

#### Dumbster Driving 16: 4G LTE BaseStations

Hendrik Schmidt <hschmidt@ernw.de> / @hendrks\_ Brian Butterly <bbutterly@ernw.de> / @BadgeWizard



#### Who we are

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



# 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

- o 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)
  - $\circ$  May be placed on the cell mast or on the ground
- o Antenna
  - Come in various shapes and sizes
  - o Nowadays often vector antennas
- All active parts are interconnected
  - o BBU, RRU, sensors, power supply, vents





# **Power Supply**

- o 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
  - $\circ$   $\;$  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



# Variants of an eNodeB

- $\circ~$  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)
  - o (WiFi/WiMax)
- Termination Point for Encryption
  - o 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

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









Our Lab 😊

Let's start reconnaissance!





## Ericsson RBS6601 - DUL RJ-45 & Gbic Interfaces

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

o IDL

• Inter-DUL-Link

- TN B
   Backhaul Access S1
- A, B, C, D, E, F
   Interfaces towards RRU



40.	Time	Source	Destination	Protocol	Length	info
110	1.0.00000000	Ericsson ad.,	- Broatcast	A89	in the second	de Gratuitous ARP. for 10.27.00.174 (Reguesi)
	2 9.900022178	Ericsson_4di.	Broadcast	A89		60 Gratuitous ARP for 19.27.99.170 (Request)
	3 1.803704294	Erlesson_4d	Broadcast	ARP		68 Gratuitous ARP for 10.27,99.170 (Request)
	4 1.819685846	Ericesan_4d	Broadcast	ARP		68 Bratultous ARP for 18.27.99.174 (Request)
	5 3,876954738	Ericsson_4d	Breadcast	NP		00 Who Nas 10.27.99.1697 Tell 18.27.99.179
	6 4.879734573	Eracsaan_4d	Broadcast	ASP		68 Who Res 10.27.99.1697 Tell 18.27.99.170
	7.5.983781258	Ericsson_Ad:.	Broadcast	ARP		60 Who has 10.27.99.1697 Tell 10.27.99.179
	8 5.188718998	Erlesson_4d:	Broadcast	ARP		00 Who has 10.27.99.109? Tell 18.27.99.170
	9 7,191741421	Ericsson_4d	Broadcast	ARP		68 Who has 10.27.99.169? Tell 19.27.99.170
	18 8.195764499	Ericsson_4d	Broadcast	ARP		60 Who Has 10,27,99,160? Tell 10,27,99,170
	11 10.589075146	Ericsson_4d	Broadcast	ARP		00 Who has 10.27.99.1697 Tell 10.27.00.170
	12 17.591871975	Ericsson_4d	Broadcast	A892		66 Who has 19.27.99.1597 Tell 18.27.99.170
	13 18.295904034	Ericsson_4d	Broadcast	405		60 Who has 10.27 MU.1507 Hell 18.27 WL170
	14 19./488/00/5	tricsson_4d	Broadcast	N/GP		60 Whit New 10.27, WE 1997 Tell 18.27, 99, 170
	15 20.743097859	Tricston 4d	Broadcast	AND		NU WHO HAS 10.27, WP.1507 Jell 10.27, 90.170
	16 21,747924885	Ericsson_4d	Broapcast	4892		60 WHI RAS 10.27.99.1507 Tell 10.27.99.170
	17 23.013382018	Ericsson_40:	Broadcast	ARP		00 MHD Ras 10.27.99.1007 Tell 10.27.99.170
	18 24 015941400	EF128501_40	Broadcast	ARC <sup>2</sup>		00 WHI GAS 19.27.09,1007 1011 10.27.09.170
	18 20.019901089	Ericsson_4d	Broadcast	480		00 WHO 588 10.27.39.1007 TELL 10.27.99.170
	28 28.389222479	Ericsson_4d	Broadcast	ADD		00 WHO Real 10, 27, 07, 1001 10, 27, 99, 170
	21 29.0220980/13	Er lesson_4d	Broadcant	ADD		50 WHO HER 19,27,39,1997 1011 20.27,99 170
	12 30,318625685	Ericeron 4d	Recordsort	490		60 WHO has 10 77 06 1007 1611 18 27 90 176
	33 30,481348254	Ericeson 4d	Broadcast	400		40 WHI NAS 19,27,39,1997 1841 18.27,99 178
	28 37,484043733	Ericsson_4d	Broadcast	ADD		20 400 0as 10.27.30,1007 1811 10.27.30,10
	25 28,482081899	Ericsion 40	Remainder	400		50 WHI 1985 10,27 WE 1997 1911 10,27 WE 170
	20 39.5770150080	Ericsson 40:	Broadcast	ARC		00 MPG Ram 10,27, MP.1000 TELL 10.27, MP.170
	21 48,000101221	Erisson dd	Breadcast	ARP ARE		00 WHO THIS 19,27,99,1007 FELL 10,27,00,170
	28 41,042/98133	Ericsson_4d	Breadcast	ARP		00 WED RES 10.27 07:1737 FELL 10.27 09:174
	29 41.084100028	Ericsson_4d	Broadcast	ANY		90 WTO 685 10.27.99.1097 1011 10.27.90.170
	30 42.044138347	Ericsson_40	Broadcast	400		10 WHO HER 10/2/100.1/07 HELL 20.2/102.2/4
	31 43.040070200	Ericsson 40	Broadcast	400		70 WHO Has 20.27 JUL17 (1112 20.27 JUL1 40 21 20.27 JUL1 4
	39 49 760535004	Ericeton 4d	Breadcast	APO		40 Heb has 10 7 00 1792 Tell 10 27 00 172
	34 49,784186001	Ericason 4d	Breadcast	ARP		60 Who nas 10, 27, 99, 1727 Tail 10, 27, 00, 174
	Wireshark Pa	iciant 30 · wines	hark, Jan. 201	60707144955		E # Wireshark - Packet 29 - wireshark _lan_20160707144955_f5hgzh _ U ×
Fram Ethe HD2. 0	e 30: 50 bytes en i rmet 11, Src: Eric 10 Virtual LAM, PR 80.	wirw (480 hits son_4d:#0:92 I: 0, CFI: 0, = Priority: Be = CFI: Canonic = ID: 3 000000000000000000000000000000000000	), 60 bytes c (90:55:ae 4d) 10:3 est Effort (d al (6) 2008 J	aptured (486 e9:92), Dst: efault) (9)	Bits} on inter Broadcast (ff)	<pre>rface 1     Frame 29: 00 bytes on wire (480 bits), 80 bytes cmptured (488 bits) on interface 8     iff:ff         Finermet II, Err: Frinsson 4d:00:92 (98:55:se:4d:09:92), Dat: Broadcast (ff:ff:ff:ff:             902.30 Virtual LAM, PRI: 9, CFI: 0, ID: 2             000</pre>
417						
2009 2010 2020 2020	rf ff ff ff ff ff ff ff 80 38 86 88 81 88 80 8 34 15 63 40 ff ff f 36 88 80 80 80 80 80 8	10 55 am 40 65 16 64 66 81 90 17 77 77 77 76 18 60 80 80 80 80	92 81 00 08 95 ac 4d 09 15 63 ad 00 60	83 92 99 	U .M U.R c	Norm         Off ff

The First Sniff ©



# Let's get Started!

- The most important interfaces of our setup:
  - Vlan 3: Signalling
  - o Vlan 2: 0&M
- You see a lot of traffic, the eNB is designed to operate almost as standalone
  - $\rightarrow$  Not that many modifications needed





	68 13.836203560	10.27.99.170 10.168.128.12	SCTP 86	INIT
1	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
1	71 14.076199230	10.27.99.170 10.168.114.1	SCTP 86	INIT
I	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
1	75 14.476198764	10.27.99.170 10.168.114.1	SCTP 86	INIT
I	76 14.636181847	10.27.99.170 10.168.128.12	SCTP 86	INIT
I	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
I	79 14.876198705	10.27.99.170 10.168.114.1	SCTP 86	INIT
I	80 15.036202389	10.27.99.170 10.168.128.12	SCTP 86	INIT
I	81 15.276205130	10.27.99.170 10.168.114.1	SCTP 86	INIT
I	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
I	84 18.849426175	Ericsson_4d: Broadcast	ARP 60	Who has 10.27.99.173? Tell 10.27.99.174
1	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
	F 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
1	Frame 87: 82 bytes on wi	re (656 bits), 82 bytes capt	ured (656 bits) on interface	0
I	Ethernet II, Src: Ericss	on_4d:e9:92 (90:55:ae:4d:e9:	92), Dst: CadmusCo_d8:80:9d	(08:00:27:d8:80:9d)
1	▼ 802.10 Virtual LAN, PRI:	1, CFI: 0, İD: 3		•
I	001 =	Priority: Background (1)		
I		CFI: Canonical (0)		
I	0000 0000 0011 =	ID: 3		
I	Type: IPv4 (0x0800)			
I	Internet Protocol Version	n 4, Src: 10.27.99.174, Dst:	5.211.14.4	
I	Transmission Control Pro	tocol, Src Port: 65529, Dst	Port: 50073, Seq: 0, Len: 0	
J				
1	0000 08 00 27 d8 80 9d 90	55 ae 4d e9 92 81 00 20 03	'U .M	
I	0010 08 00 45 30 00 40 00	1d 40 00 40 06 b8 cb 0a 1b	E0.0 0.0	
	0020 63 ae 05 d3 0e 04 ff	f9 c3 99 59 90 59 c1 00 00	cY.Y	
I	0030 00 00 b0 02 80 00 bd	7a 00 00 02 04 05 b4 01 03	Z	
I	0040 03 00 04 02 01 01 01	01 08 0a 00 00 00 01 00 00		
l	0050 00 00			
1				
1				

#### The Second Sniff



# Attacking the BS

- o Signalling Traffic
- Local Maintenance Interface
- Remote OAM Interface
- o Physically
- Our goals: <u>Understanding</u> the device, <u>configuration</u> access and finally – <u>getting root</u>
- $\rightarrow$  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

- $\circ~$  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





#### 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

 $\rightarrow$  S1 Application Protocol (S1AP)

1	8.999999999	18.27.99.179	19,168,113,12	SCIP	86 INI
- 4	0.499978216	10.27.99.170	10.168.113.12	SCTP	86 INIT
5	0.800955018	10.27.99.170	10.168.113.12	SCTP	86 INIT
6	1.290968964	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	2.800897083	10.27.99.170	10.168,113.12	SCTP	86 INIT
11	2.400088190	10.27.99.170	10.168.113.12	SCTP	86 INI1
22	4.104433920	10.27.99.170	10.168.105.108	SCTP	86 INI1
23	4.104592561	10.27.99.170	10.168.111.12	SCTP	86 INI1
28	4.296897428	10.27.99.170	10.168.105.108	SCTP	86 INIT
29	4.296108916	10.27.99.170	10.168.111.12	SCTP	86 INI1
-32	4.696156339	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	19.168.105.108	SCTP	86 INI1
35	5.096166153	10.27.99.170	10.168,111.12	SCTP	86 INI]
40	5.496140257	10.27.99.170	10.168.105.108	SCTP	86 INI]
41	5.496153582	10.27.99.170	10.168.111.12	SCTP	86 INI3
42	5.896177502	10.27.99.170	10.168.105.108	SCTP	86 INI1
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 INI7
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 INI1
52	7.896135747	10.27.99.170	10.168.105.108	SCTP	86 INIT
53	7.096146406	10.27.99.170	10.168.111.12	SCTP	86 INI1
- 54	12.284666659	10.27.99.170	19,168,114,108	SCTP	86 INI1
57	12.476111702	10.27.99.170	10.168.114.108	SCTP	86 INI
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 INI1
62	13.036120357	10.27.99.170	10.168.128.12	SCTP	86 INIT
63	13.276192899	10.27.99.170	19.168.114.108	SCTP	86 INI1
66	13.436199062	10.27.99.170	10.168.128.12	SCTP	86 INI1
67	13.676148344	10.27.99.170	10.168.114.108	SCTP	86 INI1
68	13.836203560	10.27.99.170	10.168.128.12	SCTP	86 INI1
71	14.076199230	10.27.99.170	10.168.114.108	SCTP	85 INI1
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 INI1
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
89	15.035202389	10.27.99.170	10.168.128.12	SCTP	86 INI1
81	15.276205130	10.27.99.170	18.168.114.108	SCTP	86 INI1
82	15.436208968	10.27.99.170	10.168,128.12	SCTP	86 INI
83	15.836449869	10.27.99.170	10.168.128.12	SCTP	86 INI1
88	24.409646654	10.27.99.170	10.168.108.108	SCTP	86 INI1



# 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
  - $\circ$  RAN Configuration
  - o E-RAB Management
  - NAS Transport

S1 SETUP REQUEST	
of Seron Redocon	_
S1 SETUP RESPONSE	



#### **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

CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       10.222.123.84       10.27.99.174       ICMP         10.222.123.84       10.27.99.174       ICMP       1         cadmusCo_d8:       Ericsson_4d:e9:       ARP         cadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP	LI 1033011_40	cauliusco_uo.oo	AILE	0
CadmusCo_d8: Ericsson_4d:e9: ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       10.222.123.84       NTP         10.222.123.84       10.27.99.174       ICMP 1         10.222.123.84       10.27.99.174       ICMP 1         10.222.123.84       10.27.99.174       ICMP 1         10.222.123.84       10.27.99.174       ICMP 1         cadmusCo_d8: Ericsson_4d:e9: ARP       CadmusCo_d8: ARP         cadmusCo_d8: Ericsson_4d:e9: ARP       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4       TCP </td <td>CadmusCo_d8:</td> <td>Ericsson_4d:e9:…</td> <td>ARP</td> <td>6</td>	CadmusCo_d8:	Ericsson_4d:e9:…	ARP	6
10.27.99.174       5.211.14.4       TCP         10.27.99.174       10.222.123.84       10.27.99.174       ICMP       1         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174	CadmusCo_d8:	Ericsson_4d:e9:…	ARP	6
10.27.99.174       10.222.123.84       NTP         10.222.123.84       10.27.99.174       ICMP       1         10.222.123.84       10.27.99.174       ICMP       1         10.222.123.84       10.27.99.174       ICMP       1         10.222.123.84       10.27.99.174       ICMP       1         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         I0.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4       TCP	10.27.99.174	5.211.14.4	TCP	8
10.222.123.84       10.27.99.174       ICMP       1         10.222.123.84       10.27.99.174       ICMP       1         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       CadmusCo_d8:80:       ARP         Ericsson_4d:       CadmusCo_d8:80:       ARP         10.27.99.174       5.211.14.4       TCP         <	10.27.99.174	10.222.123.84	NTP	9
10.222.123.84       10.27.99.174       ICMP       1         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         Ericsson_4d:       CadmusCo_d8:80:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       5	10.222.123.84	10.27.99.174	ICMP	12
CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         Ericsson_4d:       CadmusCo_d8:80:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4	10.222.123.84	10.27.99.174	ICMP	12
CadmusCo_d8:       Ericsson_4d::e9:       ARP         Ericsson_4d:       CadmusCo_d8:80:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4       TCP <td>CadmusCo_d8:</td> <td>Ericsson_4d:e9:…</td> <td>ARP</td> <td>6</td>	CadmusCo_d8:	Ericsson_4d:e9:…	ARP	6
Ericsson_4d: CadmusCo_d8:80: ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.1	CadmusCo_d8:	Ericsson_4d:e9:…	ARP	6
10.27.99.174       5.211.14.4       TCP	Ericsson_4d:	CadmusCo_d8:80:	ARP	6
10.27.99.174       5.211.14.4       TCP	10.27.99.174	5.211.14.4	тср	8
10.27.99.174       5.211.14.4       TCP	10.27.99.174	5.211.14.4	TCP	8
10.27.99.174       5.211.14.4       TCP	5 10.27.99.174	5.211.14.4	тср	8
10.27.99.174       5.211.14.4       TCP	10.27.99.174	5.211.14.4	тср	8
10.27.99.174       5.211.14.4       TCP	10.27.99.174	5.211.14.4	тср	8
10.27.99.174       5.211.14.4       TCP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4	10.27.99.174	5.211.14.4	TCP	8
10.27.99.174       5.211.14.4       TCP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4	10.27.99.174	5.211.14.4	TCP	8
10.27.99.174       5.211.14.4       TCP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4	5 10.27.99.174	5.211.14.4	тср	8
10.27.99.174       5.211.14.4       TCP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4	10.27.99.174	5.211.14.4	тср	8
10.27.99.174       5.211.14.4       TCP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4<	10.27.99.174	5.211.14.4	TCP	8
10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4       TCP         Ericsson_4d:       CadmusCo_d8:80:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4<	10.27.99.174	5.211.14.4	тср	8
10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4       TCP         Ericsson_4d:       CadmusCo_d8:80:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174       5.211.14.4	10.27.99.174	5.211.14.4	тср	8
10.27.99.174       5.211.14.4       TCP         Ericsson_4d:       CadmusCo_d8:80:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP         10.27.99.174	5 10.27.99.174	5.211.14.4	тср	8
Ericsson_4d: CadmusCo_d8:80: ARP         CadmusCo_d8: Ericsson_4d:e9: ARP         CadmusCo_d8: Ericsson_4d:e9: ARP         CadmusCo_d8: Ericsson_4d:e9: ARP         10.27.99.174       5.211.14.4         TCP         10.27.99.174       5.211.14.4	10.27.99.174	5.211.14.4	TCP	8
CadmusCo_d8:       Ericsson_4d:e9:       ARP         CadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP	Ericsson_4d:…	CadmusCo_d8:80:	ARP	6
CadmusCo_d8:       Ericsson_4d:e9:       ARP         10.27.99.174       5.211.14.4       TCP	GadmusCo_d8:	Ericsson_4d:e9:	ARP	6
10.27.99.174       5.211.14.4       TCP	GadmusCo_d8:	Ericsson_4d:e9:…	ARP	6
10.27.99.174       5.211.14.4       TCP	10.27.99.174	5.211.14.4	тср	8
10.27.99.174       5.211.14.4       TCP	5 10.27.99.174	5.211.14.4	тср	8
10.27.99.174       5.211.14.4       TCP	10.27.99.174	5.211.14.4	тср	8
10.27.99.174       5.211.14.4       TCP	10.27.99.174	5.211.14.4	TCP	8
i0.27.99.174       5.211.14.4       TCP         i0.27.99.174       5.211.14.4       TCP         .10.27.99.174       5.211.14.4       TCP	10.27.99.174	5.211.14.4	тср	8
10.27.99.174       5.211.14.4       TCP	10.27.99.174	5.211.14.4	тср	8
10.27.99.174         5.211.14.4         TCP	10.27.99.174	5.211.14.4	TCP	8
) 10.27.99.174 5.211.14.4 TCP 5 10.27.99.174 5.211.14.4 TCP 7 10.27.99.174 5.211.14.4 TCP	. 10.27.99.174	5.211.14.4	TCP	8
0 10.27.99.174 5.211.14.4 TCP 10.27.99.174 5.211.14.4 TCP	10.27.99.174	5.211.14.4	TCP	8
10.27.99.174 5.211.14.4 TCP	10.27.99.174	5.211.14.4	TCP	8
	10.27.99.174	5.211.14.4	TCP	8

Adv CadmusCo d8,80.

VBD



ERNW	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
providing security.	Reason: 65529 resets
	21/tcn open ftp
	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)
	<pre>  ssh-dss AAAAB3NzaC1kc3MAAACBAKjBoRJD3xs/PDF7i8Zh6VVNlnykkT0aZ/0JoZM0Qb/2Zm1SruM5bYkwAczqstUWXygtgSTmP4 Dv5VHNkmR5Gb5Kle2e5GXNp4HACdAVjThkpBzK27ai+Pj+CXIHQxHcZIMgJyQDA29oCg5KFk9lbtdDkiocabW/KyuAQmxB0 mIVAAAAFQCPdjPIB+E7/0QKPKXG0pcRglibLQAAAIBLD689UE2fmlufS53dHWsgxm9SsGD4GgP4bnRfV+G494PNfimiVv0W oqAeDFtVqQLlxZHU2pJ275kgRyDHcp4fTaPssxZpljyVNiZkjLjDVeZb8D562E4PnG3BVFy2VcMrq4klb002wKwE5zQrLQfGf70 o1rv81+10dpZzU3N48wAAAIEAhj3FTj4i2s8vKEVXzUtdK081YHhyv0J077niYmJ+jG2I0tt4tJpuNfvdc19ab2wtrqerQ1R6KTA9 2lnhktEZvS2e4peeVho0htYoDIDQTybpw5v/LaX8c0/7vtcKJt70n+A0rZwCAd2ScQxNKpcyJAqNf9J+esFJXo9K0NWkpms=   1024 e8:c6:48:a5:f8:7b:ed:c3:6b:30:86:a6:42:c6:04:a6 (RSA)</pre>
	l_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAz4L21u3pCegfluL0+iz8te/XmrNhNSeCFf9SCwd8GYL7D1yktvdhn3kFPb+4gwM2B+sIn hs0TM6+bt7HfW7AU0cPTMy3kgLxv0KU9V+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:
Nmap Results	I_ Supported Methods: GET HEAD POST
	I_http-server-header: WEBS - USE web server
	I_MUP-UNUP-UNUP down and a second down a sec
	L xmlrnc-methods: ERROR: Scrint execution failed (use -d to debug)
	56834/tcp open unknown syn-ack ttl 64



#### Maintenance Terminals

- o 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







Install-Asymptotic is a registered instantant of Microsomer, Constraints

Notes



LMT Software Installation

... and Windows XP ...

🔄 My Documents		<u></u>	8 ×
🗄 🖳 Element Management Applicat	tions		×
		Choose Java Virtual Machine	•
<ul> <li>Free Agreement</li> <li>Choose Java Virtual Mac</li> <li>Choose Install Folder</li> <li>Choose Products</li> <li>Choose Shortcut Folder</li> <li>Pre-Installation Summary</li> <li>Installing</li> <li>Install Complete</li> </ul>	Please Choose a Java 1.5 Applications. Please read suitable Java VM versions C:\j2sdk1.4.2_04\jre\bin\java.e	5 VM for Use by the Installed 1 the Installation Guide for information on s. exe Ch <u>o</u> ose Another	
InstallAnywhere by Macrovision			
De: <u>C</u> ancel		Previous <u>N</u> ext	
🛃 Start 🛛 😰 🍠 🚽 🚾 C:\WIN	ID   🥌 2 Intern 🖌 🏠 M 🔊 💿	ly Docum 🛛 🥶 Element 🔄 💽 📆 🐝 1 🖅 🖉 🗔 드 🖅 💷 🐼 😨 Strg Recht	.9:56 ts

10.27.99.174 - PHLe0760889 - RBS Element Manager		
File View MO Alarm Tools Help		
🔅 🚸 Radio Network 👻 View Descriptions		
	Table MO Properties Description Views	
MO Tree	Attributes(687) Actions(3)	
NodeBFunction=1 Radio Network Configuration + EUxan/EdgConflutation=2300 = EUxan/EdgColorHitedme2300 + EUxan/EdgColorHitedme2300 + EUxan/EdgColorHitedme2300 + EUxan/EdgColorHitedme3300 + EUxan/EdgColorHitedme3300		
	i       diChannelBandwidth:       3000         j       diConfigurableFrequencyStart:       0         i       dPrequencyAllocationProportion:       100         i       dPrequencyAllocationProportion:       False       Image: Image	
Refresh Tree 200		Agen Refres

#### A REAL PROPERTY AND ADDRESS OF TAXABLE PARTY. -Introductory line data into ----1.1 Anton Control - Changed 2010-47-46 (122) \$2-1218 Ann Libbary in at-10-0011pp 1 . 75m RU UnCalue Specify Problem Accessive Text A Probable Cause Salahusk-OBP,507,903,530MoveMIM,08,Noren-IP(al700007/mageExem-L2gamen-L Martin OPACIES AND ADDRESS IN Tex-second period has great maint IN CF Separative part is named in Comparison. Calment . 2014-07-011 2007 ND A Subleventeite OK/InConstrative Must State Database State of State August Advance Industrial mout. to Westmand in and Lowestein's released 2007 ND X-Sphenost-Phi-DE/NO7100-Phis/2008 Assard/anerty. Expensive Sphenost-Reprint v. Reprint V. miles. No SPicelapetrie, and K, calculate G ruPortio 8 Dagnett ... 200-07-06 i ... marent. NOT placed in part 1, canademic reported 2011 YO 2 Lightwork PK 04/MCHLOHMAN MILING BRANCH Lightwork Close Chapter C Republic Report Palamet National Tainert . Incolution ind half. the DP using adding pert 1, can addres 1, called the of Tableton (1988) 1001 PD & Laboratoria (1987) and 1988 all Williams and Emerged Experiments of Sector (1987) and 1987 active Destructed STATISTY TRANSMIT Satisfyore-OPP 2001 PC A Satisfyore-PE dia Access 6-PE at 10081 Apropriate and a specific at a speci **Decontracted** Budney, Stirtini. Industry and Michigan And Annual A Interaction in the

Double Chi

**Designment** 

Discontented

Industry Production of Personship

Addationar-Oph Vich Mr. A Addational-Hig did Netwide-High Hullet, Name Science & Diggs and Control Space High ante-

halfstrond-child SOCT IN: A halfstrond-MC DB Receipt -Marthall, Nacadarani, Japanese, Linguese, Colling and Malache-

habiteseiselletti (KOT) (K. J. Jahlatseiselletti (B. Philetesiselletti (New York)), Bargertine, Neteriselletti (Bargertine), Bargertine, Neteriselletti (Bargertine), Bargertine), Bargertine, Bargertine, Bargertine), Bargertine, Barge

Tables of ARM NOT NO. A tables of AR REPORT ARM REPORT REPORT Apparents ( ) and a long the end of the second s

And it was to be addressed the same through A TALLY IN THE PROPERTY AND DESCRIPTION OF TAXABLE PROPERTY. NO. Ann. Talk the Natural Steel Int. Gam 198 it Contenent 243Plant2 # Ten Decenters Inter Diversion Lags. M. Property .: December .: Heart Ing (Hp) - threat multi-sumplement 101744 360 Autre(1) Event Tax Size of NO SERVER - Prillaik Caver - Sends Hubers - Additional Your of Children I Proceeding were allow 2011/27/06 10 (Pr. . . . . (UM/p16/27/2...) Cardigonalise in Co. . . Second and Cardia. . Other the CPIC rule. In Intelligible Providence Casts. Loss and a incomentary To spield DASK'S CARP (Rent) IN HARRANTERS 140 List'slaw. a more that -111 a maile and a 1440 - mone-etc.-1 unitative. · material A AND a Janet 1.400 Porsenty and attended to the second s - Abdatated Nationary evolution at the Christian and Christian and Carl Comparison of Carl Science and - Rocket-c -mailentet recodence-/amet-chine-3e-chines-chines (amit...) Set in Automation Appare C ROPED 100708-01 a benefitter-Eastern and Storten to the State of State of States and States. And ad 1.1 initian. MPHO-DATE\_F 1.1 2000 manute. C. C. COLOR California ------ Hatter A BARRIER 1000 W. Stationer Dett CONTRACT. a declare Provide and the second se 2.0000 standard days. "Man Aller in the Including a Strength Long Report. a Richard -C # Sidealed Widewided gave means + EasterCognitTyphi-1 a labored a lational-Panaphiswetter-I · Transmittanter Australia Including on Public V I Telefissen Parketel maintent | recome | redu Datast Net

Natifune 2040-80404 ancies

Comments . Interferent.

Training The Child I

Line Of Send root

tone of Send Last ...

Los P Spiel and

Viel STF UKgentik, .

Loss of Arrist Loss.

the OP chained in .

Loss O'Real part.

tion Print and

the OT plaquel in.

Low FSpatum.

Annual Property lies

of the local division of the local divisiono

town? Rend net.



#### 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

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

Address	Name	Comment	
10.27.99.174	RBS	oam	
			Rem
Address *	Name	Corr	ment



#### Well...

[hschmidt@hslaptop -]\$ ssh -oKexAlgorithms=+diffie-hellman-group1-shal 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. \$

> [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

Username: rbs / cellouser

Password: rbs



#### Webserver

- Running WEBS OSE web server
  - $\circ \quad \mathsf{EM} \ \mathsf{Download}$
  - XML Configuration
- Java JDK (1.1.6, 1.2.1, 1.3.1, 1.4.2, 1.5.0, 1.6.0)
- o Somehow, not very load resistant
   → Leading to a DoS of the whole machine





# Insights

"No magic behind"



#### What We've Seen so far

- $\circ~$  The device was obviously not wiped
- $\circ~$  No IPSEC on S1 interface
- Hardcoded & default credentials
  - $\circ$  rbs rbs
  - cellouser rbs
- o Telnet in use
- Unencrypted maintenance interface





#### Well...

- o RTOS OSE 5.5
  - Running on a Motorola MPC 85xx
  - Assisted by FPGA + ARM
- o GZIP Volumes and Files
  - $_{\odot}$   $\,$  Starting with 1F 8B  $\,$

 $\circ~$  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	Bearbeit	en	An	sicht	Su	cher	ŧ. (	Term	inal	Hi	lfe						
024200	00 1F	88	68	68	8A	D9	31	4E	02	03	68	74	74	70	5F	73	1Nhttp s
02420C	10 65	72	76	65	72	2E	70	70	63	2E	65	6C	66	2E	73	74	erver.ppc.elf.st
02420C	20 72	69	70	2E	70	60	2E	63	бF	6E	66	00	EC	DA	79	70	rip.pl.confyp
02420C	30 97	E5	85	07	FØ	BC	AÐ	4C	A5	62	45	2B	73	5D	AA	88	L.bE+s]
02420C	40 2D	52	88	21	09	24	21	81	28	01	03	06	B2	BØ	84	AO	-R.1.\$!.(
02420C	50 B4	1A	86	BØ	24	F9	25	21	18	01	D9	A4	41	20	20	20	\$.%!A
02420C	60 22	28	65	B5	EC	14	50	5C	61	20	58	2C	AB	C8	56	B4	"(eP\a,X,V.
02420C	70 CA	AD	1B	5A	68	3B	53	3B	D7	7B	EB	D8	4D	EF	2F	BC	Zk;S;.{M./.
02420C	80 9F	20	F4	DA	4E	EF	FF	66	26	90	BC	BF	F7	79	CE	73	Nf&y.s
02420C	90 96	EF	F9	9E	F3	FC	74	7A	66	76	9F	A0	59	10	73	FE	tzfvY.s.
02420C	A0 A7	59	CC	B7	A3	FF	06	57	86	4F	50	A3	BF	CF	F8	AB	.YW.0]
02420C	B0 6D	CC	25	31	1D	62	AE	8E	69	7C	15	DD	70	49	87	73	m.%1.bi pI.s
02420C	C0 7F	9D	5B	F8	0D	BF	D1	15	E1	6F	<b>B3</b>	98	98	CB	3B	7C	[0;]
02420CI	D0 A9	B4	D7	5D	FE	68	7A	1F	DD	9F	5B	71	7E	7B	F3	EF	].hz[q~{
02420CI	E0 2E	3A	F7	18	13	73	69	4C	68	4A	10	D3	BC	ZA	66	78	.:siLhJ*fx
024200	F0 F4	8F	E1	A1	51	03	62	62	EE	6E	D4	D1	22	FA	DB	36	Q.bb.n"6
02420D	00 E6	DF	FF	69	18	9E	15	D3	22	F4	27	B7	22	A6	D9	FE	i".'."
02420D	10 8A	7F	78	DF	F8	73	FD	45	BB	9A	D7	θC	FØ	57	6B	FB	xs.EWk.
02420D	20 1B	6D	BE	3C	FA	DB	C9	73	<b>B</b> 3	2B	18	F5	34	BF	FA	DD	.m.<5.+4
02420D	30 98	98	C2	0B	ED	F9	06	D9	FE	5F	E8	68	7E	81	BE	2E	
02420D	40 E7	F5	9D	8B	C1	F9	75	31	17	C4	AB	F1	A7	BB	75	C1	u1u.
02420D	50 F0	8B	F5	35	FD	34	25	80	D7	BF	B9	2E	B7	E9	DC	70	5.4%p
02420D	60 5D	55	E3	BF	03	BE	E2	DC	AC	7F	E1	C7	37	2E	FØ	E3	]U
CI	ompactd	isk	fl	ippe	d.in	na		1.1	-0x	242	0D6	F/0>	(7D1)	300	- 00		



	\$ rld
	nu Displaying ramlog virtual range 0x0 - 0x3af7
EKINVV	RAMIOG SESSION START
providing security.	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.
Ramlog	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...?

#### $\circ$ Looks like a BaseStation from the US $\odot$

c/logfiles/alarm\_event/ALARM\_LOG.xml:1f1;x4;x4;EUtranCellFDD;SubNetwork=ONRM\_ROOT\_MO\_R,Sub Network=PHL-ENB,MeContext=PHLe0760889,ManagedElement=1,ENodeBFunction=1,EUtranCellFDD=PHLe07608893;4 17;135588376835330000;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;



## Using passwd

- $\circ~$  We have the users cellouser and rbs
  - $\circ$   $\;$  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-group1sha1 rbs@10.27.99.174





#### Cell & UE Traces

- The eNodeB is able to create both traces for cells and UEs
- $\circ$   $\,$  We found a set of traces on the device
- Sadly the traces seem to be purely cell traces
  - Containing data on packet loss etc.
  - o No "interesting" information

S cat CellTraceFilesLocation cat CellTraceFilesLocation /c/pn data S cat UeTraceFilesLocation cat UeTraceFilesLocation /c/pm\_data \$ 15 ls Directory '/j/pm\_data/' A20160706.0930-0945:1.xml.gz A20160706.0945-1000:1.xml.gz A20160706.1008-1015:1.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 A28160706.1288-1215:1.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.oz A20150413.0545-0600:1.xml.gz A28158413.8688-8615:1.xml.gz A20150413.0615-0630:1.xml.gz A20150413.0630-0645:1.xml.oz A20150413.0645-0700:1.xml.gz A20150413.0700-0715:1.xml.gz A20150413.0715-0730:1.xml.oz 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 A20150413.1008-1015:1.xml.gz A20150413.1015-1030:1.xml.gz A20150413.1030-1045:1.xml.gz A20150413.1045-1100:1.xml.gz A20150413.1108-1115:1.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 A20150413.1238-1245:1.xml.gz



#### **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
```

59         10.27.99.174         5.211.14.4           13         10.27.99.174         5.211.14.4           14         10.27.99.174         5.211.14.4           12         10.27.99.174         5.211.14.4           16         10.27.99.174         5.211.14.4           16         10.27.99.174         5.211.14.4           11         10.27.99.174         5.211.14.4           11         10.27.99.174         5.211.14.4           11         10.27.99.174         5.211.14.4           12         10.27.99.174         5.211.14.4	TCP TCP TCP	82 TCP Rei 82 TCP Rei	tra tra
1310.27.99.174         5.211.14.4           1410.27.99.174         5.211.14.4           1210.27.99.174         5.211.14.4           1610.27.99.174         5.211.14.4           1110.27.99.174         5.211.14.4           1110.27.99.174         5.211.14.4           1110.27.99.174         5.211.14.4           1110.27.99.174         5.211.14.4	TCP	82 TCP Rei	tra
14         10.27.99.174         5.211.14.4           12         10.27.99.174         5.211.14.4           36         10.27.99.174         5.211.14.4           11         10.27.99.174         5.211.14.4           10         10.27.99.174         5.211.14.4           10         10.27.99.174         5.211.14.4           10         10.27.99.174         5.211.14.4	TCP		
42. 10.27.99.174 5.211.14.4 36. 10.27.99.174 5.211.14.4 51. 10.27.99.174 5.211.14.4 10.10.27.99.174 5.211.14.4 10.10.27.99.174 5.211.14.4	77010	82 65467-50	907
36. 10.27.99.174 5.211.14.4 1 10.27.99.174 5.211.14.4 10 10.27.99.174 5.211.14.4	TCP	82 [TCP Rel	tra
51. 10.27.99.174 5.211.14.4 0. 10.27.99.174 5.211.14.4	TCP	82 TCP Ret	tra
0 10.27.99.174 5.211.14.4	TCP	82 TCP Rei	tra
	TCP	82 65466→50	007
0, 10.27.99.174 5.211.14.4	TCP	82 [TCP Rei	tra
7. 10.27.99.174 5.211.14.4	TCP	82 TCP Ret	tra
4. 10.27.99.174 5.211.14.4	TCP	82 TCP Ret	tra
30 10.27.99.174 5.211.14.4	TCP	82 65465-50	907
4. 10.27.99.174 5.211.14.4	TCP	82 [TCP Rei	tra
98. 10.27.99.174 5.211.14.4	TCP	82 [TCP Ret	tra
7 10 27 99 174 5 211 14 4	TCP	82 [TCP Rei	tra
2 10.27.99.174 5.211.14.4	TCP	82 65464-50	907
10.27.99.174 5.211.14.4	TCP	82 [TCP Rei	tra
15. 10.27.99.174 5.211.14.4	TCP	82 [TCP Ret	tra
14. 10.27.99.174 5.211.14.4	TCP	82 [TCP Rei	tra
03. 10.27.99.174 5.211.14.4	TCP	82 65463-50	907
1. 10.27.99.174 5.211.14.4	TCP	82 [TCP Rei	tra
2. 10.27.99.174 5.211.14.4	TCP	82 [TCP Ret	tra
3. 10.27.99.174 5.211.14.4	TCP	82 [TCP Rei	tra
1 10.27.99.174 5.211.14.4	TCP	82 65462-50	907
4. 10.27.99.174 5.211.14.4	TCP	82 [TCP Re	tra
2 10 27 99 174 5 211 14 4	1 GP	82 [TCP Ret	tra
1. 10.27.99.174 5.211.14.4	ICP	82 [ICP Ret	tra
3. 10.27.99.174 5.211.14.4	TCP	82 65461-50	961
	TOP	82 TOP Rel	tra
7 40 27 00 474 5 244 44 4	TCP	82 [TCP Rel	LI a
	TOP	OZ TUP REI	LI d
13. 10.27.99.174 0.211.14.4	TCP	82 00400→00 70 50070 60	SOI EAC
3. 5.211.14.4 10.27.99.174	TUP	78 50073-0	340
32 10 27 00 174 5 211 14 4	TCP	70 65460 5	
1210.27.00.474 5.211.14.4	CTOD	205 CT00 1	100
10.27, 99.174 $3.211.14.4$	TCD	70 50072 6	546
	TCP	70 5007540.	040 0 A
0. 0.211.14.4 10.27.99.174	I GP		D A



#### 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

N This is the RIPE Database query service. W 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@Mcl.ir' 5-211.0.0 - 5.211.255.255 inetnum: netnane: **GPRS** LTE descri country: 18 admin-cl 东1.7844·秋1PE tech-C: RL7844-RIPE statust ASSIGNED PA nnt-by; MCCI-MNT created: 2015-82-18T18158:50Z Last-Modified: 2015-02-18710:58:507 source: 8195 person: Reza Taham Latiberi address: Hanzah Tower - Kordestan High way cross Vanak st.Tehran Iran +98 21 88640934 phone: nic hdl: #17844-#1PE NCCI-MNT ntit-by: created: 2012-09-05711:41:382 last-modified: 2012-09-05713:41:392 RIPE # Filtered source: % Information related to '5.211.0.0/16A5197207' route: 5.211.0.0/10

route: 9.41.0.8/00 descr: New services for 4G origin: AS197207 ant.by: NCCI-NN1 created: 2015-02-18711149:182 last-nodified: 2015-82-18711149:182 Source: E2015

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





#### IP Address: 5.211.14.4

o 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



o 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!





hschmidt@ernw.de bbutterly@ernw.de

@hendrks\_

@BadgeWizard

www.ernw.de





