   22 28 65 B5   EC 14 50 5C   61 2C 58 2C   AB C8 56 B4   "(e...P\a,X,..V.
02420C70   CA AD 1B 5A   6B 3B 53 3B   D7 7B EB D8   4D EF 2F BC   ...Zk;S;.{..M./.
02420C80   9F 20 F4 DA   4E EF FF 66   26 9C BC BF   F7 79 CE 73   . ..N..f&....y.s
02420C90   96 EF F9 9E   F3 FC 74 7A   66 76 9F A0   59 10 73 FE   ......tzfv..Y.s.
02420CA0   A7 59 CC B7   A3 FF 06 57   86 4F 5D A3   BF CF F8 AB   .Y.....W.O].....
02420CB0   6D CC 25 31   1D 62 AE 8E   69 7C 15 DD   70 49 87 73   m.%1.b..i|..pI.s
02420CC0   7F 9D 5B F8   0D BF D1 15   E1 6F B3 98   98 CB 3B 7C   ..[......o....;|
02420CD0   A9 B4 D7 5D   FE 68 7A 1F   DD 9F 5B 71   7E 7B F3 EF   ...].hz...[q~{..
02420CE0   2E 3A F7 1B   13 73 69 4C   68 4A 10 D3   BC 2A 66 78   .:...siLhJ...*fx
02420CF0   F4 8F E1 A1   51 03 62 62   EE 6E D4 D1   22 FA DB 36   ....Q.bb.n.."..6
02420D00   E6 DF FF 69   1B 9E 15 D3   22 F4 27 B7   22 A6 D9 FE   ...i....".'."...
02420D10   8A 7F 78 DF   F8 73 FD 45   BB 9A D7 0C   F0 57 6B FB   ..x..s.E.....Wk.
02420D20   1B 6D BE 3C   FA DB C9 73   B3 2B 1B F5   34 BF FA DD   .m.<...s.+..4...
02420D30   98 98 C2 0B   ED F9 06 D9   FE 5F E8 6B   7E 81 BE 2E   ........._.k~...
02420D40   E7 F5 9D 8B   C1 F9 75 31   17 C4 AB F1   A7 BB 75 C1   ......u1......u.
02420D50   F0 8B F5 35   FD 34 25 B0   D7 BF B9 2E   B7 E9 DC 70   ...5.4%........p
02420D60   5D 55 E3 BF   03 BE E2 DC   AC 7F E1 C7   37 2E F0 E3   ]U..........7..
---  compactdisk_flipped.img       --0x2420D6F/0x7D13C000--------------------
```

Ramlog

```
$ rld
rld
Displaying ramlog virtual range 0x0 - 0x3af7
__RAMLOG_SESSION_START__
0.000:BOS detected board type: gpm3blue
0.000:Number of items in the board param list=192
0.000:INFO: system pool cleared from address 0x09400000 to 0x097fffff
0.000:Detected Motorola MPC 85xx, pvr: 0x80210022
0.000:cpu_hal_85xx: init_cpu
0.000:L1CSR0=0, L1CSR1=0
0.000:mm: Using extended addressing for physical addresses.
[…]
1.3655:Timestamp format tick.usec: (1 tick = 4000 micro seconds)
1.3655:Starting HEAP
1.3960:Starting FSS
1.3979:Starting PTHREADS
1.3981:initPthreads called, not needed from OSE5.5.
1.3994:Starting GZIP volume.
2.0097:Starting RAM PMM
2.0102:PM regions= 200
2.0134:PMM: Magic not found.
2.0139:PMM: Cold start
2.0220:PMM: Restore phase completed
2.0224:Starting PM
2.0245:Starting SHELLD
2.0258:OSE5 core basic services started.
2.2744:rmm_offspring: disconnecting: 0x1001C
2.2761:rmm: disconnecting offspring due to: client killed.
2.2792:core: Starting DEVMAN
```

And the BS belongs to…?

- Looks like a BaseStation from the US ☺

```
c/logfiles/alarm_event/ALARM_LOG.xml:1f1;x4;x4;EUtranCellFDD;SubNetwork=ONRM_ROOT_MO_R,SubNetwork=PHL-ENB,MeContext=PHLe0760889,ManagedElement=1,ENodeBFunction=1,EUtranCellFDD=PHLe07608893;417;1355883768353300 00;SubNetwork=ONRM_ROOT_MO_R,SubNetwork=PHL-ENB,MeContext=PHLe0760889;356;6;ServiceUnavailable;0;S1 Connection failure for PLMN mcc:311 mnc:660;SubNetwork=ONRM_ROOT_MO_R,SubNetwork=PHL-ENB,MeContext=PHLe0760889_415;;0;2;0;0;
```

ERNW
providing security.

Using passwd

- We have the users cellouser and rbs
  - By the way, rbs is not in the passwd file
- While checking for use of hardcoded passwords in the management tool, we changed the user for rbs using passwd
- Afterwards cellouser's password was also change to the password

ERNW
providing security.

SSH

- SSH access to the device is enabled
- Sadly the only supported key exchange algorithm is disabled by default in current ssh clients
  - ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 rbs@10.27.99.174

ERNW
providing security.

Cell & UE Traces

- The eNodeB is able to create both traces for cells and UEs
- We found a set of traces on the device

- Sadly the traces seem to be purely cell traces
  - Containing data on packet loss etc.
  - No “interesting” information

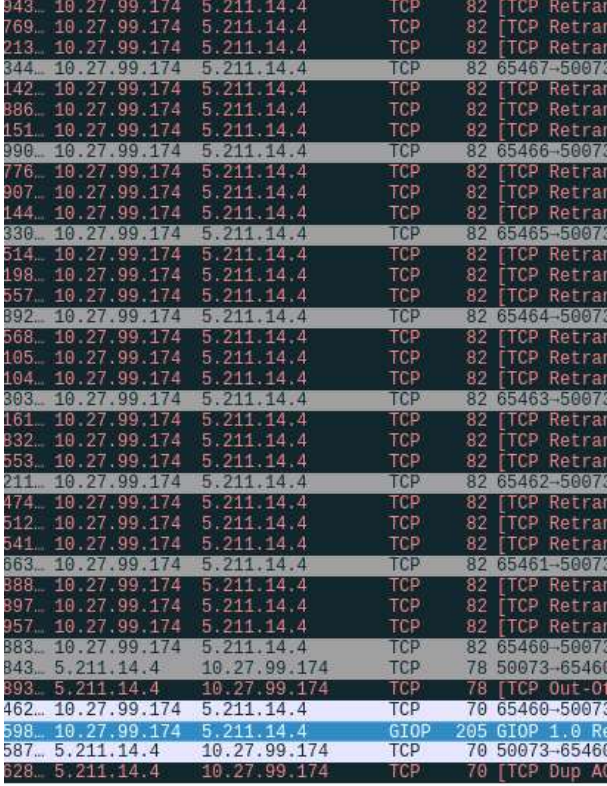
```
$ cat CellTraceFilesLocation
cat CellTraceFilesLocation
/c/pm_data
$ cat UeTraceFilesLocation
cat UeTraceFilesLocation
/c/pm_data
$ ls
ls
Directory '/j/pm_data/'
A20160706.0930-0945:1.xml.gz
A20160706.0945-1000:1.xml.gz
A20160706.1000-1015:1.xml.gz
A20160706.1015-1030:1.xml.gz
A20160706.1030-1045:1.xml.gz
A20160706.1045-1100:1.xml.gz
A20160706.1100-1115:1.xml.gz
A20160706.1115-1130:1.xml.gz
A20160706.1130-1145:1.xml.gz
A20160706.1145-1200:1.xml.gz
A20160706.1200-1215:1.xml.gz
A20160706.1215-1230:1.xml.gz
A20160706.1230-1245:1.xml.gz
A20150413.0500-0515:1.xml.gz
A20150413.0515-0530:1.xml.gz
A20150413.0530-0545:1.xml.gz
A20150413.0545-0600:1.xml.gz
A20150413.0600-0615:1.xml.gz
A20150413.0615-0630:1.xml.gz
A20150413.0630-0645:1.xml.gz
A20150413.0645-0700:1.xml.gz
A20150413.0700-0715:1.xml.gz
A20150413.0715-0730:1.xml.gz
A20150413.0730-0745:1.xml.gz
A20150413.0800-0815:1.xml.gz
A20150413.0815-0830:1.xml.gz
A20150413.0830-0845:1.xml.gz
A20150413.0845-0900:1.xml.gz
A20150413.0900-0915:1.xml.gz
A20150413.0915-0930:1.xml.gz
A20150413.0930-0945:1.xml.gz
A20150413.0945-1000:1.xml.gz
A20150413.1000-1015:1.xml.gz
A20150413.1015-1030:1.xml.gz
A20150413.1030-1045:1.xml.gz
A20150413.1045-1100:1.xml.gz
A20150413.1100-1115:1.xml.gz
A20150413.1115-1130:1.xml.gz
A20150413.1130-1145:1.xml.gz
A20150413.1145-1200:1.xml.gz
A20150413.1200-1215:1.xml.gz
A20150413.1215-1230:1.xml.gz
A20150413.1230-1245:1.xml.gz
```

ERNW
providing security.

GIOP Remote Session

- The eNodeB ties to establish a TCP session with 5.211.14.4
- When connected it sends a simple GIOP request
- Seems to be: Java IDL: Interoperable Naming Service (INS)

```
root@eNodeB-ROUTE:~# nc -l 50073
GIOP{    JACnode
                NameService_is_a+IDL:omg.org/CosNaming/NamingContextExt:1.0
```



ERNW
providing security.

IP Address: 5.211.14.4

- This is the only public IP address the device talks to
- Strangely (reminder of the operator: MetroPCS, USA) the IP address is located in Iran
- From the dates we've seen the eNodeB was initially provisioned and setup in 2013
  - The IP address range was registered in 2012 for an Iranian telco

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '5.211.0.0 - 5.211.255.255'

% Abuse contact for '5.211.0.0 - 5.211.255.255' is 'abuse@mci.ir'

inetnum:        5.211.0.0 - 5.211.255.255
netname:        GPRS
descr:          LTE
country:        IR
admin-c:        RL7844-RIPE
tech-c:         RL7844-RIPE
status:         ASSIGNED PA
mnt-by:         MCCI-MNT
created:        2015-02-18T10:58:50Z
last-modified:  2015-02-18T10:58:50Z
source:         RIPE

person:         Reza Taham Latibari
address:        Hamrah Tower - Kordestan High way cross Vanak st.Tehran Iran
phone:          +98 21 88640934
nic-hdl:        RL7844-RIPE
mnt-by:         MCCI-MNT
created:        2012-09-05T13:41:38Z
last-modified:  2012-09-05T13:41:39Z
source:         RIPE # Filtered

% Information related to '5.211.0.0/16AS197207'

route:          5.211.0.0/16
descr:          New services for 4G
origin:         AS197207
mnt-by:         MCCI-MNT
created:        2015-02-18T11:49:18Z
last-modified:  2015-02-18T11:49:18Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.87.4 (BLAARKOP)
```

IP Address: 5.211.14.4

- Looks strange?
- Well, we can not disprove:
  - The IP address range might have been shared/let/lent
  - The operator might have misused public IPs privately
- The port seems to be down

ERNW
providing security.

Summary

- Signalling: Security based on IPSec, but Attackers might be able to get the keys easily via local access
- OAM: Hardcoded passwords, weak management protocols
- Physical Access: LMT, no local encryption, debug interfaces

ERNW
providing security.

Thank you for your Attention!

hschmidt@ernw.de
bbutterly@ernw.de

@hendrks_
@BadgeWizard

www.ernw.de

www.insinuator.net