P1 SECURITY

LTE Pwnage: Hacking HLR/HSS and MME Core Network Elements

HITB

HITB Security Conference - Sept.2013

Contact:

Philippe Langlois
contact@p1sec.com

Table of contents

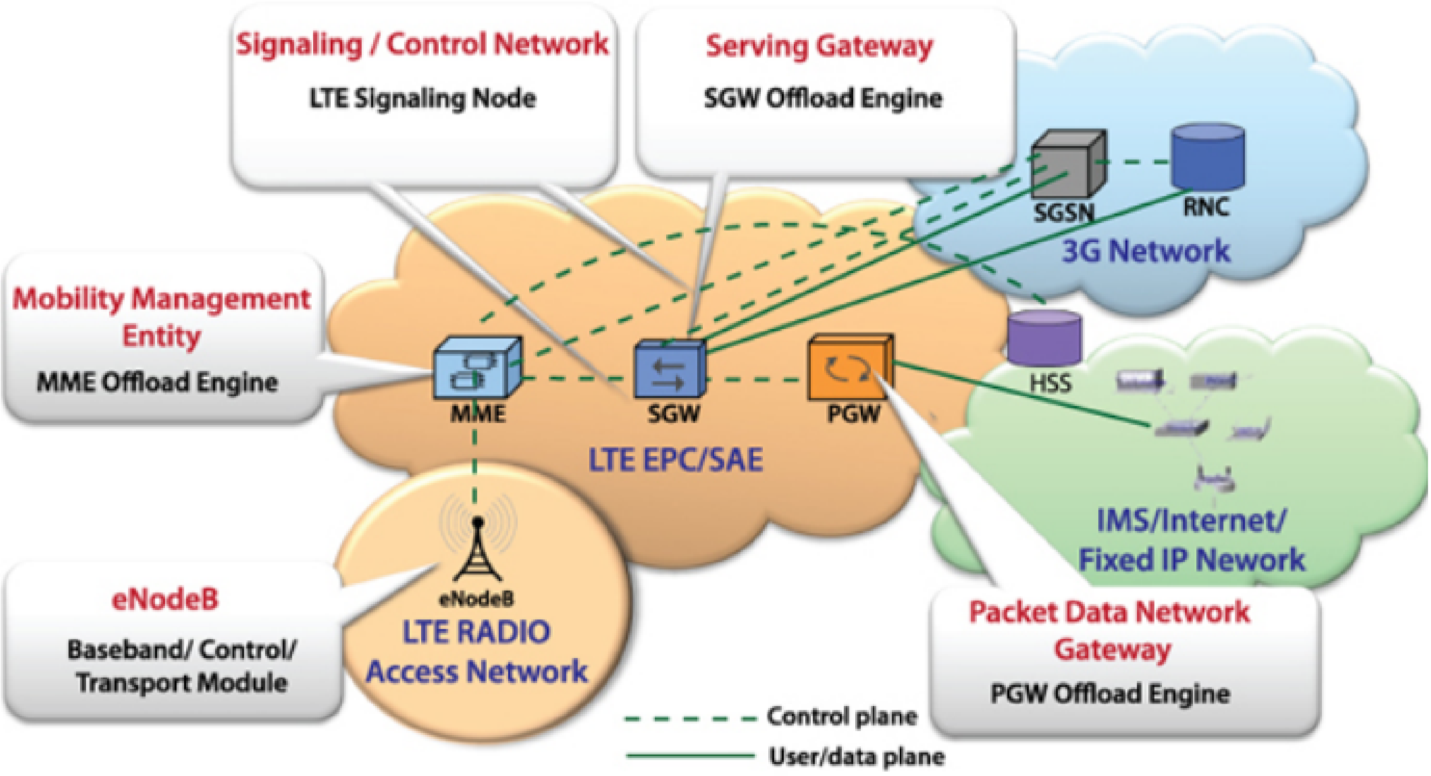
Executive summary

Welcome to the LTE Pwnage PDF file! This document is a comprehensive guide to the risks and vulnerabilities of LTE (Long-Term Evolution) networks, which are widely used for mobile communication and data transfer. As the use of LTE networks continues to grow, so does the risk of cyber attacks that can compromise sensitive corporate and personal data. This document aims to provide an in-depth analysis of the various attack methods used by hackers to exploit LTE networks and offers practical solutions to mitigate these risks.

The document is divided into several sections, starting with an overview of the LTE environment and the increased risk of corporate and mobile data breaches. It then delves into the LTE network attack surface, exploring the different types of attacks that can be launched against LTE networks, including spear-phishing, botnets and malware, flooding, and Trojan and backdoors. The document also examines the impact of IPv6 on the security of LTE networks and the intricate and new protocols used in LTE networks, such as Diameter, S1, X2, and GTP. Finally, the document offers practical solutions to mitigate the risks of LTE network attacks, including network segmentation, intrusion detection and prevention systems, and security monitoring.

1. LTE Environment

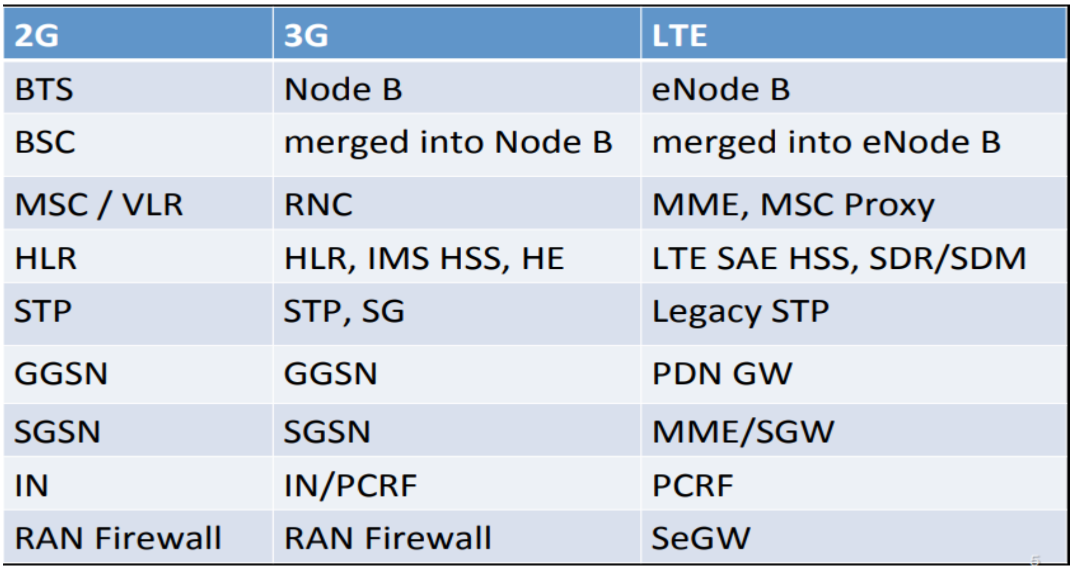
LTE Overview



1.1 Corporate and Mobile Data risk has increased

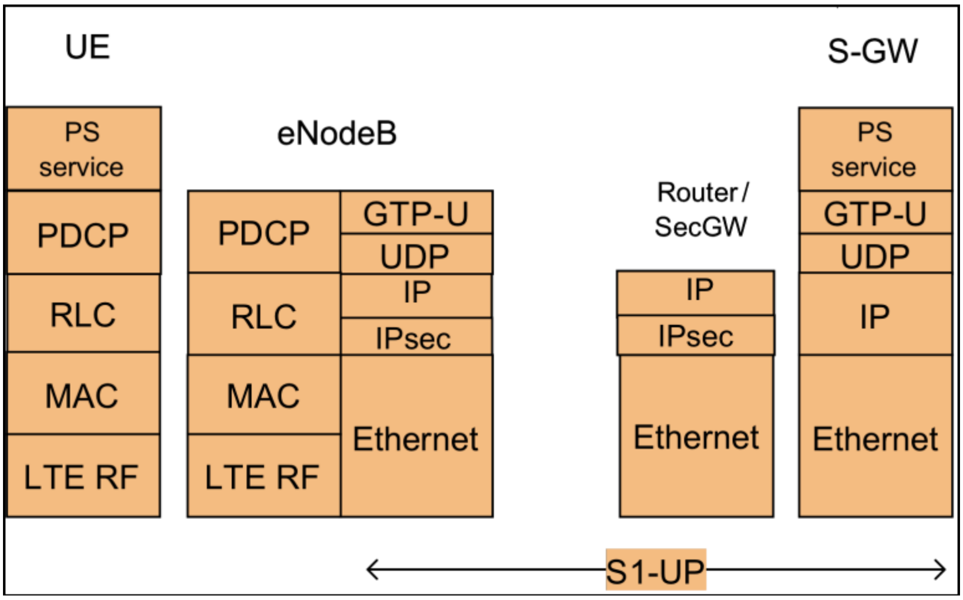
- LTE from attackers' perspective
- All IP are always on, thus always vulnerable?
  - Spear-phising
  - Botnets & Malware
  - Flooding
  - Trojan & Backdoors
- IPv6 renders NAT protection inefficient
- Split Handshake TCP attacks prevents IPS and Antivirus
- Very similar architecture for attackers: ATCA, Linux
- Intricate and new protocols: Diameter, S1, X2, GTP

2G, 3G and LTE: Reality and Legacy



2G	3G	LTE
BTS	Node B	eNode B
BSC	merged into Node B	merged into eNode B
MSC / VLR	RNC	MME, MSC Proxy
HLR	HLR, IMS HSS, HE	LTE SAE HSS, SDR/SDM
STP	STP, SG	Legacy STP
GGSN	GGSN	PDN GW
SGSN	SGSN	MME/SGW
IN	IN/PCRF	PCRF
RAN Firewall	RAN Firewall	SeGW

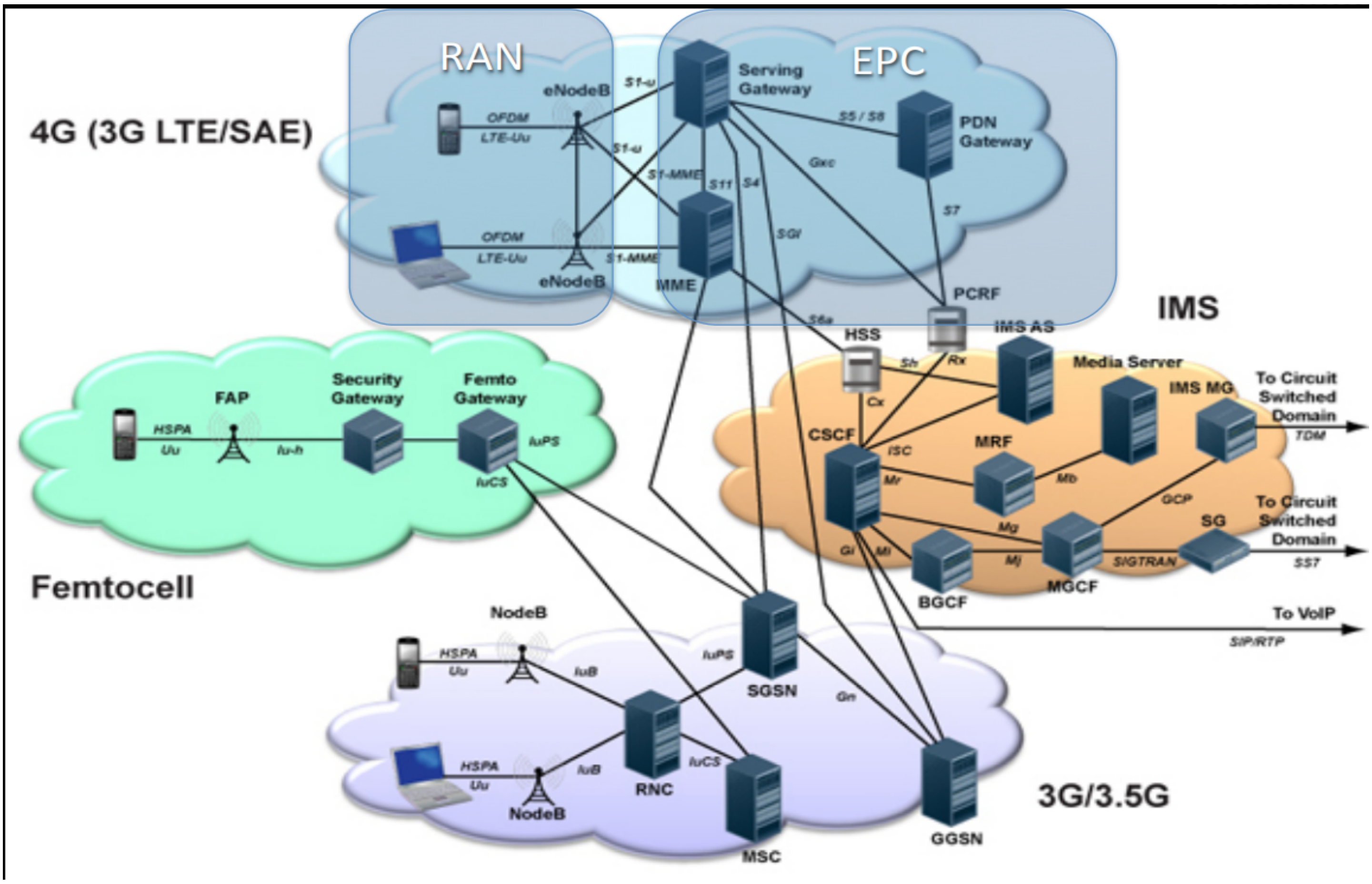
User data content: LTE User Plane



2. LTE Network Attack Surface

- Full IP only
  - No: full IP double exposure
- Packets (PS Domain)
  - 2x attack surface
    - GTP still present
    - S1AP/X2AP new
- Circuits (CS Domain)
  - 2x attack surface
    - SIGTRAN & SS7 will stay for many years
    - IMS & Diameter

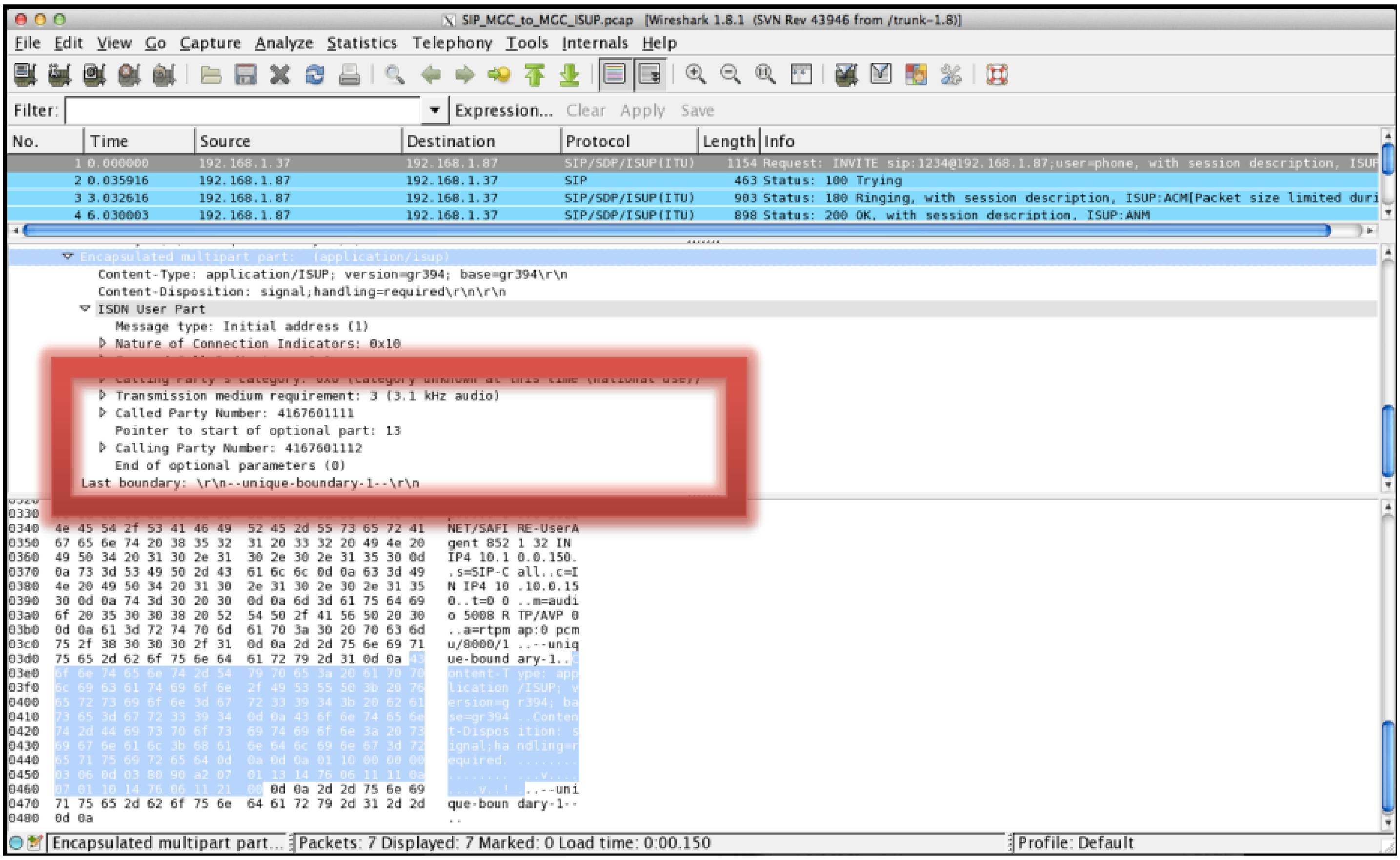
3G and LTE together



2.1 CSFB vs. VOLTE vulnerability attack surface

- CSFB
  - CS Fall Back from 4G to 3G
  - Past is present
  - SS7 and SIGTRAN stack vulnerabilities (DoS, spoof,...)
- VOLTE
  - Whole new attack surface
  - New APN, new network to hack, new servers
  - Closer to the Core Network == more serious vulnerabilities
  - IMS (CSCF = SIP servers, DNS,...)
    - Standard? No...

ISUP injection in SIP through VOLTE


SIP_MGC_to_MGC_ISUP.pcap [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time        Source          Destination     Protocol            Length Info
    1 0.000000    192.168.1.37    192.168.1.87    SIP/SDP/ISUP(ITU)     1154 Request: INVITE sip:1234@192.168.1.87;user=phone, with session description, ISUP
    2 0.035916    192.168.1.87    192.168.1.37    SIP                    463 Status: 100 Trying
    3 3.032616    192.168.1.87    192.168.1.37    SIP/SDP/ISUP(ITU)      903 Status: 180 Ringing, with session description, ISUP:ACM[Packet size limited duri
    4 6.030003    192.168.1.87    192.168.1.37    SIP/SDP/ISUP(ITU)      898 Status: 200 OK, with session description, ISUP:ANM
```

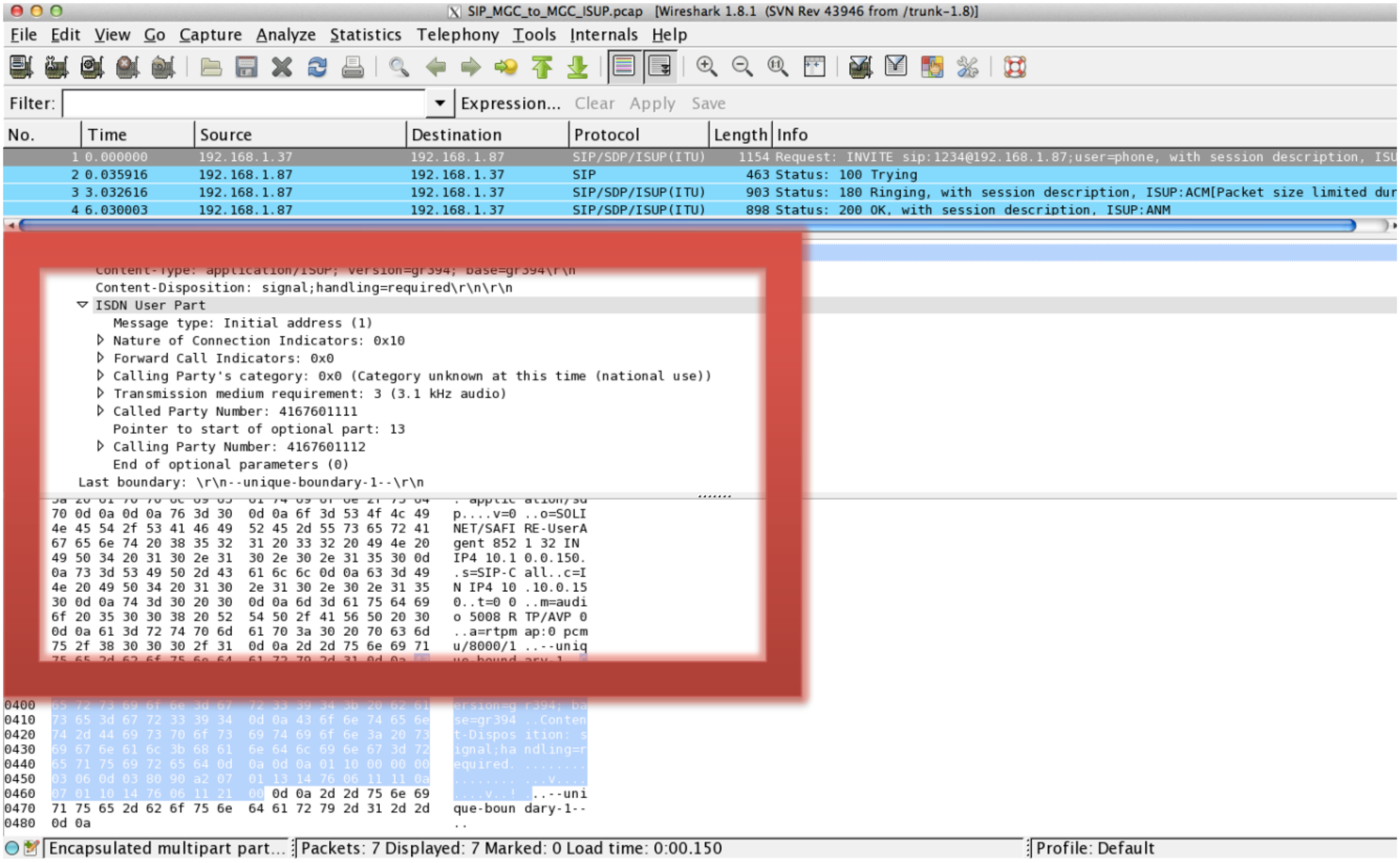
```
  ▽ Encapsulated multipart part:  (application/isup)
      Content-Type: application/ISUP; version=gr394; base=gr394\r\n
      Content-Disposition: signal;handling=required\r\n\r\n
    ▽ ISDN User Part
        Message type: Initial address (1)
      ▷ Nature of Connection Indicators: 0x10
      ▷ Calling Party's category: 0x0 (category unknown at this time (national use))
      ▷ Transmission medium requirement: 3 (3.1 kHz audio)
      ▷ Called Party Number: 4167601111
        Pointer to start of optional part: 13
      ▷ Calling Party Number: 4167601112
        End of optional parameters (0)
    Last boundary: \r\n--unique-boundary-1--\r\n
```

```
0330
0340  4e 45 54 2f 53 41 46 49  52 45 2d 55 73 65 72 41   NET/SAFI RE-UserA
0350  67 65 6e 74 20 38 35 32  31 20 33 32 20 49 4e 20   gent 852 1 32 IN 
0360  49 50 34 20 31 30 2e 31  30 2e 30 2e 31 35 30 0d   IP4 10.1 0.0.150.
0370  0a 73 3d 53 49 50 2d 43  61 6c 6c 0d 0a 63 3d 49   .s=SIP-C all..c=I
0380  4e 20 49 50 34 20 31 30  2e 31 30 2e 30 2e 31 35   N IP4 10 .10.0.15
0390  30 0d 0a 74 3d 30 20 30  0d 0a 6d 3d 61 75 64 69   0..t=0 0 ..m=audi
03a0  6f 20 35 30 30 38 20 52  54 50 2f 41 56 50 20 30   o 5008 R TP/AVP 0
03b0  0d 0a 61 3d 72 74 70 6d  61 70 3a 30 20 70 63 6d   ..a=rtpm ap:0 pcm
03c0  75 2f 38 30 30 30 2f 31  0d 0a 2d 2d 75 6e 69 71   u/8000/1 ..--uniq
03d0  75 65 2d 62 6f 75 6e 64  61 72 79 2d 31 0d 0a 43   ue-bound ary-1..C
03e0  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 61 70 70   ontent-T ype: app
03f0  6c 69 63 61 74 69 6f 6e  2f 49 53 55 50 3b 20 76   lication /ISUP; v
0400  65 72 73 69 6f 6e 3d 67  72 33 39 34 3b 20 62 61   ersion=g r394; ba
0410  73 65 3d 67 72 33 39 34  0d 0a 43 6f 6e 74 65 6e   se=gr394 ..Conten
0420  74 2d 44 69 73 70 6f 73  69 74 69 6f 6e 3a 20 73   t-Dispos ition: s
0430  69 67 6e 61 6c 3b 68 61  6e 64 6c 69 6e 67 3d 72   ignal;ha ndling=r
0440  65 71 75 69 72 65 64 0d  0a 0d 0a 01 10 00 00 00   equired. ........
0450  03 06 0d 03 80 90 a2 07  01 13 14 76 06 11 11 0a   ........ ...v....
0460  07 01 10 14 76 06 11 21  00 0d 0a 2d 2d 75 6e 69   ....v..! ...--uni
0470  71 75 65 2d 62 6f 75 6e  64 61 72 79 2d 31 2d 2d   que-boun dary-1--
0480  0d 0a                                              ..
```

```
Encapsulated multipart part... Packets: 7 Displayed: 7 Marked: 0 Load time: 0:00.150    Profile: Default
```

Even though SIP is known...Internet SIP + SS7 ISUP == SIP-I and SIP-T == ISUP Injection !

- Remote Core Network DoS
- SS7 compromise
- External signalling injection
- Spoofing of ISUP messages
- Fake billing



SIP_MGC_to_MGC_ISUP.pcap [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time       Source         Destination    Protocol            Length Info
    1 0.000000   192.168.1.37   192.168.1.87   SIP/SDP/ISUP(ITU)     1154 Request: INVITE sip:1234@192.168.1.87;user=phone, with session description, ISU
    2 0.035916   192.168.1.87   192.168.1.37   SIP                    463 Status: 100 Trying
    3 3.032616   192.168.1.87   192.168.1.37   SIP/SDP/ISUP(ITU)      903 Status: 180 Ringing, with session description, ISUP:ACM[Packet size limited dur
    4 6.030003   192.168.1.87   192.168.1.37   SIP/SDP/ISUP(ITU)      898 Status: 200 OK, with session description, ISUP:ANM
```

```
    Content-Type: application/ISUP; version=gr394; base=gr394\r\n
    Content-Disposition: signal;handling=required\r\n\r\n
  ▽ ISDN User Part
      Message type: Initial address (1)
    ▷ Nature of Connection Indicators: 0x10
    ▷ Forward Call Indicators: 0x0
    ▷ Calling Party's category: 0x0 (Category unknown at this time (national use))
    ▷ Transmission medium requirement: 3 (3.1 kHz audio)
    ▷ Called Party Number: 4167601111
      Pointer to start of optional part: 13
    ▷ Calling Party Number: 4167601112
      End of optional parameters (0)
  Last boundary: \r\n--unique-boundary-1--\r\n
```

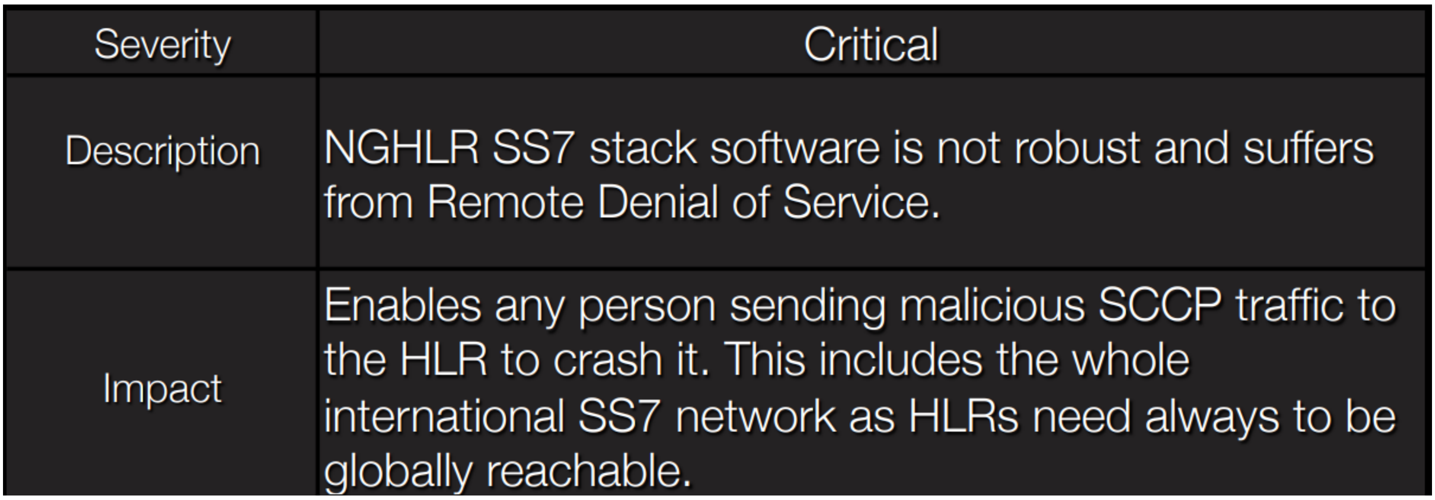
```
     3a 20 61 70 70 6c 69 63  61 74 69 6f 6e 2f 73 64   : applic ation/sd
     70 0d 0a 0d 0a 76 3d 30  0d 0a 6f 3d 53 4f 4c 49   p....v=0 ..o=SOLI
     4e 45 54 2f 53 41 46 49  52 45 2d 55 73 65 72 41   NET/SAFI RE-UserA
     67 65 6e 74 20 38 35 32  31 20 33 32 20 49 4e 20   gent 852 1 32 IN 
     49 50 34 20 31 30 2e 31  30 2e 30 2e 31 35 30 0d   IP4 10.1 0.0.150.
     0a 73 3d 53 49 50 2d 43  61 6c 6c 0d 0a 63 3d 49   .s=SIP-C all..c=I
     4e 20 49 50 34 20 31 30  2e 31 30 2e 30 2e 31 35   N IP4 10 .10.0.15
     30 0d 0a 74 3d 30 20 30  0d 0a 6d 3d 61 75 64 69   0..t=0 0 ..m=audi
     6f 20 35 30 30 38 20 52  54 50 2f 41 56 50 20 30   o 5008 R TP/AVP 0
     0d 0a 61 3d 72 74 70 6d  61 70 3a 30 20 70 63 6d   ..a=rtpm ap:0 pcm
     75 2f 38 30 30 30 2f 31  0d 0a 2d 2d 75 6e 69 71   u/8000/1 ..--uniq
     75 65 2d 62 6f 75 6e 64  61 72 79 2d 31 0d 0a 43   ue-bound ary-1..C
0400 65 72 73 69 6f 6e 3d 67  72 33 39 34 3b 20 62 61   ersion=g r394; ba
0410 73 65 3d 67 72 33 39 34  0d 0a 43 6f 6e 74 65 6e   se=gr394 ..Conten
0420 74 2d 44 69 73 70 6f 73  69 74 69 6f 6e 3a 20 73   t-Dispos ition: s
0430 69 67 6e 61 6c 3b 68 61  6e 64 6c 69 6e 67 3d 72   ignal;ha ndling=r
0440 65 71 75 69 72 65 64 0d  0a 0d 0a 01 10 00 00 00   equired. ........
0450 03 06 0d 03 80 90 a2 07  01 13 14 76 06 11 11 0a   ........ ...v....
0460 07 01 10 14 76 06 11 21  00 0d 0a 2d 2d 75 6e 69   ....v..! ...--uni
0470 71 75 65 2d 62 6f 75 6e  64 61 72 79 2d 31 2d 2d   que-boun dary-1--
0480 0d 0a                                              ..
```

Encapsulated multipart part... | Packets: 7 Displayed: 7 Marked: 0 Load time: 0:00.150 | Profile: Default

2.2 CSFB Attack surface through MSC Proxy and SS7 + SIGTRAN

- All SIGTRAN attack surface exposed
- All SS7 attack surface exposed
- Most dangerous:
    - Logical Denial of Service attacks
        - SSP-based SCCP DoS (P1 CVID#480)
        - TFP-based SS7 DoS (P1 CVID#481)
    - Equipment Crash/Denial of Service attacks
        - Ericsson MSC Crash DoS (P1 VID#330)
        - NSN HLR Crash DoS (P1 VID#148)
        - Ericsson STP Crash DoS (P1 VID#187)

3. NSN NGHLR remote Denial of Service caused by fragile SS7 stack

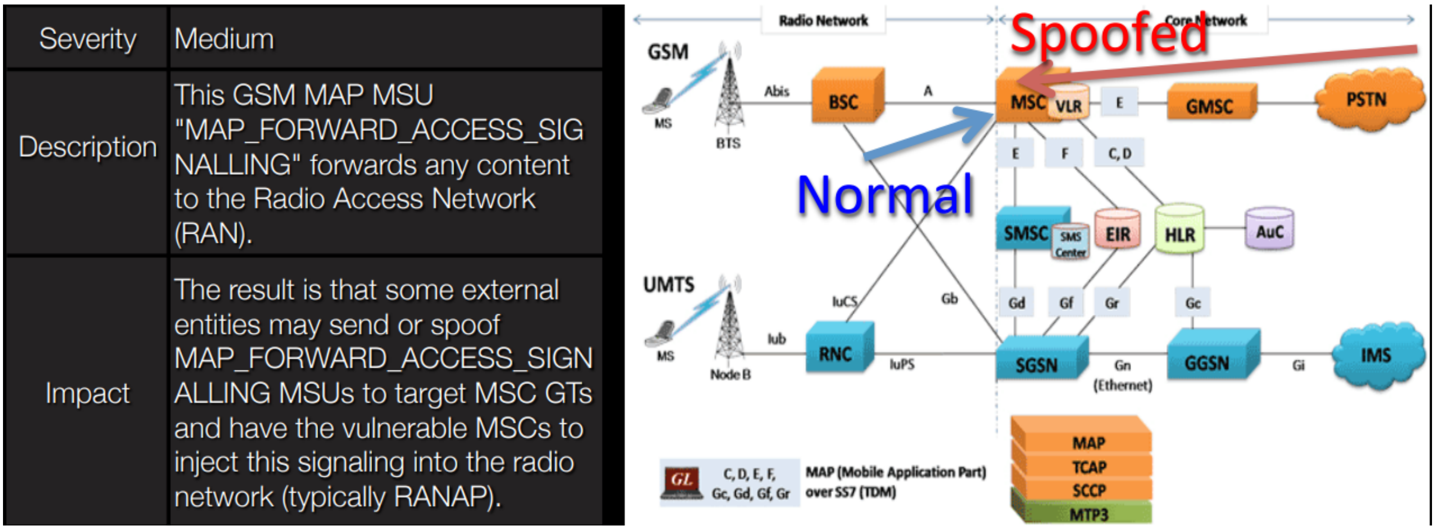


Severity	Critical
Description	NGHLR SS7 stack software is not robust and suffers from Remote Denial of Service.
Impact	Enables any person sending malicious SCCP traffic to the HLR to crash it. This includes the whole international SS7 network as HLRs need always to be globally reachable.

Reliability for telecom

- Ability to cope with X million of requests
- Inability to cope with malformed traffic

3.1 GSM MAP primitive MAP_FORWARD_ACCESS_SIGNALLING enables RAN signalling injection

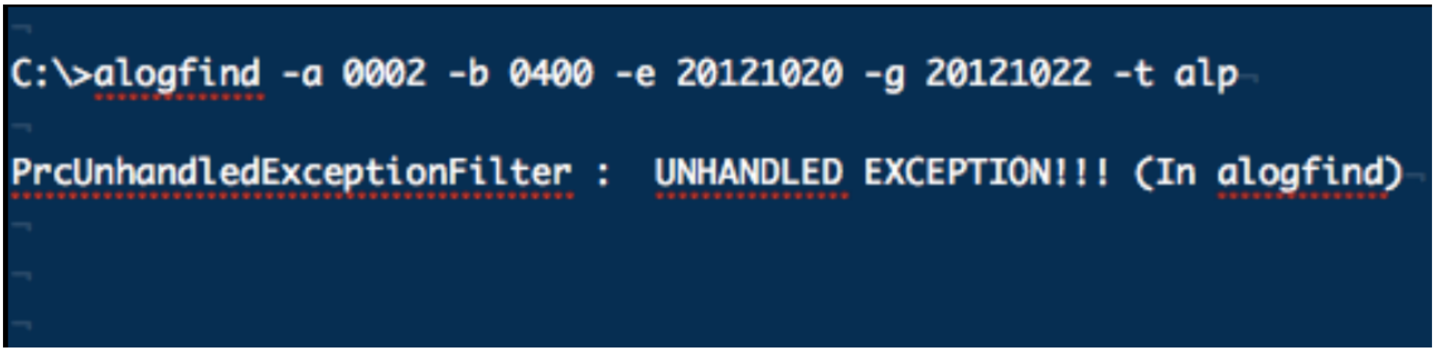


Severity	Medium
Description	This GSM MAP MSU "MAP_FORWARD_ACCESS_SIGNALLING" forwards any content to the Radio Access Network (RAN).
Impact	The result is that some external entities may send or spoof MAP_FORWARD_ACCESS_SIGNALLING MSUs to target MSC GTs and have the vulnerable MSCs to inject this signaling into the radio network (typically RANAP).

- Spoof and inject radio signalling
- As if it was coming from Radio Network

3.1.1 Fun Anti-forensics

- Same attack as VID#187
- Also crash Ericsson traffic monitoring log analysis forensic tools (P1 VKD VID#213)
- Code sharing between enforcement and forensic tools

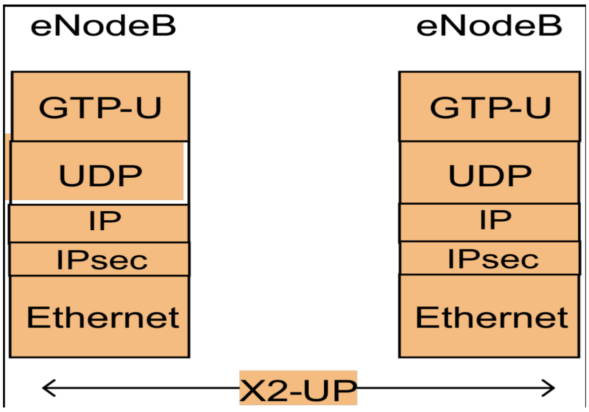


```
C:\>alogfind -a 0002 -b 0400 -e 20121020 -g 20121022 -t alp

PrcUnhandledExceptionFilter :  UNHANDLED EXCEPTION!!! (In alogfind)
```

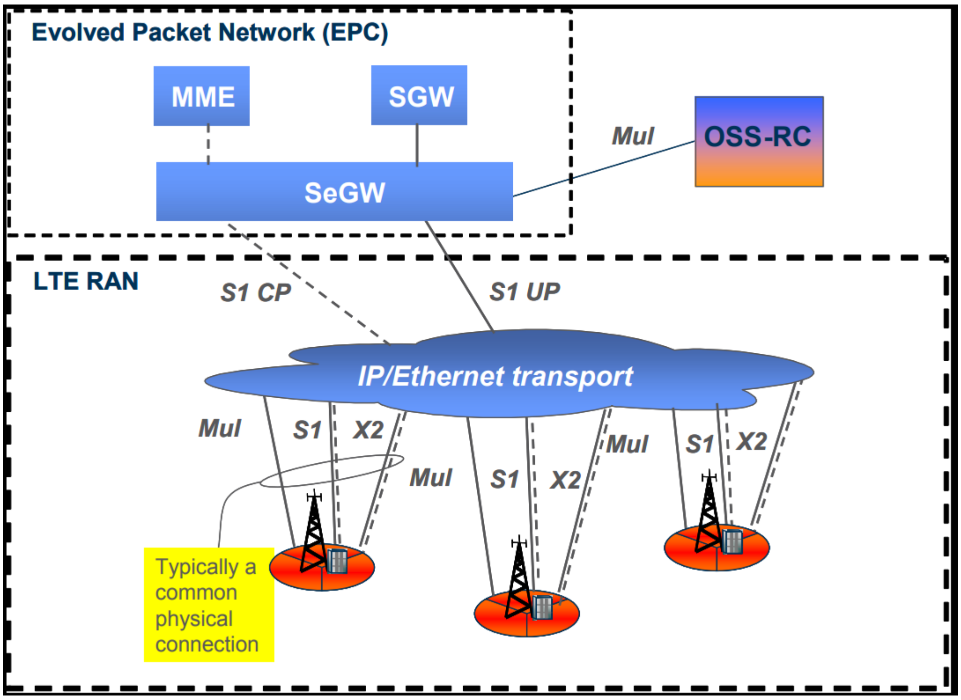
3.2 Peer to Peer Radio Access Network

- X2AP
    - eNodeB's
    - Peer to Peer
- Translation
    - Every base station can talk to every other
    - Network attack surface increase
    - Total spread into the RAN network
- Operator-wide L2 network
    - L2 attacks, less defence in depth, scanning only blocked by size of network
    - Did GTP disappear? No

User data between eNBs: LTE User Plane



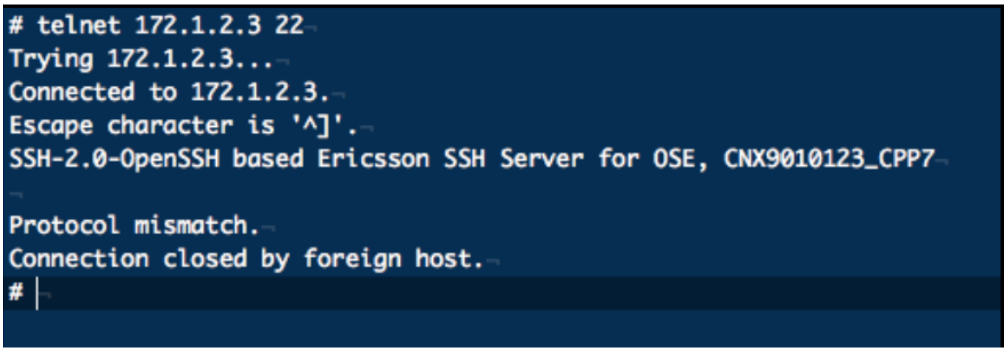
LTE RAN Overview



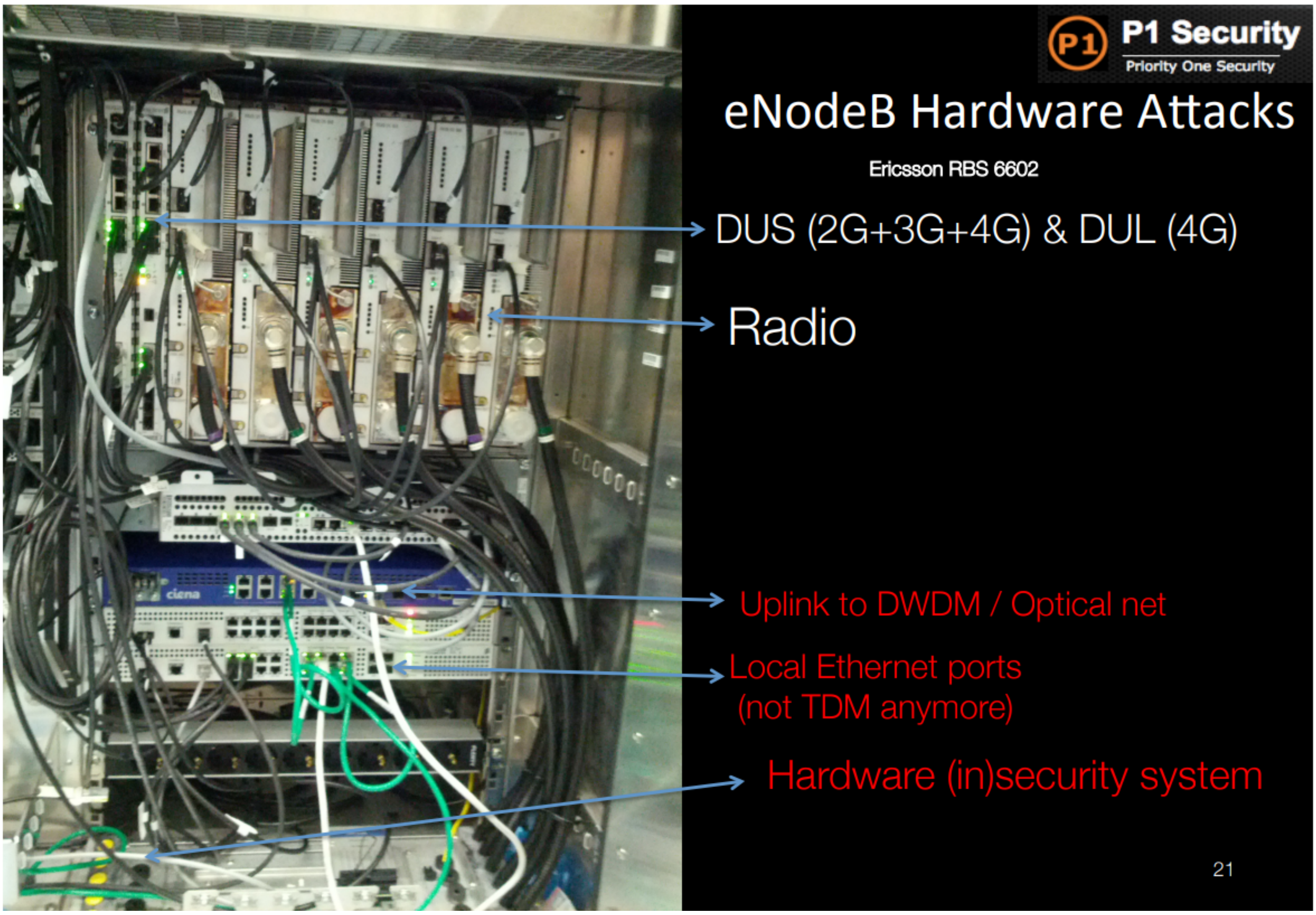
4. Pwning OSS

L2 network mistakes always happen

- Can’t catch it with multiple overlapping /8 networks: automate!
- From any eNodeB to the NMS
- From any eNodeB to any eNodeB
    - You can bet on insecure provisioning
- American example & Remote misconfiguration



```
# telnet 172.1.2.3 22
Trying 172.1.2.3...
Connected to 172.1.2.3.
Escape character is '^]'.
SSH-2.0-OpenSSH based Ericsson SSH Server for OSE, CNX9010123_CPP7

Protocol mismatch.
Connection closed by foreign host.
# |
```



P1 Security
Priority One Security

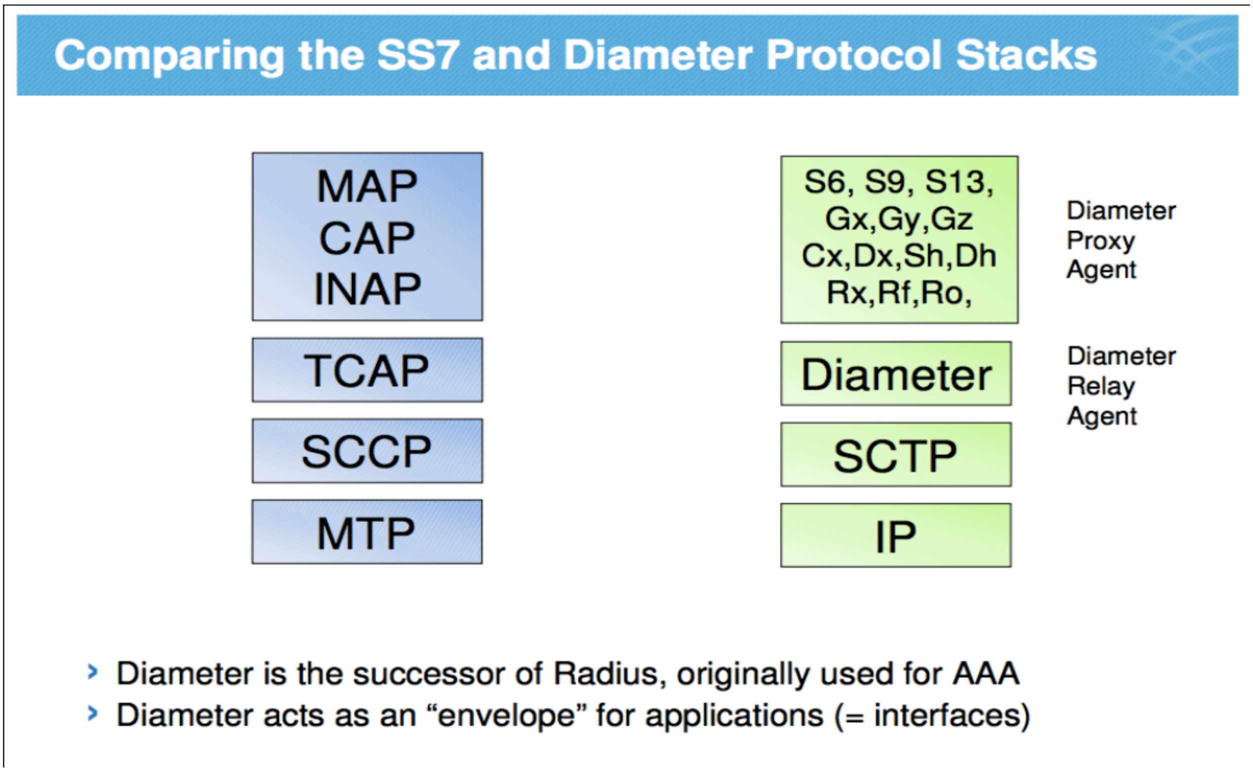
eNodeB Hardware Attacks

Ericsson RBS 6602

DUS (2G+3G+4G) & DUL (4G)
Radio
Uplink to DWDM / Optical net
Local Ethernet ports
(not TDM anymore)
Hardware (in)security system
21

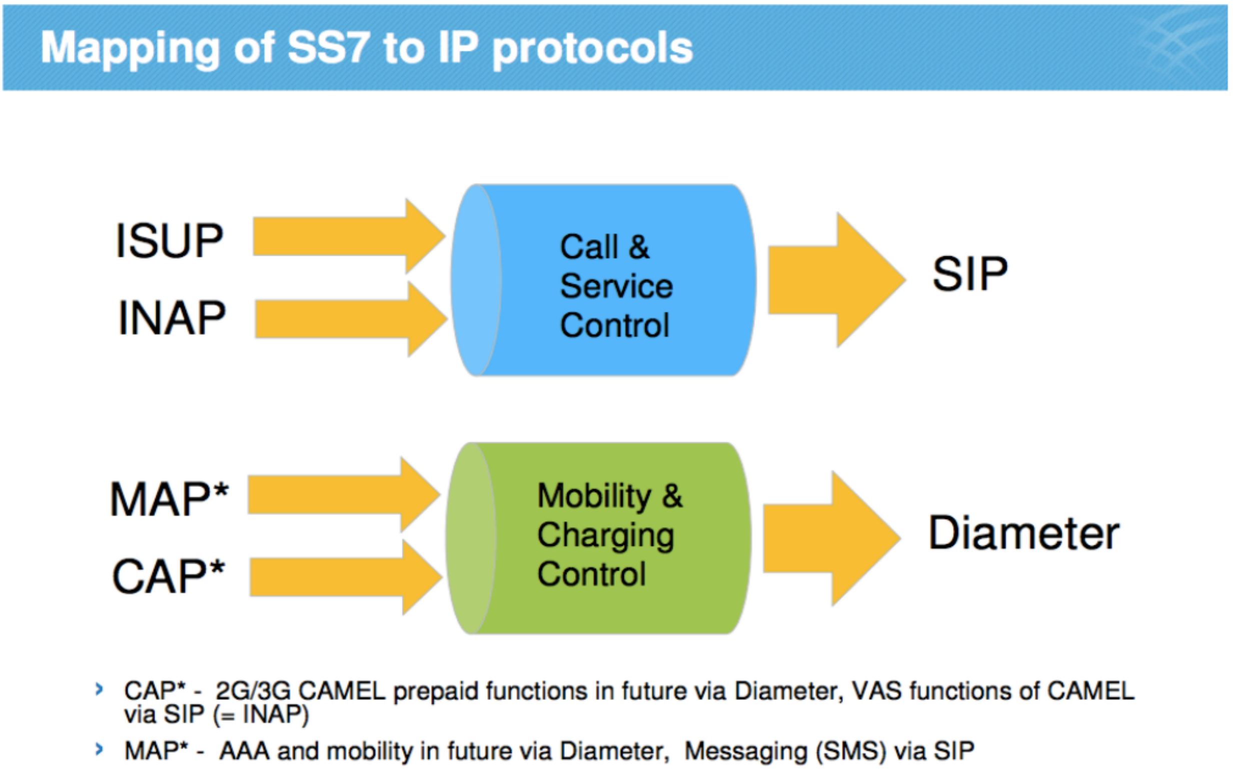
4.1 LTE: Equipment Attack surface increase

- Diameter (New)
  - Added surface
  - New code, maturity in question
  - Very few commercial fuzzers support it
  - Even less really trigger bugs in Diameter (depth pbm)
- S1/X2AP (New)
  - GTP + MAP within two completely new protocols
  - With encapsulation of user traffic (Non Access Stratum protocol)
- What could possibly go wrong?



Comparing the SS7 and Diameter Protocol Stacks

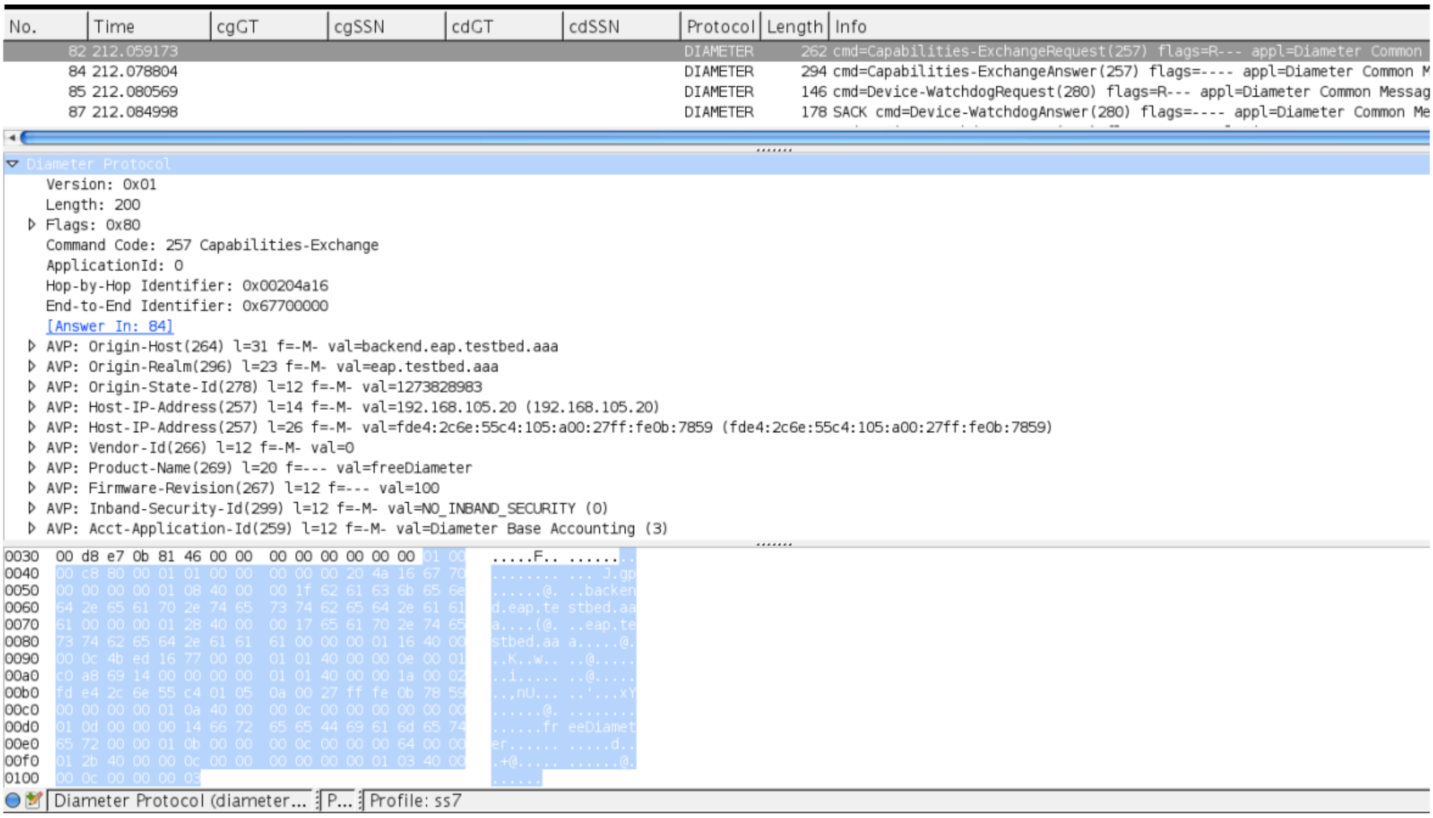
- Diameter is the successor of Radius, originally used for AAA
- Diameter acts as an “envelope” for applications (= interfaces)



Mapping of SS7 to IP protocols

- CAP* - 2G/3G CAMEL prepaid functions in future via Diameter, VAS functions of CAMEL via SIP (= INAP)
- MAP* - AAA and mobility in future via Diameter, Messaging (SMS) via SIP

4.2 Diameter audit/fuzzing problem



```
No.    Time        cgGT  cgSSN  cdGT  cdSSN  Protocol  Length  Info
    82 212.059173                            DIAMETER     262 cmd=Capabilities-ExchangeRequest(257) flags=R--- appl=Diameter Common
    84 212.078804                            DIAMETER     294 cmd=Capabilities-ExchangeAnswer(257) flags=---- appl=Diameter Common M
    85 212.080569                            DIAMETER     146 cmd=Device-WatchdogRequest(280) flags=R--- appl=Diameter Common Messag
    87 212.084998                            DIAMETER     178 SACK cmd=Device-WatchdogAnswer(280) flags=---- appl=Diameter Common Me
```

```
▽ Diameter Protocol
    Version: 0x01
    Length: 200
  ▷ Flags: 0x80
    Command Code: 257 Capabilities-Exchange
    ApplicationId: 0
    Hop-by-Hop Identifier: 0x00204a16
    End-to-End Identifier: 0x67700000
    [Answer In: 84]
  ▷ AVP: Origin-Host(264) l=31 f=-M- val=backend.eap.testbed.aaa
  ▷ AVP: Origin-Realm(296) l=23 f=-M- val=eap.testbed.aaa
  ▷ AVP: Origin-State-Id(278) l=12 f=-M- val=1273828983
  ▷ AVP: Host-IP-Address(257) l=14 f=-M- val=192.168.105.20 (192.168.105.20)
  ▷ AVP: Host-IP-Address(257) l=26 f=-M- val=fde4:2c6e:55c4:105:a00:27ff:fe0b:7859 (fde4:2c6e:55c4:105:a00:27ff:fe0b:7859)
  ▷ AVP: Vendor-Id(266) l=12 f=-M- val=0
  ▷ AVP: Product-Name(269) l=20 f=--- val=freeDiameter
  ▷ AVP: Firmware-Revision(267) l=12 f=--- val=100
  ▷ AVP: Inband-Security-Id(299) l=12 f=-M- val=NO_INBAND_SECURITY (0)
  ▷ AVP: Acct-Application-Id(259) l=12 f=-M- val=Diameter Base Accounting (3)
```

```
0030  00 d8 e7 0b 81 46 00 00  00 00 00 00 00 00 01 00   .....F.. ........
0040  00 c8 80 00 01 01 00 00  00 00 00 20 4a 16 67 70   ........ ... J.gp
0050  00 00 00 00 01 08 40 00  00 1f 62 61 63 6b 65 6e   ......@. ..backen
0060  64 2e 65 61 70 2e 74 65  73 74 62 65 64 2e 61 61   d.eap.te stbed.aa
0070  61 00 00 00 01 28 40 00  00 17 65 61 70 2e 74 65   a....(@. ..eap.te
0080  73 74 62 65 64 2e 61 61  61 00 00 00 01 16 40 00   stbed.aa a.....@.
0090  00 0c 4b ed 16 77 00 00  01 01 40 00 00 0e 00 01   ..K..w.. ..@.....
00a0  c0 a8 69 14 00 00 00 00  01 01 40 00 00 1a 00 02   ..i..... ..@.....
00b0  fd e4 2c 6e 55 c4 01 05  0a 00 27 ff fe 0b 78 59   ..,nU... ..'...xY
00c0  00 00 00 00 01 0a 40 00  00 0c 00 00 00 00 00 00   ......@. ........
00d0  01 0d 00 00 00 14 66 72  65 65 44 69 61 6d 65 74   ......fr eeDiamet
00e0  65 72 00 00 01 0b 00 00  00 0c 00 00 00 64 00 00   er...... .....d..
00f0  01 2b 40 00 00 0c 00 00  00 00 00 00 01 03 40 00   .+@..... ......@.
0100  00 0c 00 00 00 03                                  ......
```

5.1. Auditor’s bias #1

Open Standards doesn’t mean vision

- Diameter
  - Nearly every parameter is optional
- Result
  - Nobody knows what is a valid combination
    - To test/fuzz/inject
- Combinational explosion
  - Sequence/Dialogue/Flow
  - AVP combination
  - AVP values
  - Fuzzed parameter
- Even manufacturers don’t know how to successfully instrument the Device Under Test
- Fuzzer Support is not Fuzzer successful triggering

5.2 Audior’s bias #2

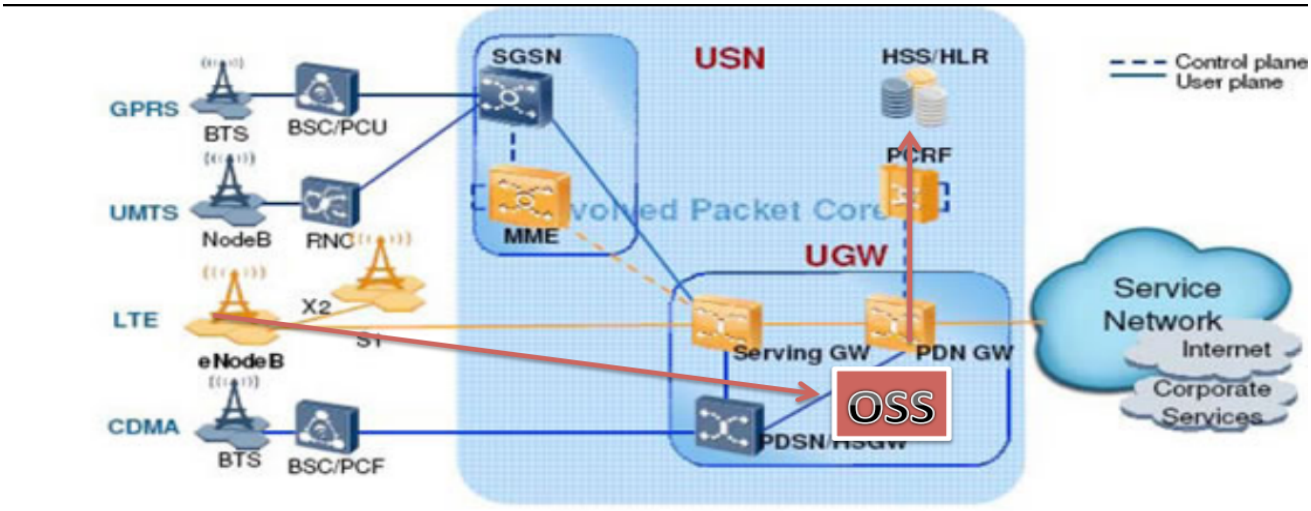
Fuzzing is a deep as fuzzer goes

- Fuzzer never go deep enough
  - Commercial fuzzer
    - 0 trigger/1000 iteration
  - Standard own fuzzer
    - 13 triggers/1000 iterations
- Need target-specific development
  - Customised own fuzzer:
    - 85 triggers/100 iterations

5.2.1 LTE: New risk with Diameter

- Diameter information network dissemination
- Diameter awesomeness
  - Distribution/centralisation
  - Its own evil side
- Present in many databases
  - HSS, SDM/SDR, CUD
- The goal was to centralise
- The result is one more database

5.2.2 LTE Huawei Specific

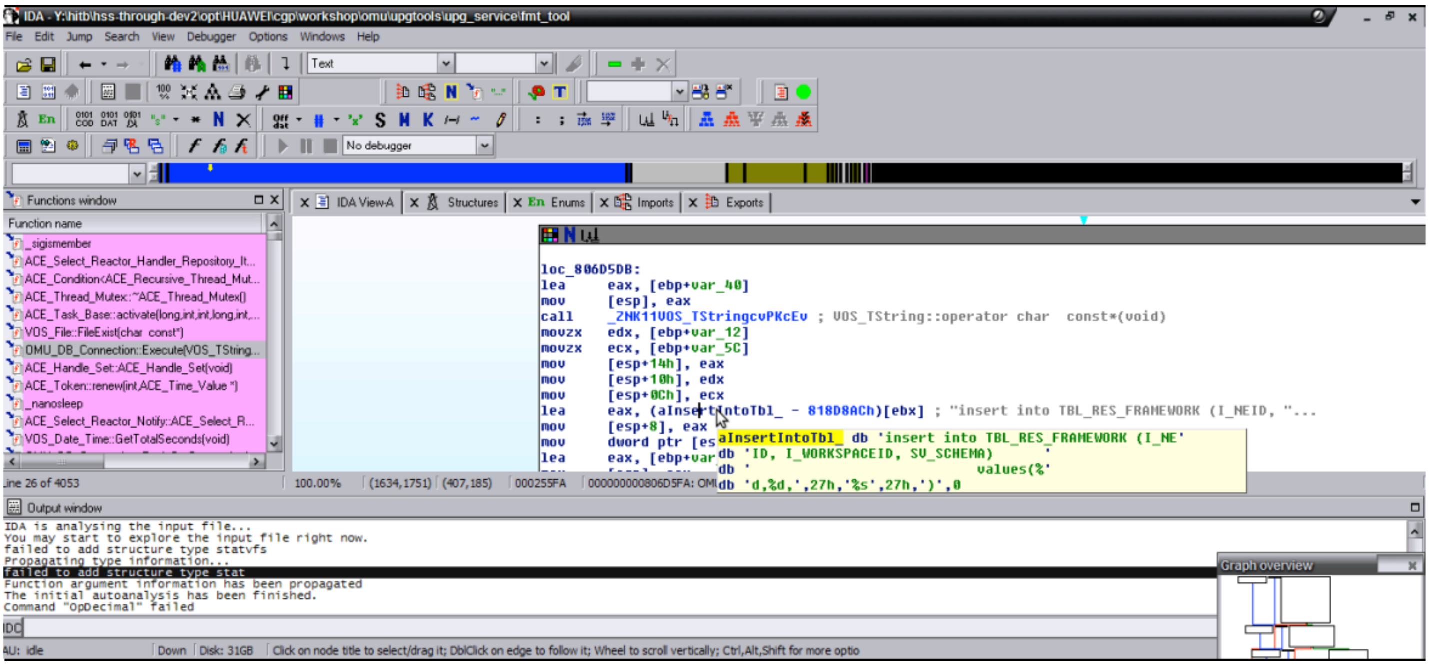


Source: 3GPP.org

- USN = SGSN + MME
- UGW = SeGW + SGW + PDN GW/PGW

5.2.3 Pwning LTE HSS

C++ SQL Injection everywhere



IDA - Y:\hitb\hss-through-dev2\opt\HUAWEI\cgp\workshop\omu\upgtools\upg_service\fmt_tool

Functions window

Function name
```
_sigismember
ACE_Select_Reactor_Handler_Repository_It...
ACE_Condition<ACE_Recursive_Thread_Mut...
ACE_Thread_Mutex::~ACE_Thread_Mutex()
ACE_Task_Base::activate(long,int,int,long,int,...
VOS_File::FileExist(char const*)
OMU_DB_Connection::Execute(VOS_TString...
ACE_Handle_Set::ACE_Handle_Set(void)
ACE_Token::renew(int,ACE_Time_Value *)
_nanosleep
ACE_Select_Reactor_Notify::ACE_Select_R...
VOS_Date_Time::GetTotalSeconds(void)
```

```
loc_806D5DB:
lea     eax, [ebp+var_40]
mov     [esp], eax
call    _ZNK11VOS_TStringcvPKcEv ; VOS_TString::operator char  const*(void)
movzx   edx, [ebp+var_12]
movzx   ecx, [ebp+var_5C]
mov     [esp+14h], eax
mov     [esp+10h], edx
mov     [esp+0Ch], ecx
lea     eax, (aInsertIntoTbl_ - 818D8ACh)[ebx] ; "insert into TBL_RES_FRAMEWORK (I_NEID, "...
mov     [esp+8], eax
mov     dword ptr [es
lea     eax, [ebp+var

aInsertIntoTbl_ db 'insert into TBL_RES_FRAMEWORK (I_NE'
db 'ID, I_WORKSPACEID, SV_SCHEMA)        '
db '                              values(%'
db 'd,%d,',27h,'%s',27h,')',0
```

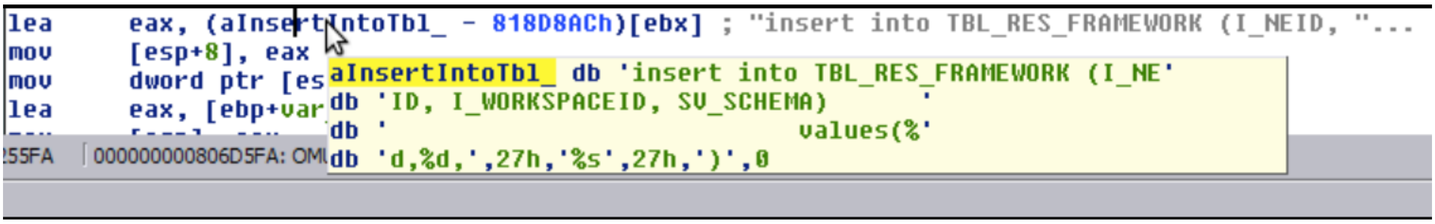
Line 26 of 4053 | 100.00% | (1634,1751) | (407,185) | 000255FA | 00000000806D5FA: OMU

Output window
```
IDA is analysing the input file...
You may start to explore the input file right now.
failed to add structure type statvfs
Propagating type information...
failed to add structure type stat
Function argument information has been propagated
The initial autoanalysis has been finished.
Command "OpDecimal" failed
```

AU: idle | Down | Disk: 31GB | Click on node title to select/drag it; DblClick on edge to follow it; Wheel to scroll vertically; Ctrl,Alt,Shift for more optio

5.2.4 LTE HSS Pwning methodology

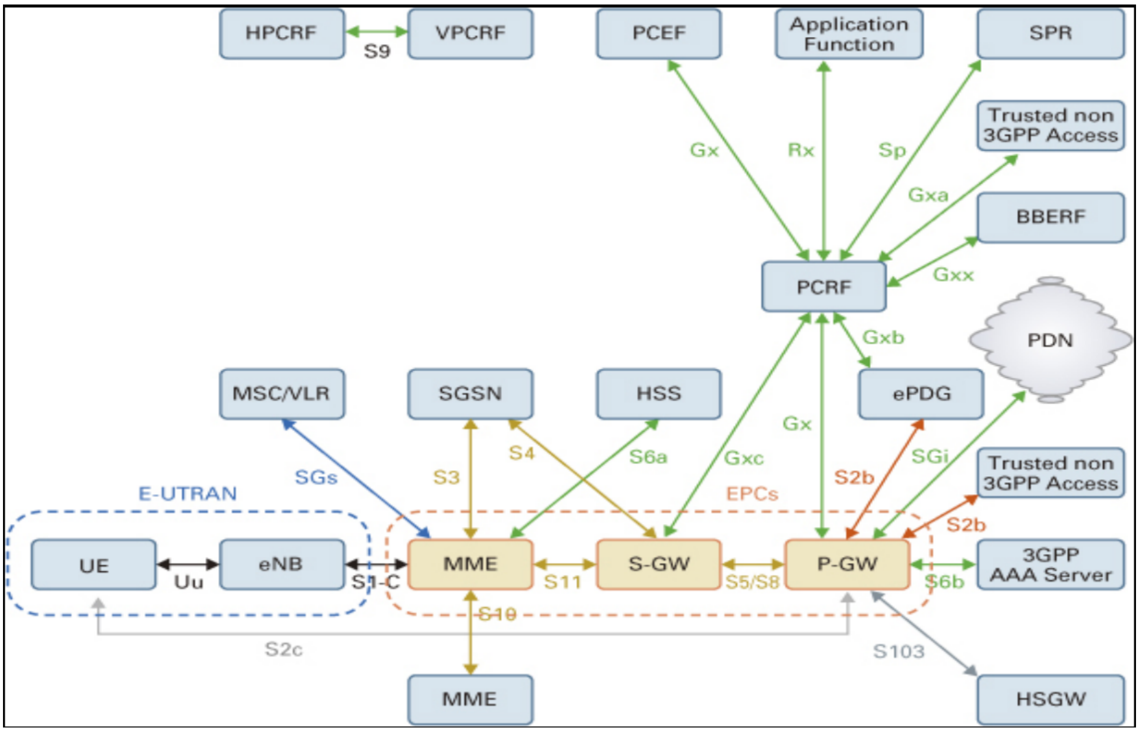
- OSS is considered Core
- It is accessible by eNodeBs
  - Sometimes: Network filtering mistakes
  - Often: Allowed for Provisioning
- OSS can connect to HSS
  - HSS exports too many services
  - Mux/Tunnel kind of thinking
    - One port == many services



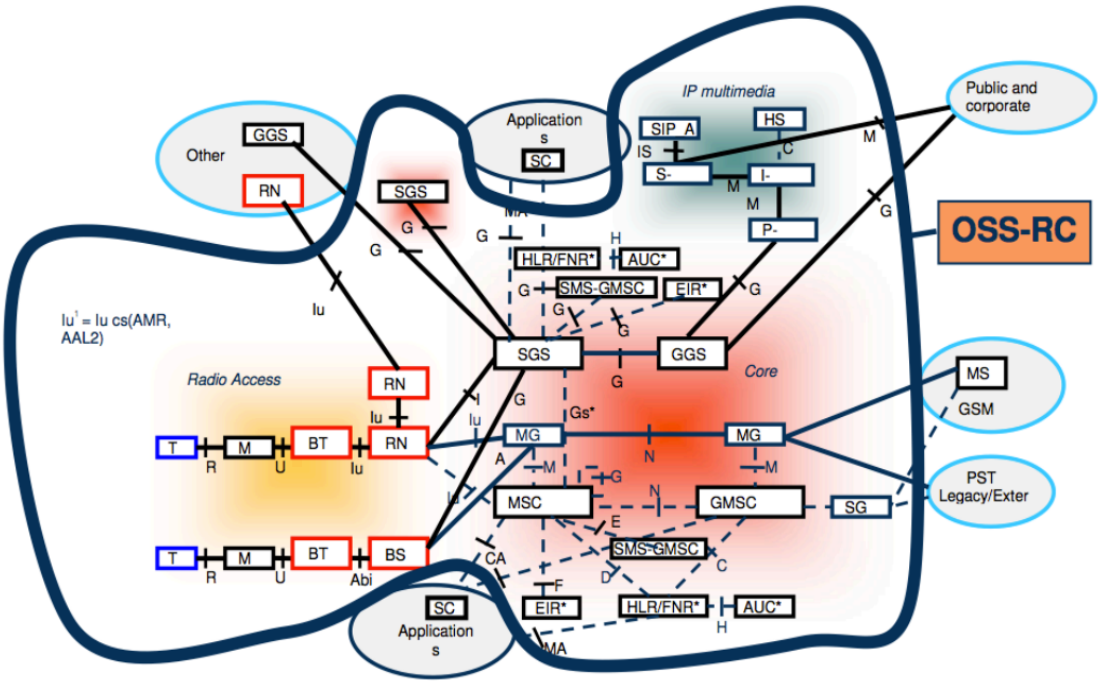
```
lea     eax, (aInsertIntoTbl_ - 818D8ACh)[ebx] ; "insert into TBL_RES_FRAMEWORK (I_NEID, "...
mov     [esp+8], eax
mov     dword ptr [es
lea     eax, [ebp+var

aInsertIntoTbl_ db 'insert into TBL_RES_FRAMEWORK (I_NE'
db 'ID, I_WORKSPACEID, SV_SCHEMA)        '
db '                              values(%'
db 'd,%d,',27h,'%s',27h,')',0
```

55FA | 00000000806D5FA: OMU

LTE EPC functional plane, no OAM



Add OAM: complexity explosion

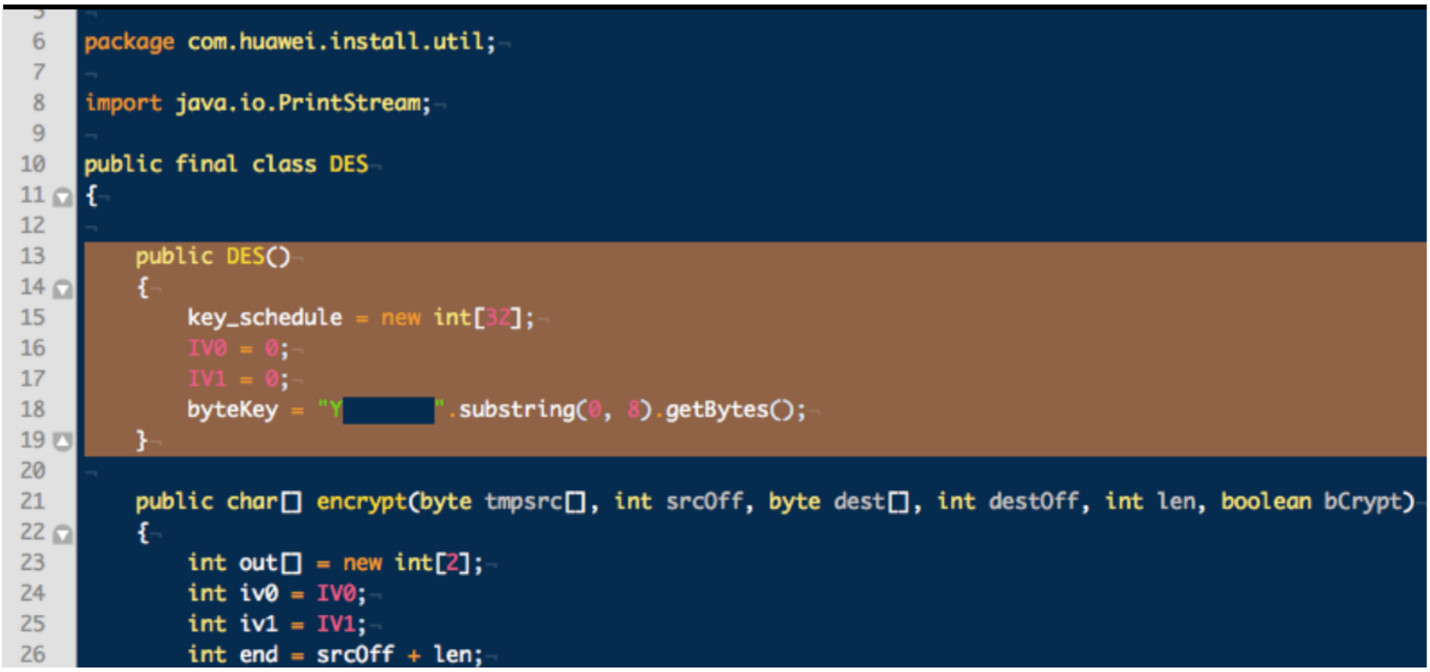


5.3 Auditor’s bias #3

Manual vision is always incomplete

- Need some automation
- 200 APNs * 16 million IPs == necessity for a dedicated scanner
  - Each valid GTP tunnel is a new 16 millions IPs to scan
  - Address space explosion
- You CANNOT do it manually
  - You CANNOT do it without specific scanners

5.3.1 Pwning MME: Hardcoded encryption keys



```
package com.huawei.install.util;

import java.io.PrintStream;

public final class DES
{

    public DES()
    {
        key_schedule = new int[32];
        IV0 = 0;
        IV1 = 0;
        byteKey = "Y[redacted]".substring(0, 8).getBytes();
    }

    public char[] encrypt(byte tmpsrc[], int srcOff, byte dest[], int destOff, int len, boolean bCrypt)
    {
        int out[] = new int[2];
        int iv0 = IV0;
        int iv1 = IV1;
        int end = srcOff + len;
```

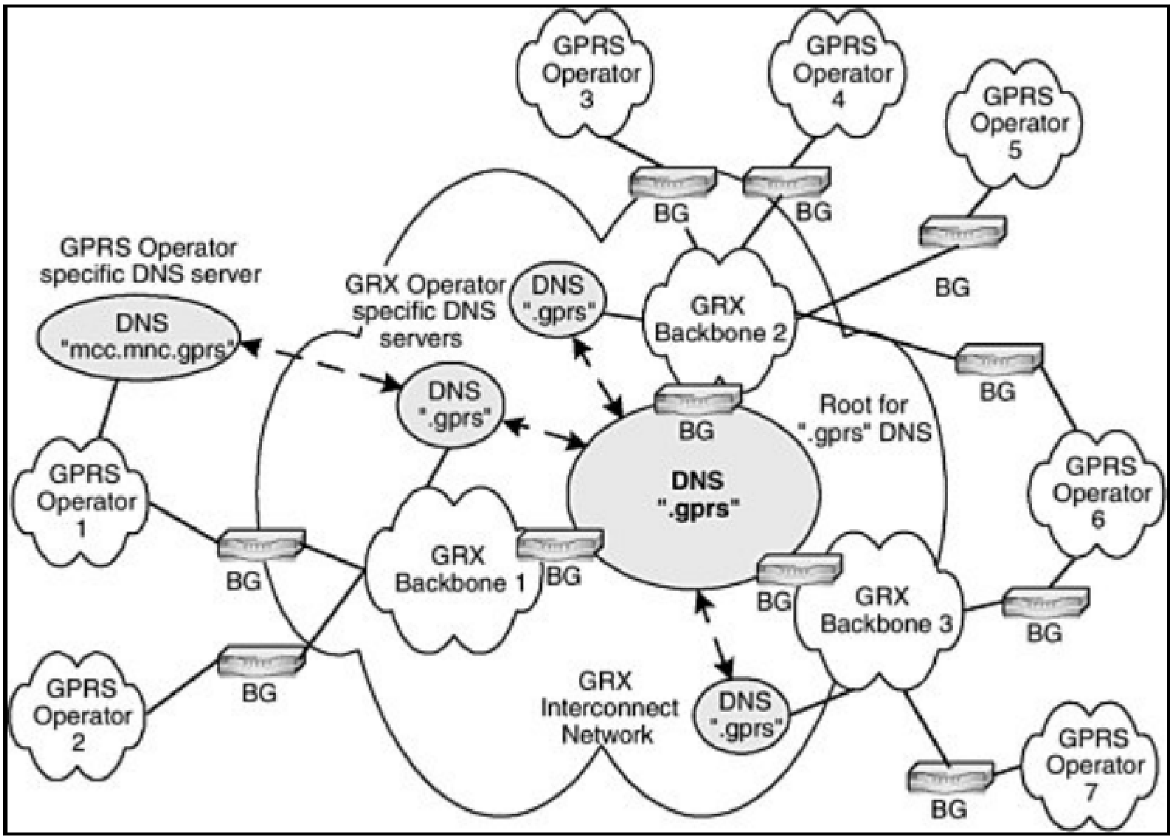
P1 VKB CVID#485 DES…Hardcoded keys everywhere

5.3.2 Legacy PS Interfaces of interest to LTE

- Gi : Interface from GGSN to Internet
- Gn : Interface between SGSN and other SGSN and (internal) GGSN
- Gp : Interface between Internal SGSN and external GGSN (GRX used here)

5.3.3 eDNS vs iDNS

- Leaks to Internet
- Passive DNSmon
- Leaks to GPRS
- Leaks to 3G data
- Leaks to LTE EPC



5.3.4 Legacy GPRS / UMTS

- GRX
- TLD/Domain . gprs
- Quite monolithic
    - APN
    - RAI
        - rai<RAI>. Mnc08. Mcc204.gprs
- Only APNs and “some” network element

5.3.5 IMS DNS

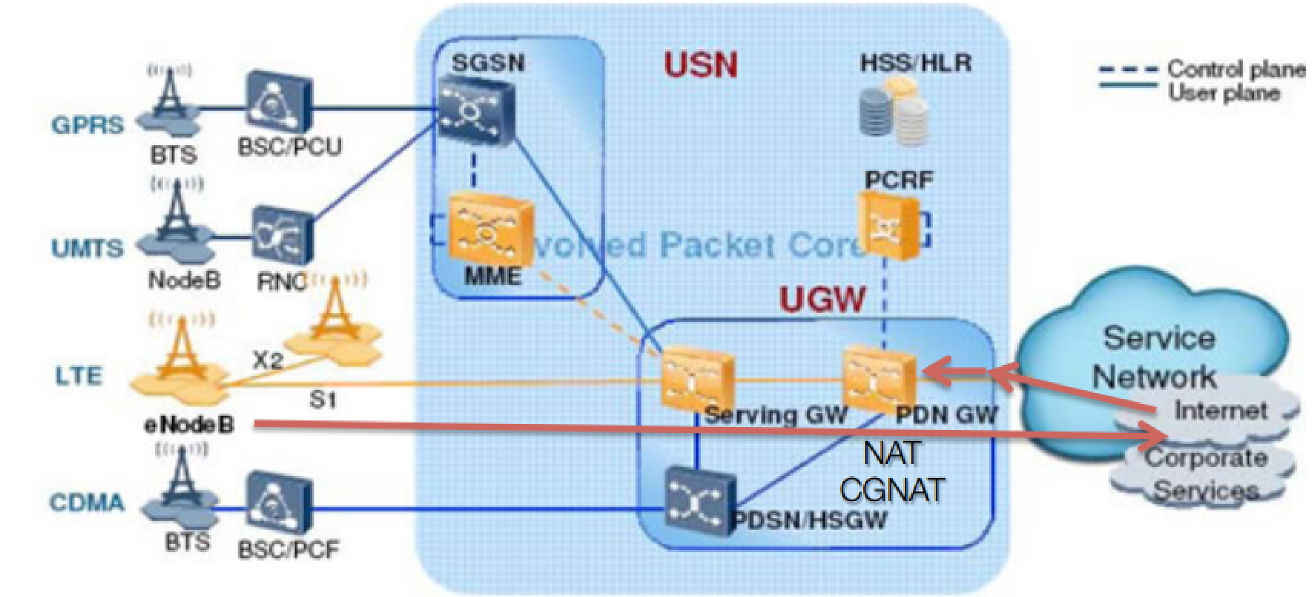
- 3gppnetwork.org
- Supports and lists all Network Element
    - LAC
    - RAC
- Examples
    - rac<RAC>.lac<LAC>.mnc08.mcc204.gprs

5.3.6 LTE EPC DNS

- Same as IMS DNS but extended
- Supports and lists most SA EPC Network Elements
    - MME
    - SGW
- Examples
    - mmec<MMEC>.mmegi<MMEGI>.mme.epc.mnc99.mcc208.3gppnetwork.org

5.3.7 Pwning from LTE mobile

- Infrastructure Reverse path protection
- LTE Mobile data access
- RFC1918 leaks (sometimes)
- Datacom IP infrastructure access (currently more usual)

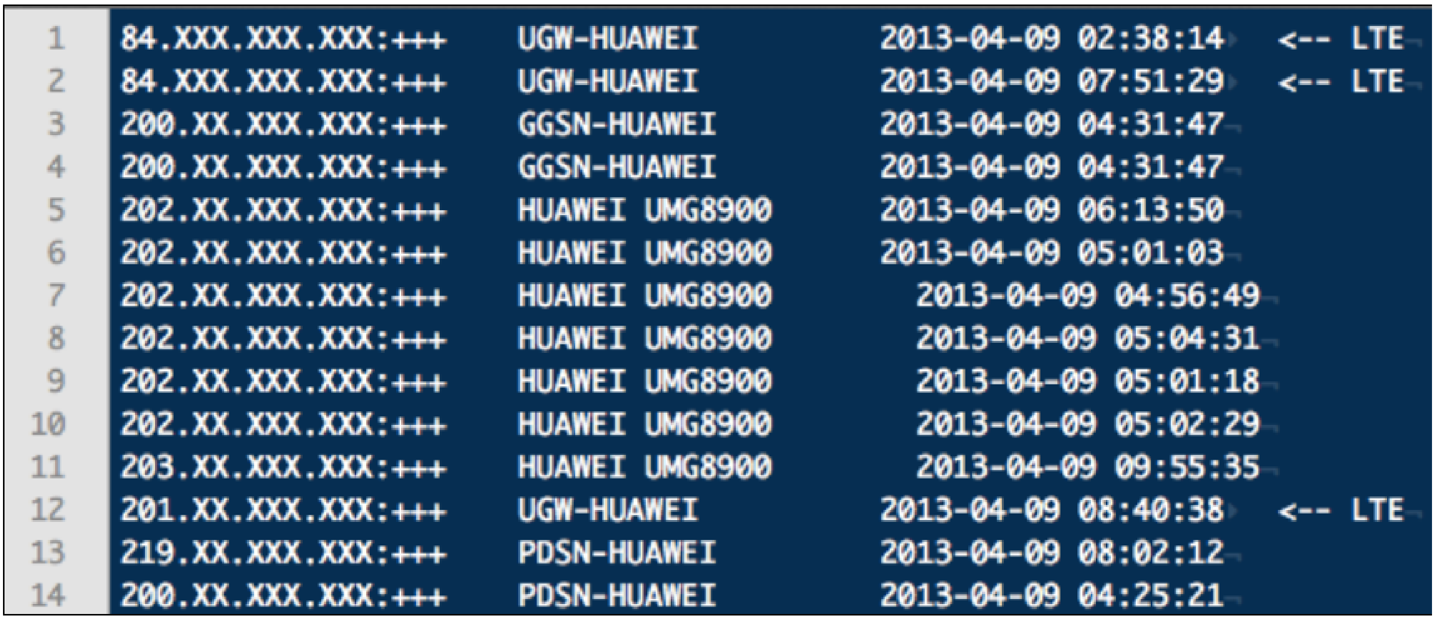


Source: 3GPP.org

5.3.8 Pwning from external

Direct MML access from Internet

- Pawning from external without any reverse path trick
- Shodan doesn’t work on these
- MML attack surface exposed



```
84.XXX.XXX.XXX:+++     UGW-HUAWEI            2013-04-09 02:38:14   <-- LTE
84.XXX.XXX.XXX:+++     UGW-HUAWEI            2013-04-09 07:51:29   <-- LTE
200.XX.XXX.XXX:+++     GGSN-HUAWEI           2013-04-09 04:31:47
200.XX.XXX.XXX:+++     GGSN-HUAWEI           2013-04-09 04:31:47
202.XX.XXX.XXX:+++     HUAWEI UMG8900        2013-04-09 06:13:50
202.XX.XXX.XXX:+++     HUAWEI UMG8900        2013-04-09 05:01:03
202.XX.XXX.XXX:+++     HUAWEI UMG8900          2013-04-09 04:56:49
202.XX.XXX.XXX:+++     HUAWEI UMG8900          2013-04-09 05:04:31
202.XX.XXX.XXX:+++     HUAWEI UMG8900          2013-04-09 05:01:18
202.XX.XXX.XXX:+++     HUAWEI UMG8900          2013-04-09 05:02:29
203.XX.XXX.XXX:+++     HUAWEI UMG8900          2013-04-09 09:55:35
201.XX.XXX.XXX:+++     UGW-HUAWEI            2013-04-09 08:40:38   <-- LTE
219.XX.XXX.XXX:+++     PDSN-HUAWEI           2013-04-09 08:02:12
200.XX.XXX.XXX:+++     PDSN-HUAWEI           2013-04-09 04:25:21
```

5.4 Auditor’s bias #4

Testbed is always more secure

- Testbed is more secure than production
    - Legacy impact
    - Scalability impact
    - There’s always something more on the production network
- Audit is often only permitted in testbed
    - Liability
    - Potential for Denial of Service
- Result
    - Attackers advantage
    - Production goes untested

5.4.1 Technical Capacity & Knowledge issue

- Who
  - Can audit all new LTE protocols and legacy protocols
  - Has expertise on the architecture & vendors equipment
- Guarantee
  - Scanning quality
  - Coverage on all protocols & arch (CSFB, IMS, Hybrid, SCharge)
- Cover all perimeters and accesses
  - APNs
  - GRX & IPX accesses
  - Split DNS
  - User plane and control plane

Conclusion

- LTE is supposed to be built with security
  - Difference between standardisation and real security
  - Network Equipment Vendors are still lagging
- Opening up of the technology
  - Good: deeper independent security research
- Operators
  - Still disinformed by vendors
  - Security through obscurity in 20..!
  - Some are getting proactive

WW

P1 SECURITY