Attacking BaseStations

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

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

- BaseStations are the big (and small) antennas in the field

- With our research we want to bring visibility to
  - How the environment works
  - What providers do
  - What vendors do
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
Typical Environment?

Source: worldlte.blogspot.com
Typical Environment?
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 -> Digital 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
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
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
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
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
The Second Sniff
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
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
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-AP

- S1 Application Protocol (S1AP), designed by 3GPP for the S1 interface
- Specified in 3GPP TS36.413
- Necessary for several procedures between MME and eNodeB
- Also supports transparent transport procedures from MME to the user equipment
- SCTP Destination Port 36412
S1AP and X2AP Functions Overview

- E-RAB management functions (setup, management, modifying)
- An "Initial Context transfer" function to establish a S1UE context in the eNodeB to setup E-RABs, IP connectivity and NAS signaling.
- UE Capability Info Indication function: providing UE capability information.
- Mobility functions for UE, active in LTE network in case of change of the eNodeB or RAN (e.g. location change).
- Paging: provides the capability for the MME to page the UE.
- NAS signaling transport
- S1 UE context release/modification functions: modify and release UE context information
- Status transfer: transferring Packet Data Convergence Protocol (PDCP) SN, defined at [31], status information between two eNodeBs.
- Trace functions
- Location Reporting functions
- LPPa (LTE Positioning Protocol Annex) signaling transport: providing the transfer of LPPa messages between eNodeB and E-SMLC.
- S1 CDMA2000 tunneling functions: carrying CDMA2000 signaling messages between the UE and the CDMA2000 RAT.
- Warning message transmission
- RAN Information Management (RIM) functions: transferring RAN system information between two RAN nodes.
- Configuration Transfer functions: requesting and transferring RAN configuration information
Let's get Started!

- S1-MME: Basically, only the S1 Setup Request is needed.
  - fake_mme.py
Working with S1AP

- After S1 Setup Request, a couple of messages can be sent.

- S1AP Scanner published in the past (www.insinuator.net)
  - S1AP_enum
  - S1AP Dizzy Scripts

- New scripts:
  - fake_mme.py
  - sctp_mitm.py
Operations & Maintenance Network

Attacking the Local and Remote Maintenance Interface
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
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

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE SERVICE</th>
<th>REASON</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td>syn-ack ttl 64</td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td>syn-ack ttl 64 [protocol 2.0]</td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td>syn-ack ttl 64</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td>syn-ack ttl 64 OSE web server</td>
</tr>
</tbody>
</table>

Nmap Results
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
RBS Element Management Applications

Available Installer

Platform: Windows

without Java VM

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.
LMT Software Installation

... and Windows XP ...
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.
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...

- Username: rbs / cellouser
- Password: rbs

```bash
[hschmidt@helaptop security]$ ls -al
insgesamt 48
dwxr-xr-x 19 hschmidt users 4096 14. Okt 18:46..
-rwxr--r-- 1 hschmidt users 70 14. Okt 18:43 banner.fc
-rwxr--r-- 1 hschmidt users 0 14. Okt 18:43 banner.txt
-rwxr--r-- 1 hschmidt users 17 14. Okt 18:43 corbasecurity
dwxr-xr-x 2 hschmidt users 4096 14. Okt 18:41 esa
dwxr-xr-x 2 hschmidt users 4096 14. Okt 18:41 ipsec
-rwxr--r-- 1 hschmidt users 52 14. Okt 18:43 lptransmode.cfg
-rwxr--r-- 1 hschmidt users 65 14. Okt 18:43 passwd
-rwxr--r-- 1 hschmidt users 958 14. Okt 18:43 security.cfg
-rwxr--r-- 1 hschmidt users 668 14. Okt 18:43 ssh_host_dsa_key
-rwxr--r-- 1 hschmidt users 534 14. Okt 18:43 ssh_host_rsa_key
[hschmidt@helaptop security]$ cat passwd
"cellouser:xxxxelzyEG9BDM:1234:1234:Cell User:/home/dir:/bin/tcsh
```
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”
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
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
Image must be flipped first.

PPC Binaries have format of *.ppc.elf.strip.pl.conf

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

**The Disk**
$ 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=PHLe0760889;417;13558837683530000;SubNetwork=ONRM_ROOT_MO_R,SubNetwork=PHL-ENB,MeContext=PHLe0760889_415;;0;2;0;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;
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
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`
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
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)
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.
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
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
Thank you for your Attention!