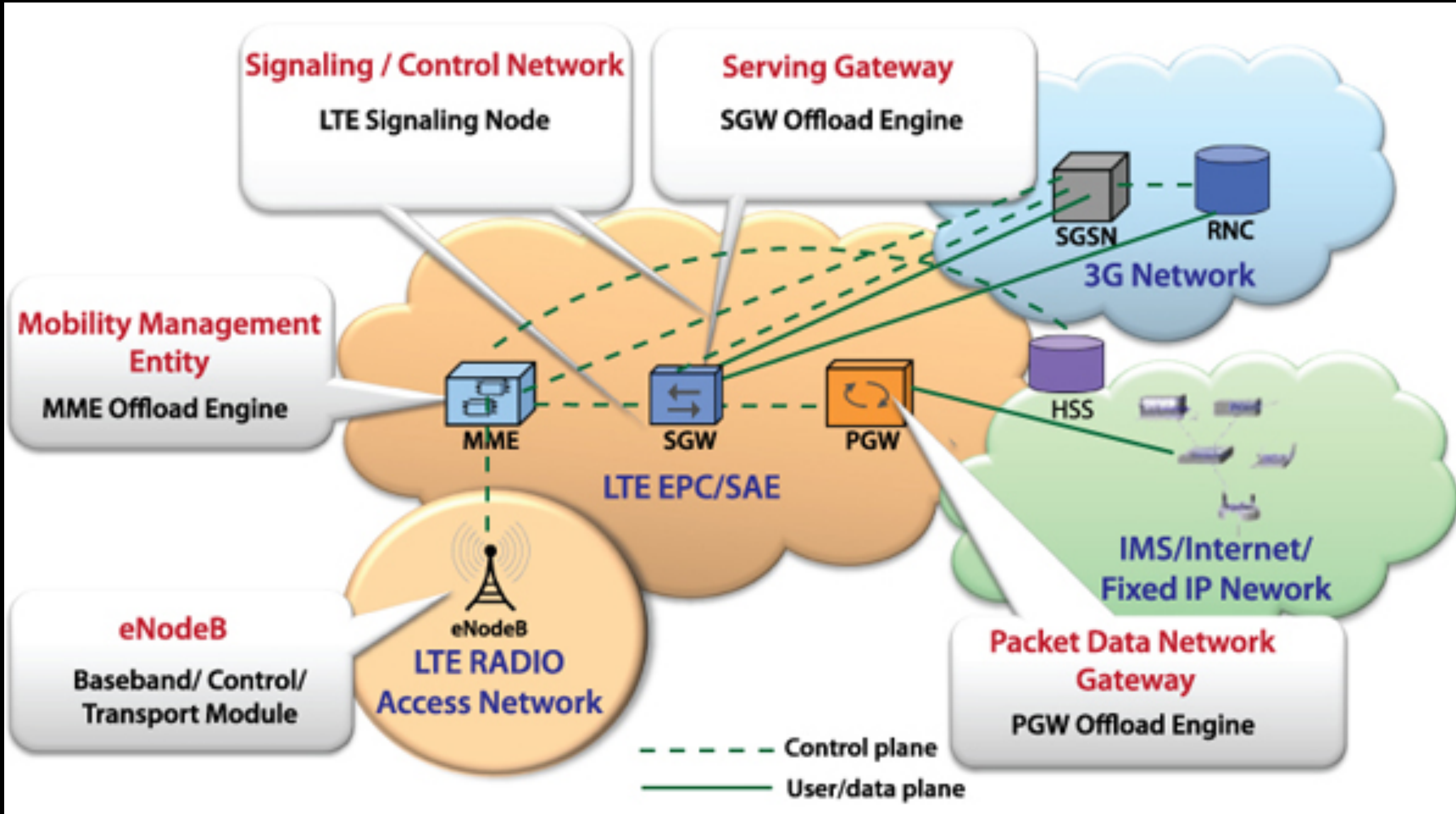
LTE Pwnage: Hacking HLR/HSS and MME Core Network Elements

P1 Security

LTE ENVIRONMENT

LTE Network Overview



Corporate & Mobile Data risk increased

P1 Security
Priority One Security

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

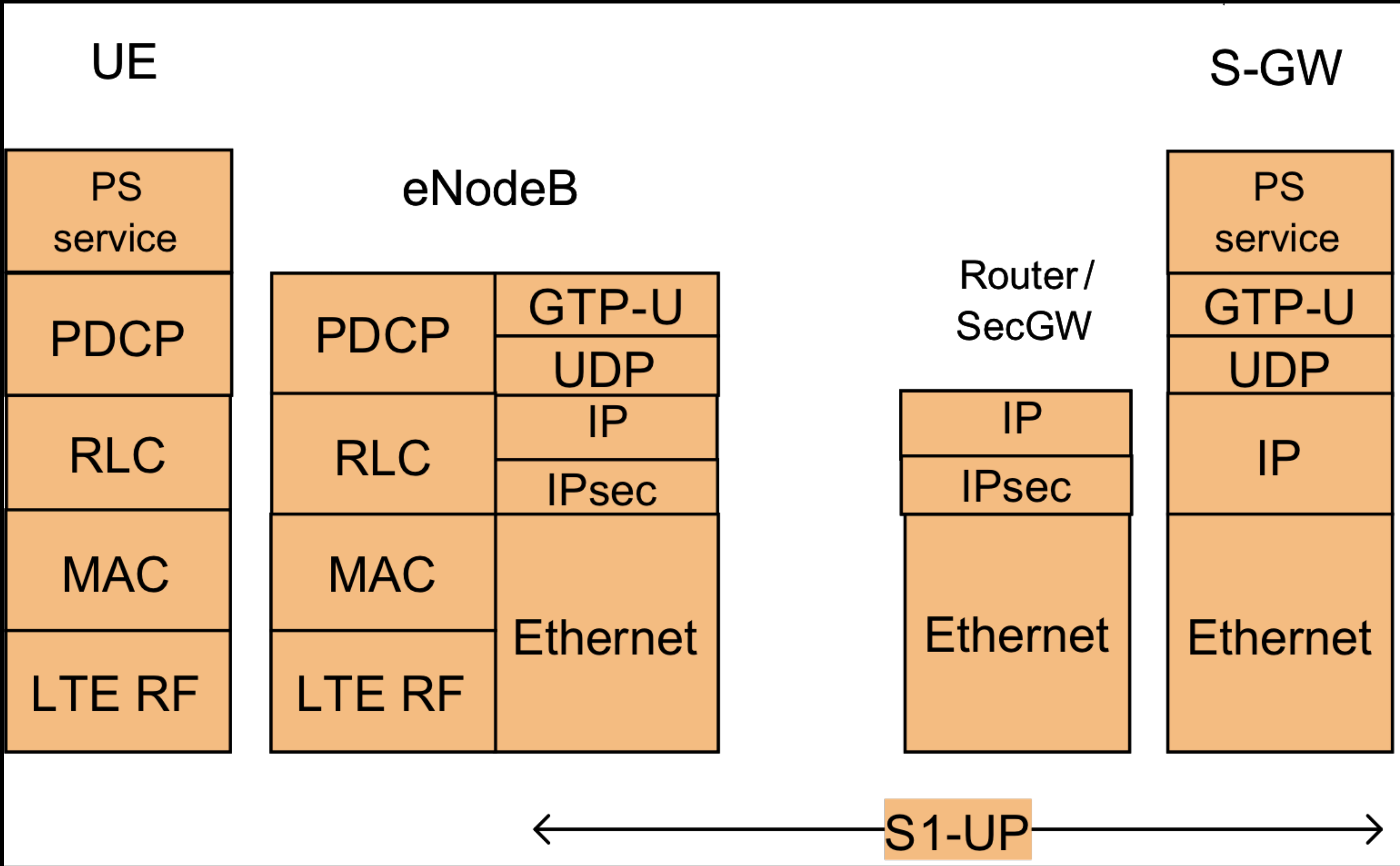
2G 3G to LTE: Reality and Legacy

P1 Security
Priority One Security

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

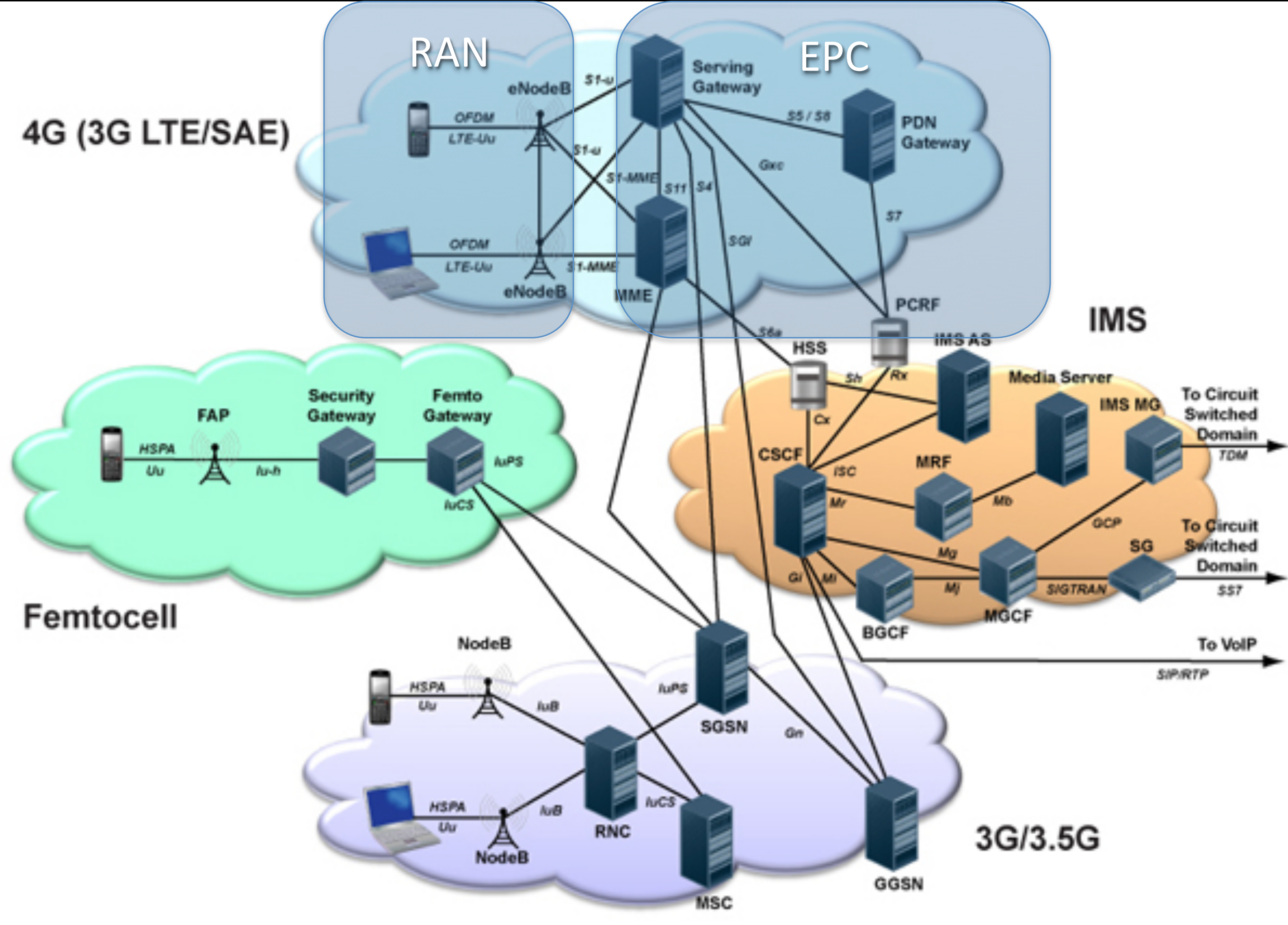
P1 Security
Priority One Security



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



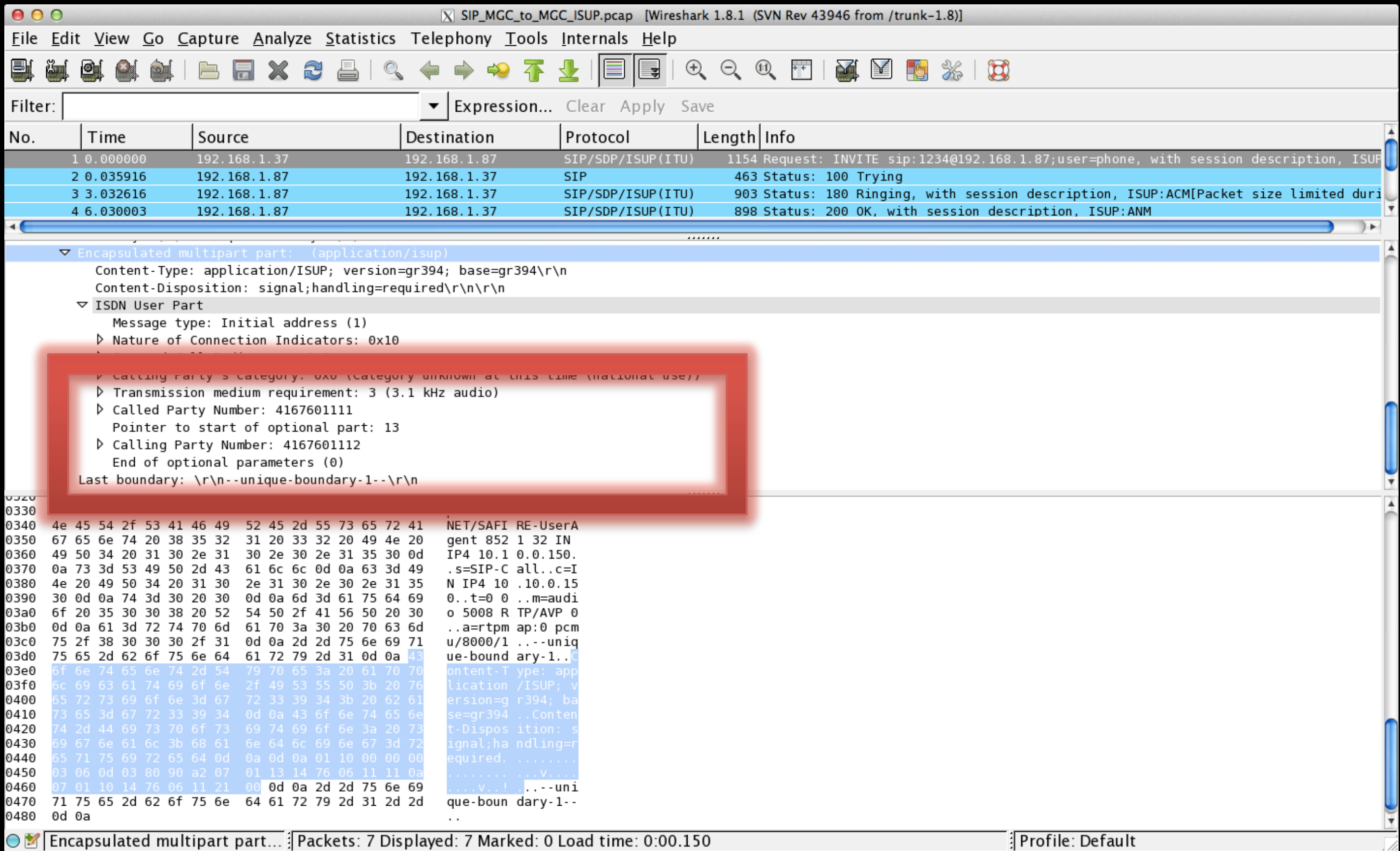
CSFB vs. VOLTE vulnerability attack surface

- 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 vulns
  - IMS (CSCF = SIP server, DNS, ...)
    - Standard? No...

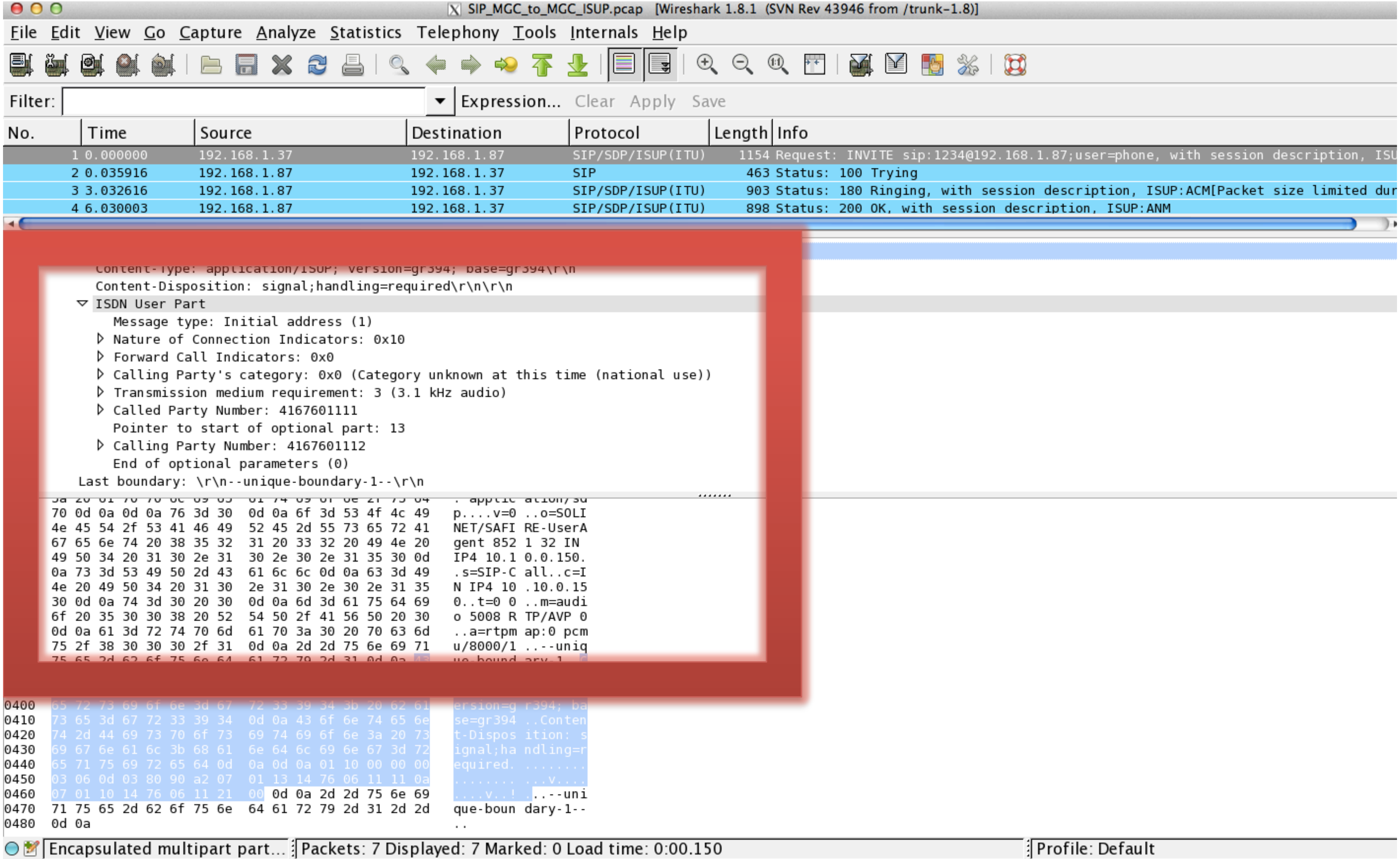
ISUP injection in SIP through VOLTE

Yes, SIP… known… but…

Internet SIP + SS7 ISUP == SIP-I and SIP-T == ISUP Injection !



- Remote Core Network DoS
- SS7 compromise
- External signaling injection
- Spoofing of ISUP messages
- Fake billing
- Ouch!


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-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
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
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

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)

P1 Security
Priority One Security

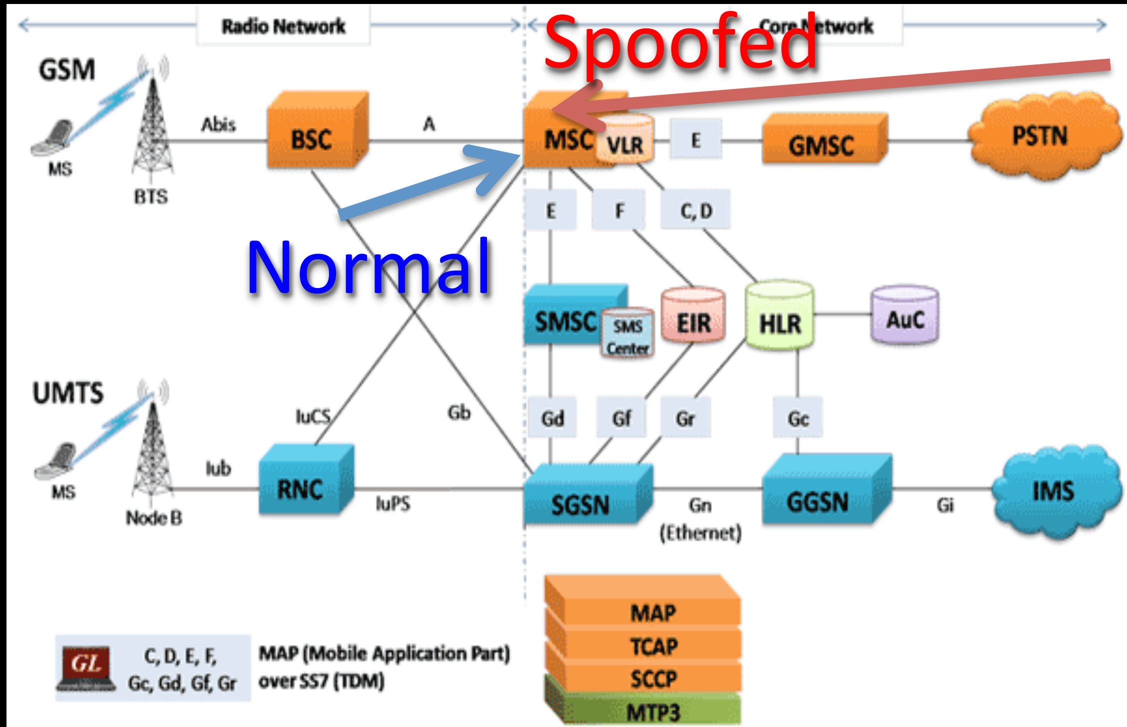
NSN NGHLR remote Denial of Service caused by fragile SS7 stack

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 telco
  - Ability to cope with X million of requests
  - Not Ability to cope with malformed traffic

GSM MAP primitive MAP_FORWARD_ACCESS_SIGNALLING enables RAN signaling 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 signaling
- As if it was coming from Radio Network

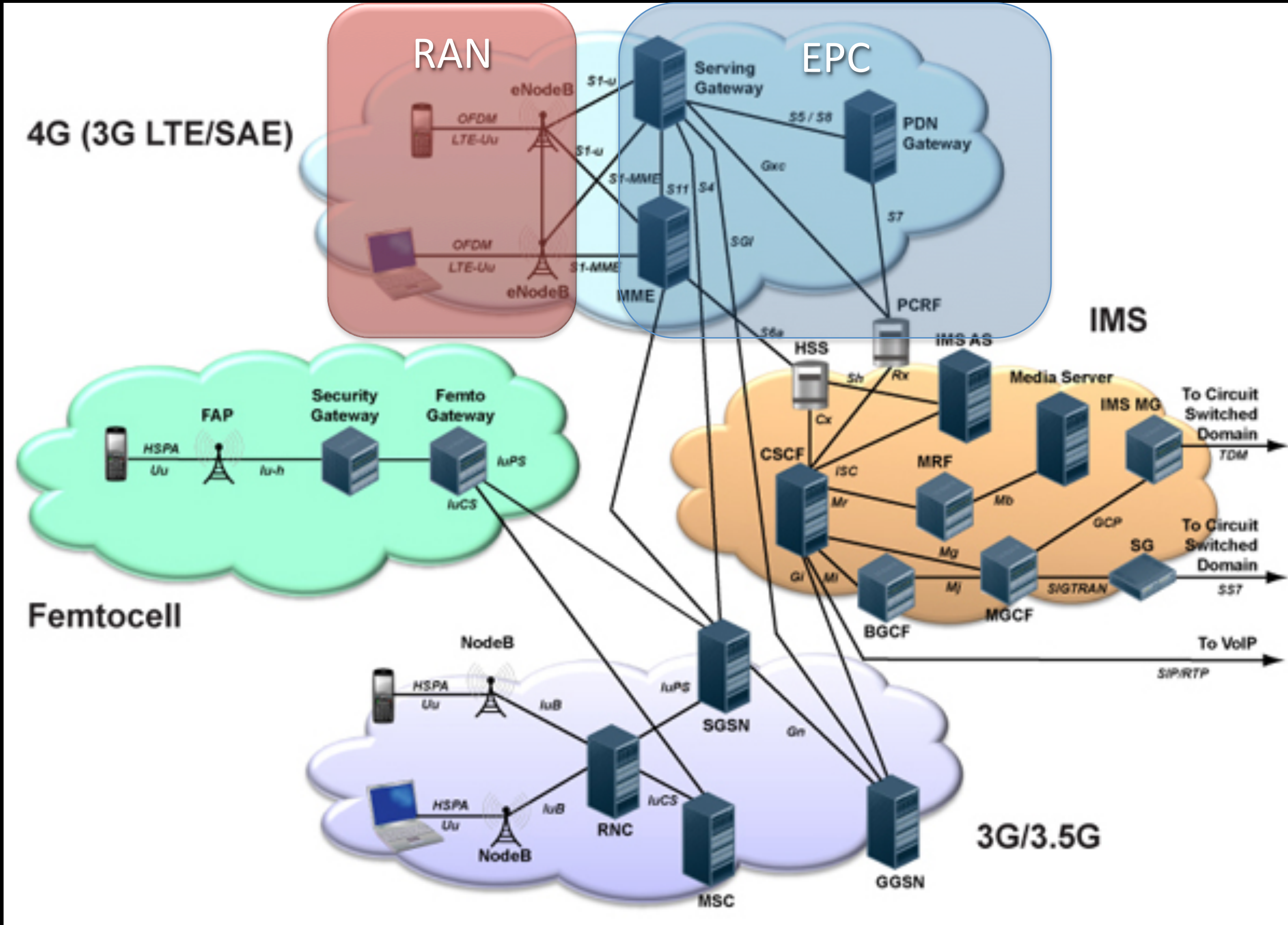
Fun Anti-forensics

- 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)
```

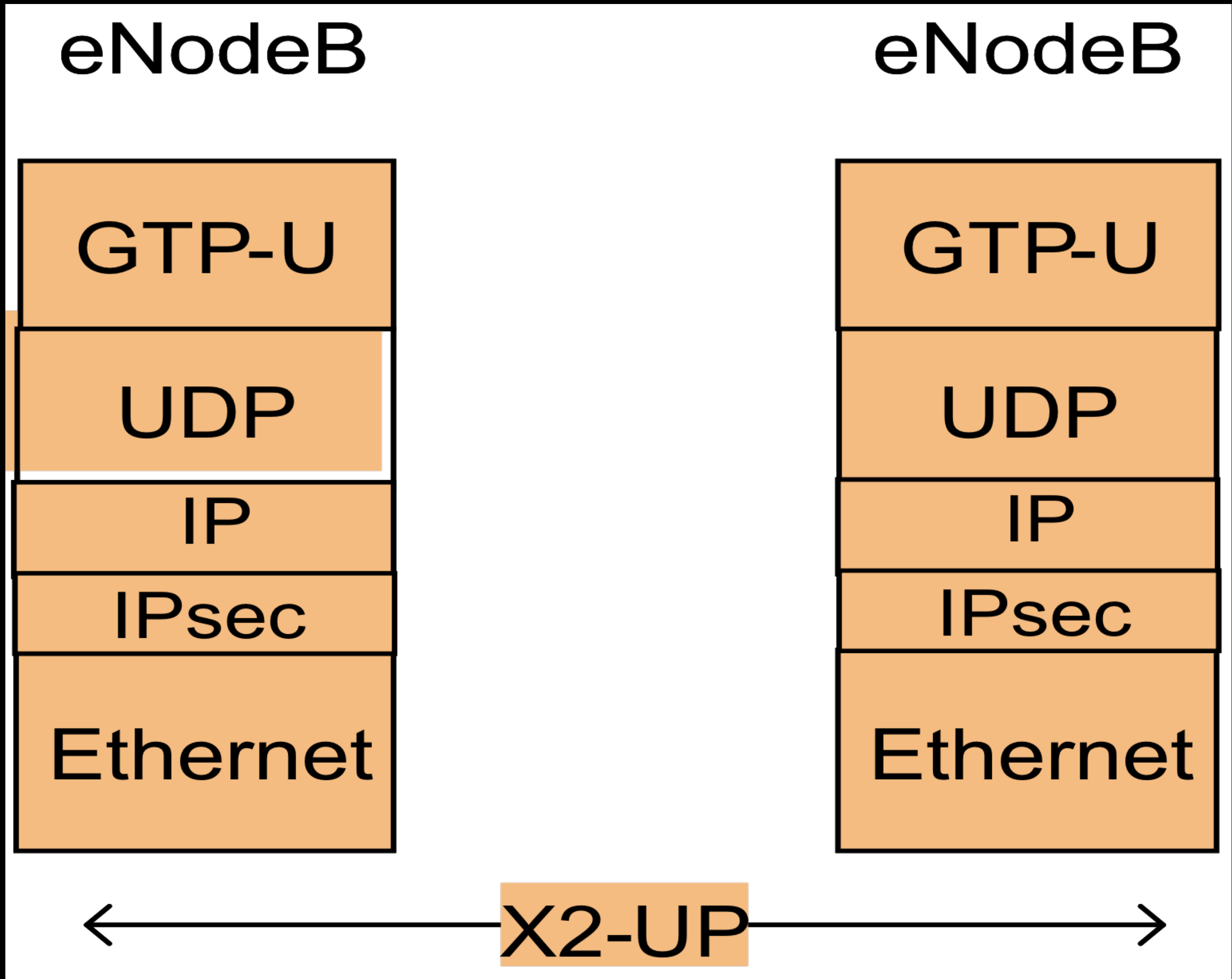
3G and LTE together



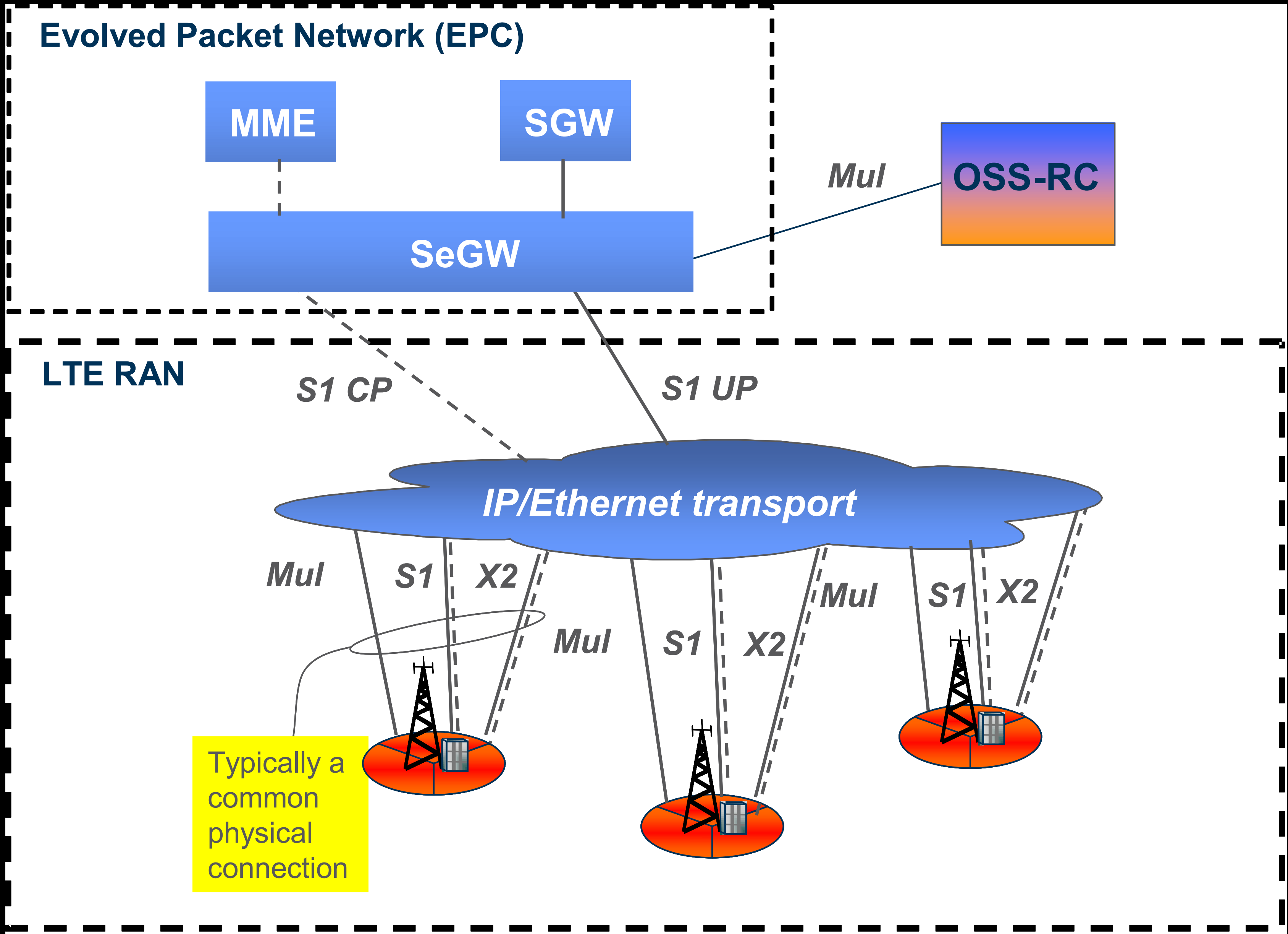
Peer to Peer Radio Access Network

- 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 defense in depth, scanning only blocked by size of network
  - Did GTP disappear? No

User data btw eNBs: LTE User Plane



LTE RAN Overview



Pwning OSS:

L2 network mistakes always happen

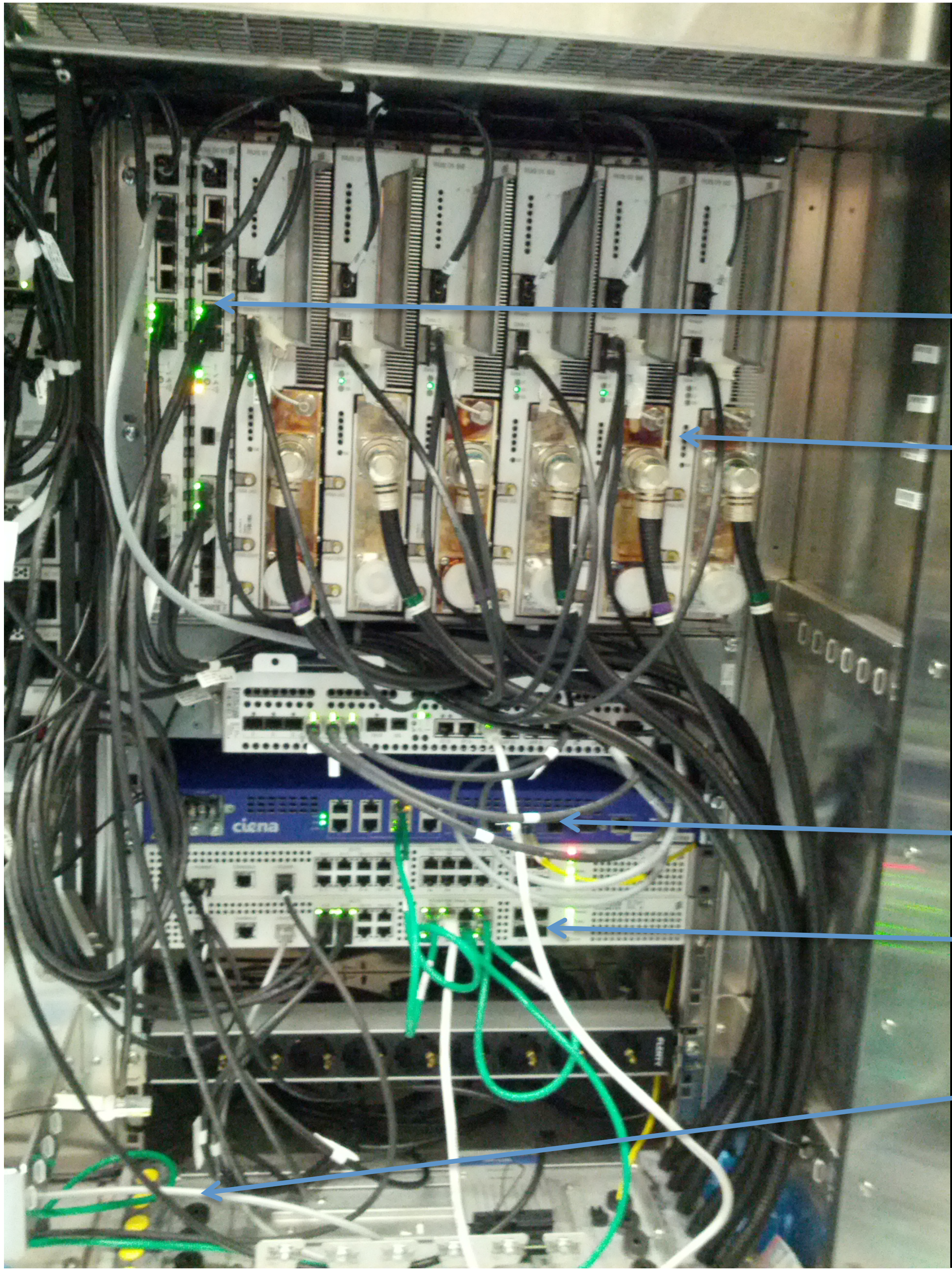
- Can’t catch it with multiple overlapping /8 networks: automate!
- From any eNodeB to the NMS
- From any eNodeB to any eNodeB
  - You can bet on insecure provisioning
- American example & Remote misconfiguration

```
# 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.
# |
```

eNodeB Hardware Attacks

Ericsson RBS 6602



DUS (2G+3G+4G) & DUL (4G)

Radio

Uplink to DWDM / Optical net

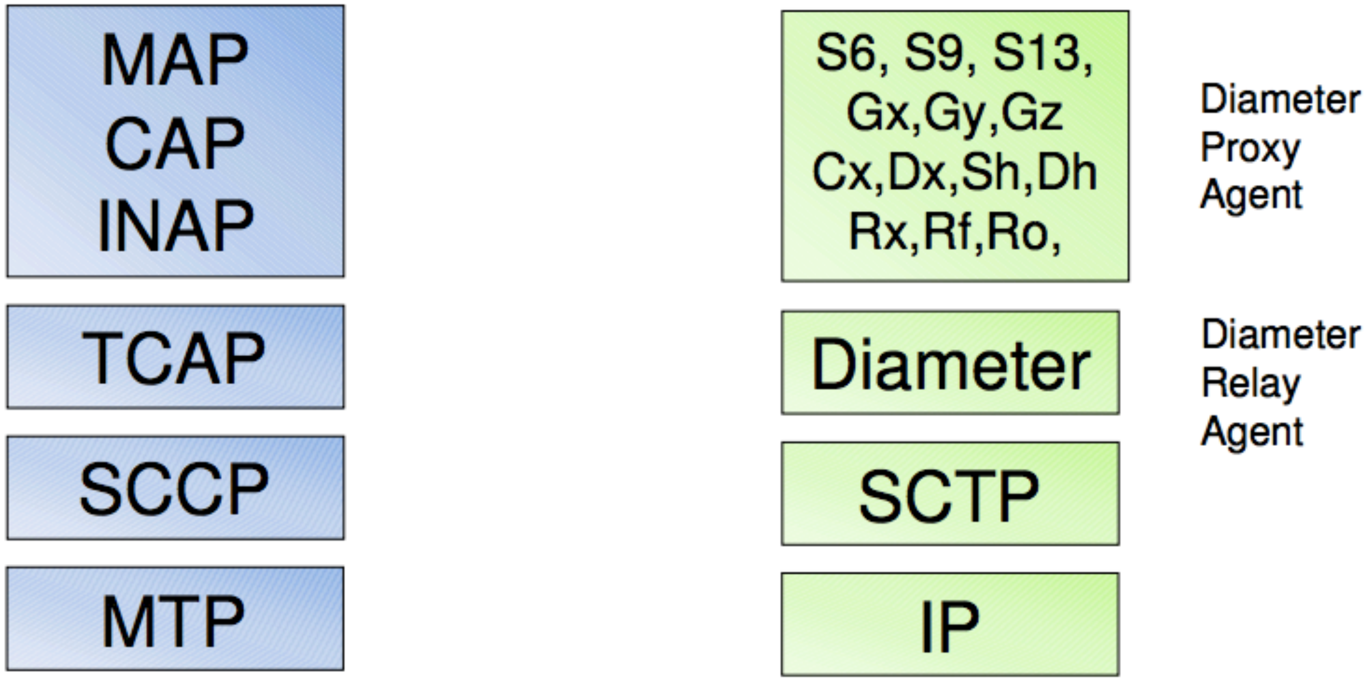
Local Ethernet ports
(not TDM anymore)

Hardware (in)security system

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?

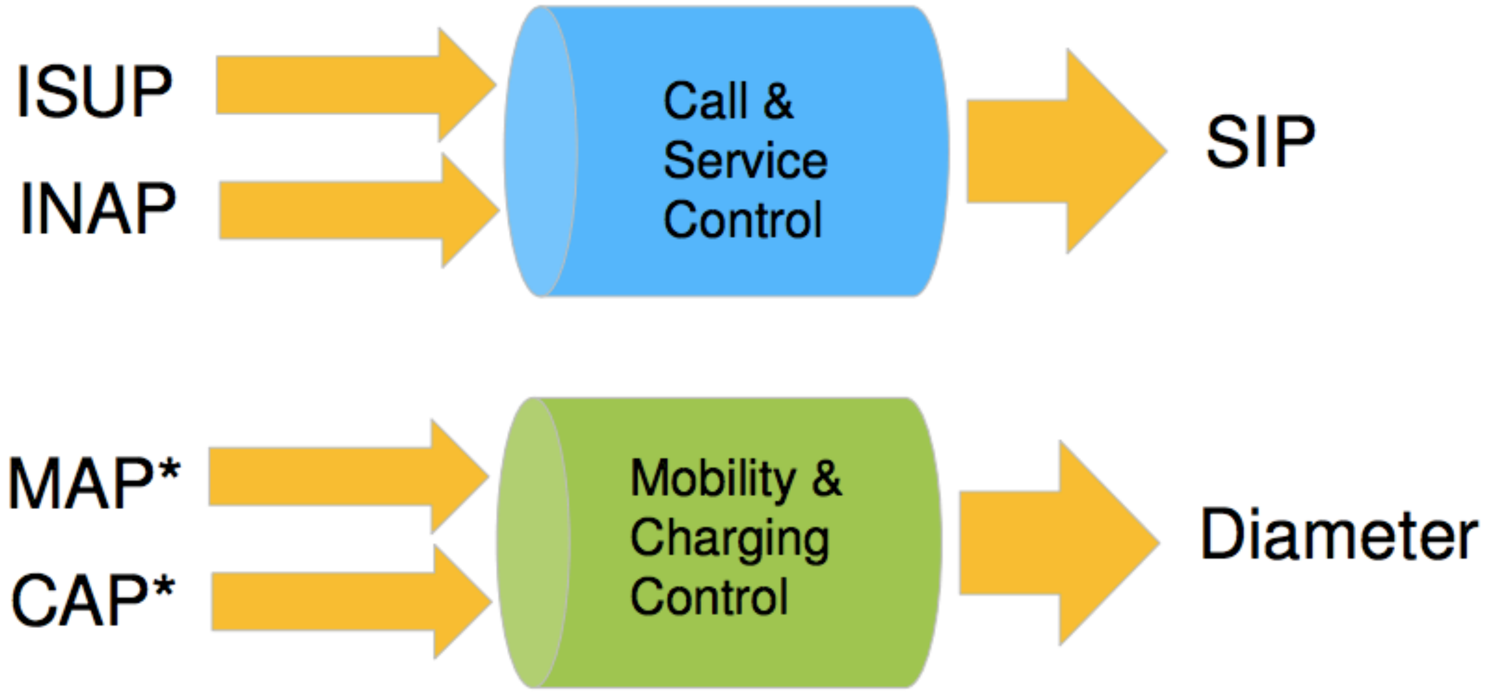
Comparing the SS7 and Diameter Protocol Stacks



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

P1 Security
Priority One Security

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

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                                  ......
```


Diameter Protocol (diameter... | P... | Profile: ss7

Auditor bias #1: Open standards doesn't mean vision

P1 Security
Priority One Security

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

Auditor bias #2: Fuzzing is as deep as fuzzer goes

- And fuzzer never go deep enough
  - Commercial fuzzer

    `0 trigger/1000 iteration`
  - Standard own fuzzer

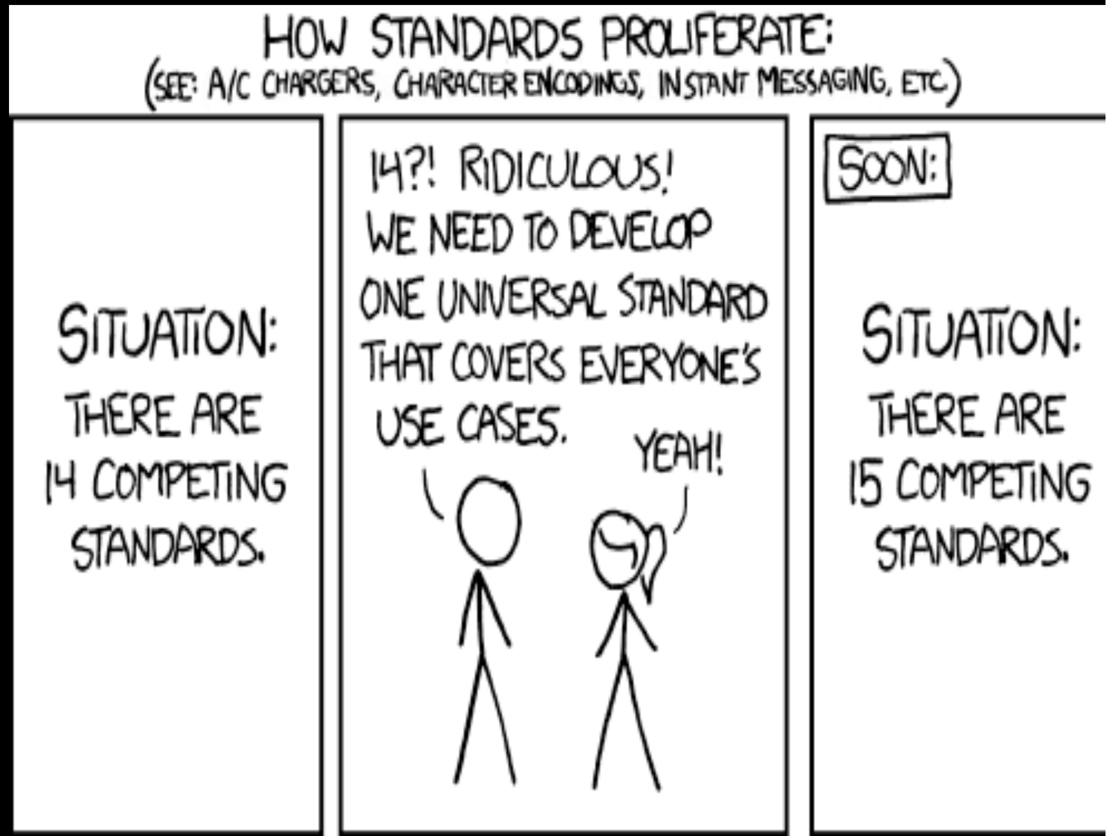
    `13 triggers/1000 iterations`

- Need target-specific development
  - Customized own fuzzer:

    `85 triggers/1000 iterations`

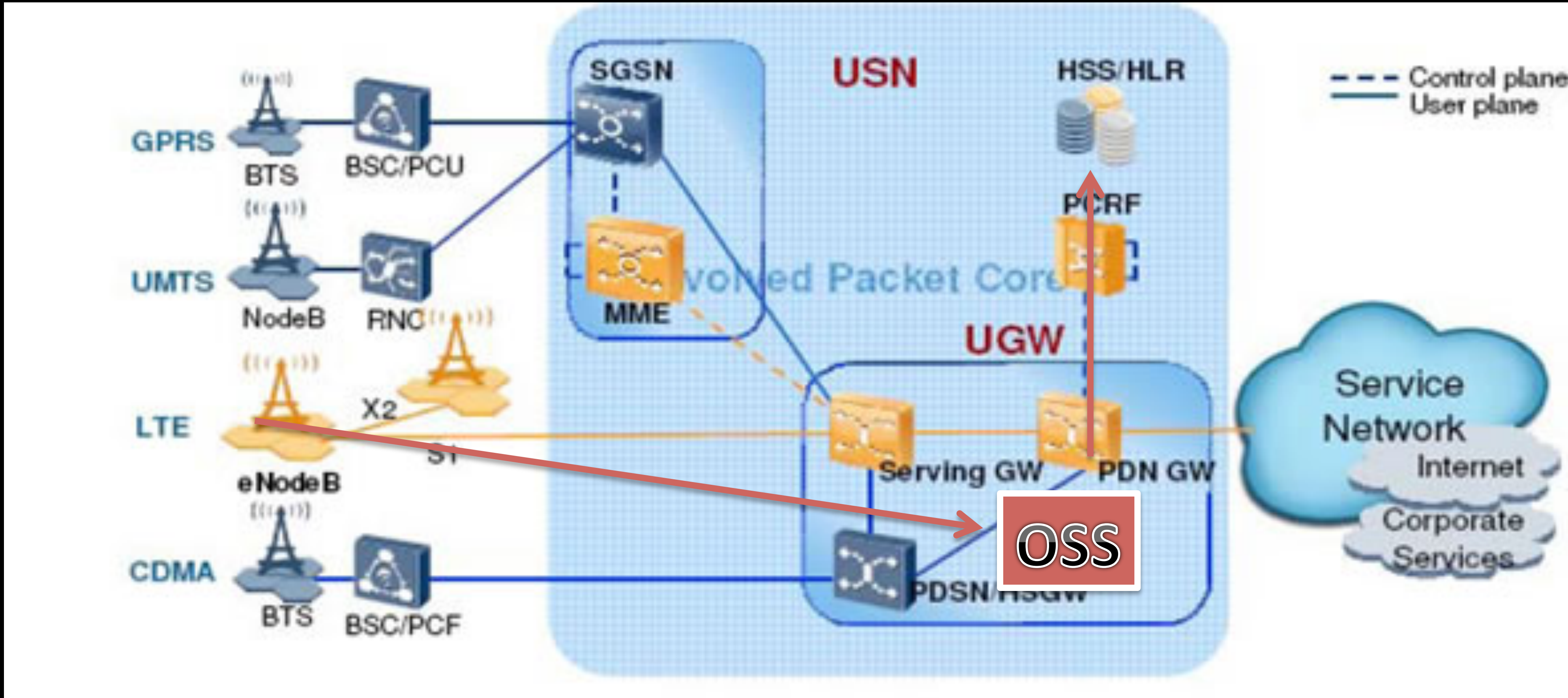
LTE: New risk with Diameter

- Diameter information network dissemination
- Diameter awesomeness
  - distribution/centralization
  - its own evil side
- Present in many database
  - HSS, SDM/SDR, CUD
- The goal was to centralize
- The result is one more database



LTE Huawei Specific

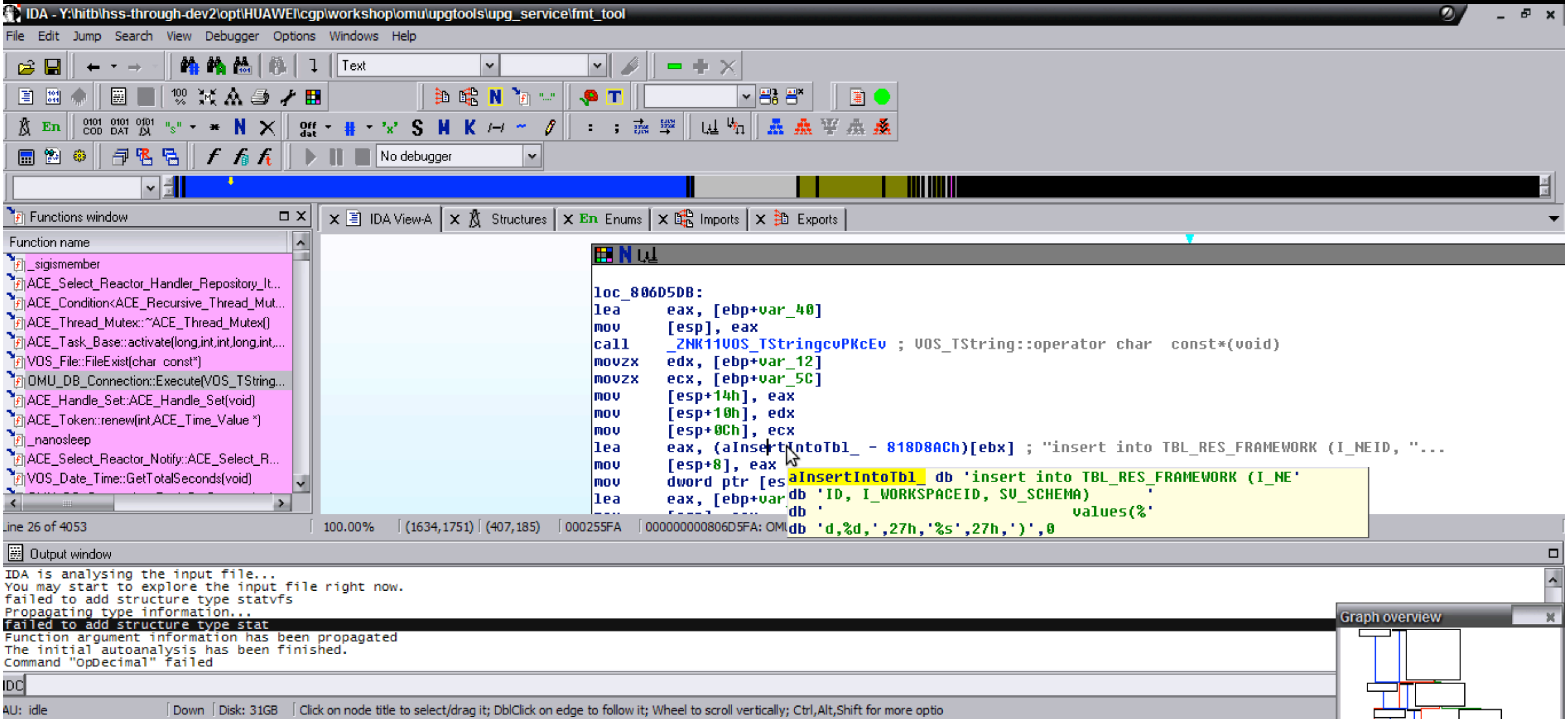
P1 Security
Priority One Security



Source: 3GPP.org

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

Pwning LTE HSS:
C++ SQL Injection everywhere



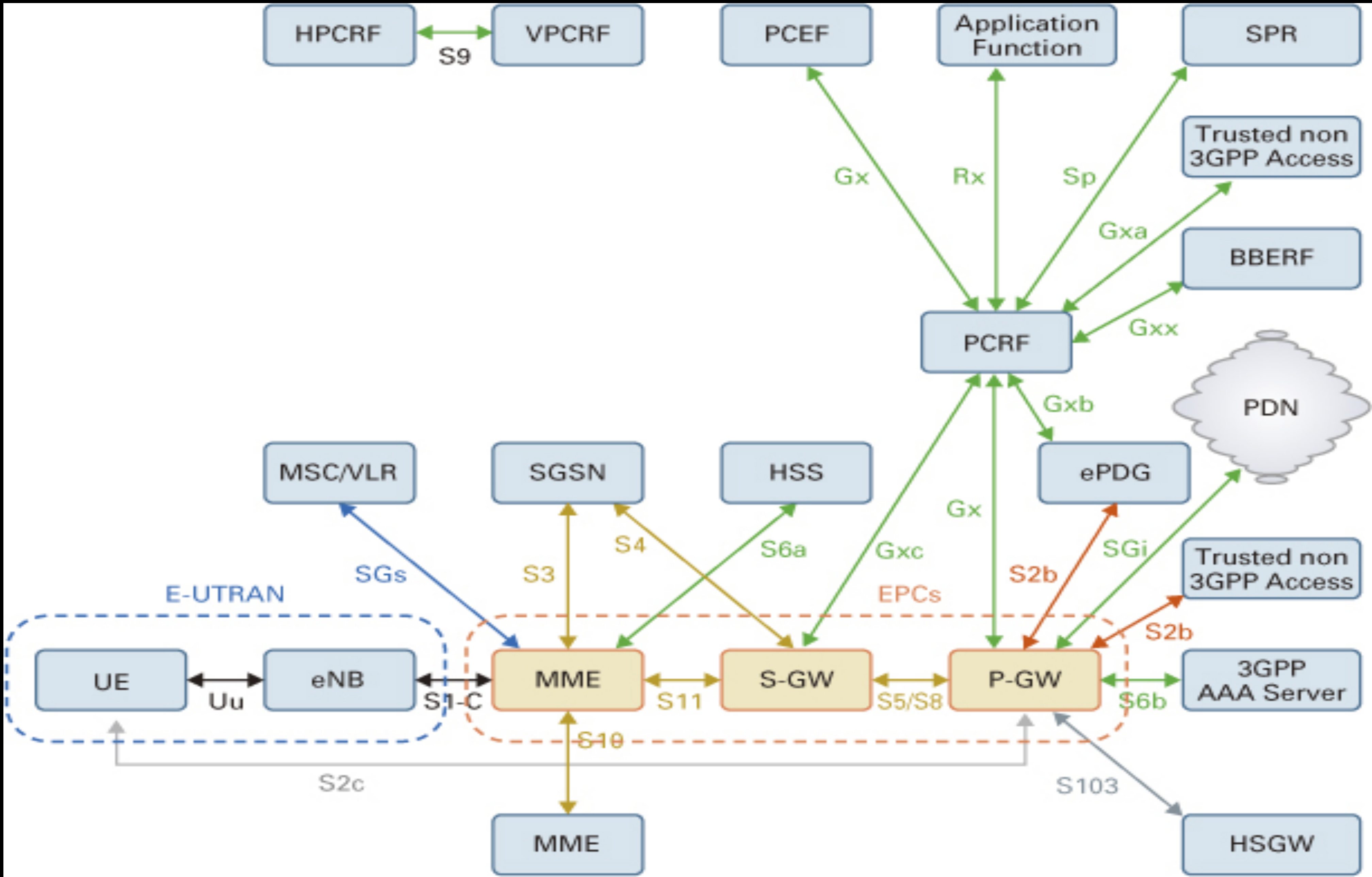
LTE HSS Pwning methodology

- OSS is considered Core
- It is accessible by eNodeBs
  - Sometime: Network filtering mistakes
  - Often: Allowed for Provisionning
- 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 aInsertIntoTbl_ db 'insert into TBL_RES_FRAMEWORK (I_NE'
lea     eax, [ebp+var db 'ID, I_WORKSPACEID, SV_SCHEMA)        '
                      db '                             values(%'
255FA   000000000806D5FA: OM db 'd,%d,',27h,'%s',27h,')',0
```

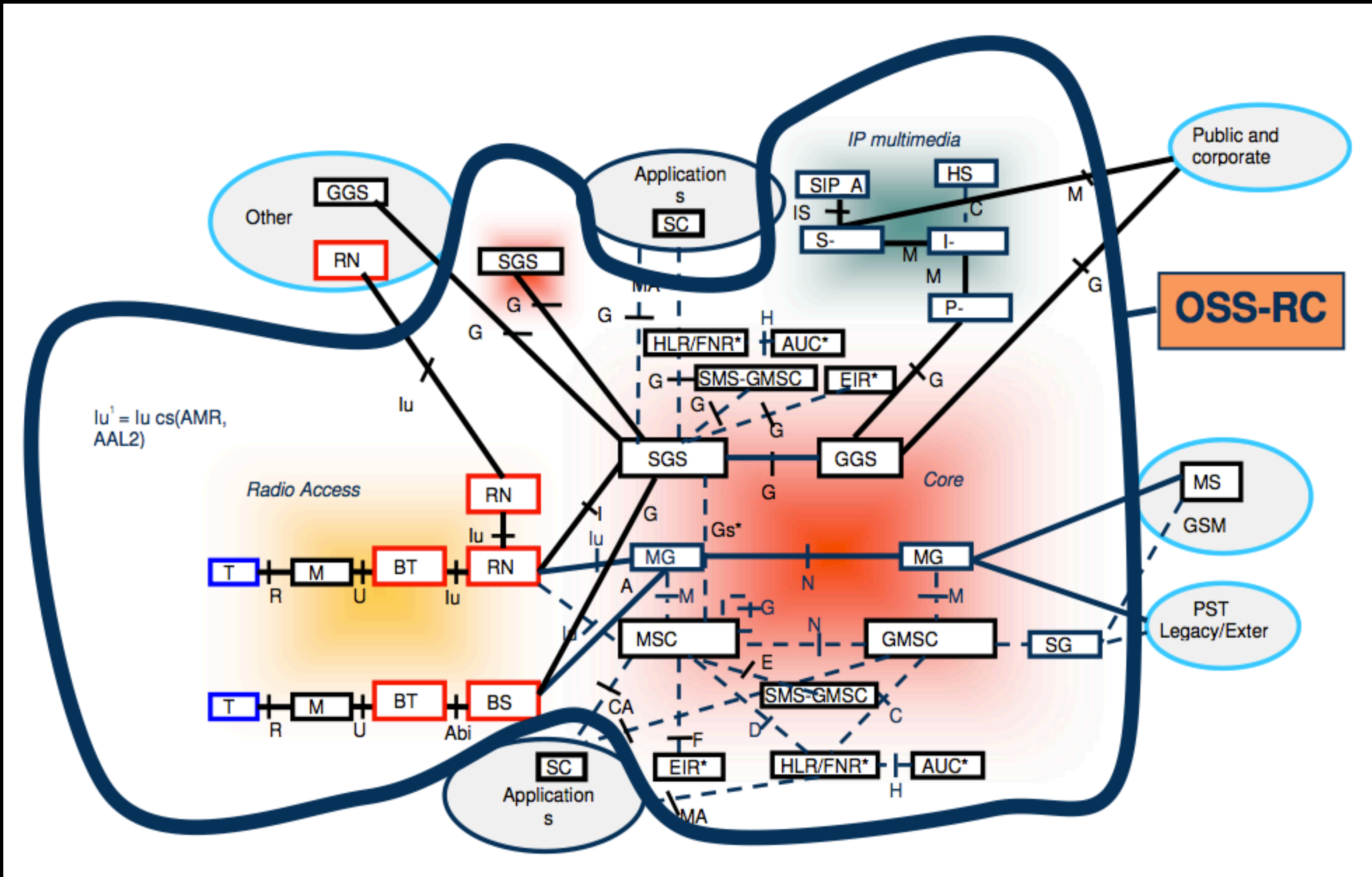
LTE EPC functional plane, no OAM

P1 Security
Priority One Security



Add OAM: complexity explosion

P1 Security
Priority One Security



Auditor bias #3: Manual vision is always incomplete

- Need some automation
- 200 APNs * 16 million IPs == need to have 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

Pwning MME: Hardcoded encryption keys

```java
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;
```

DES… Hardcoded keys everywhere…

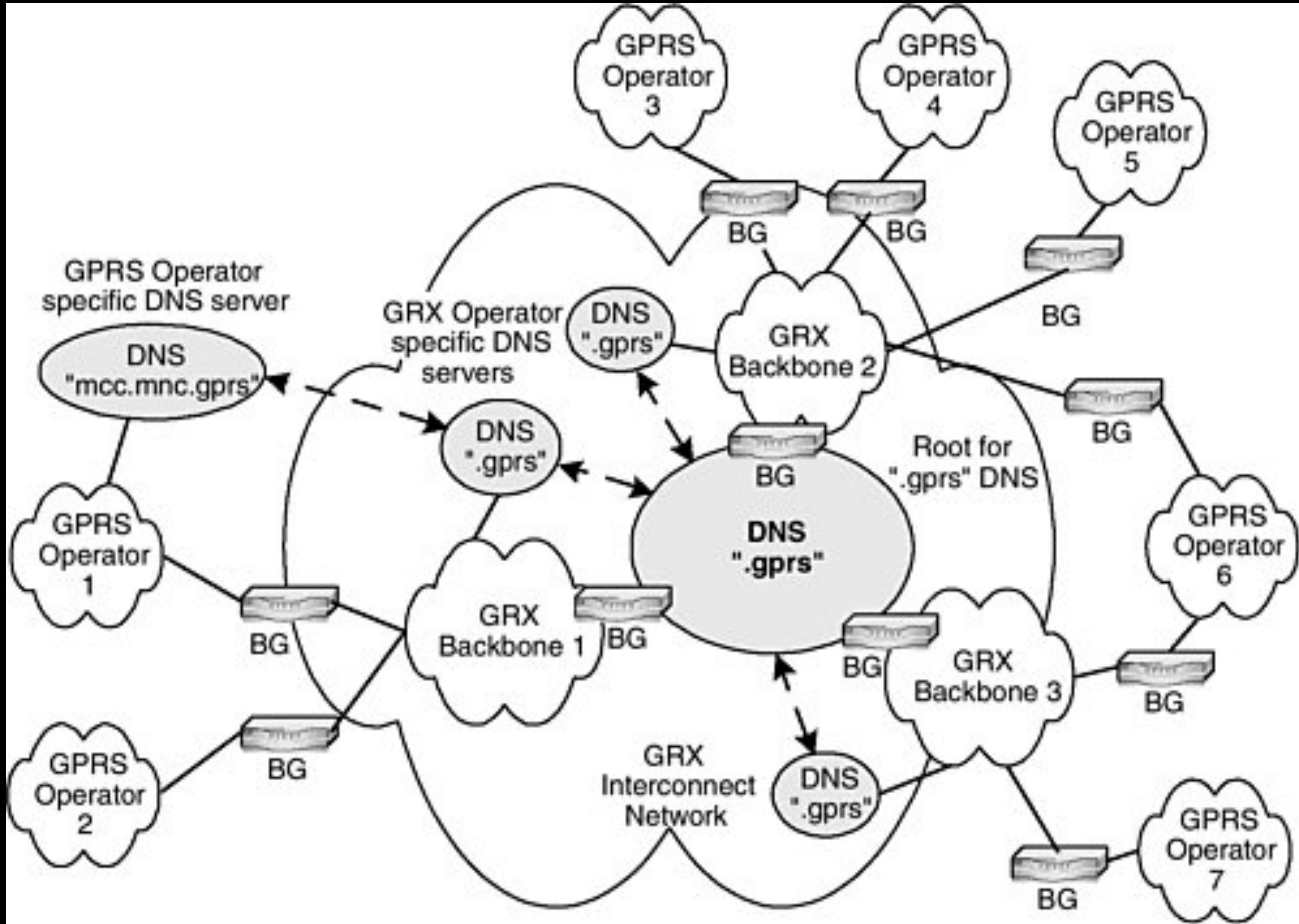
Demo

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)

eDNS vs iDNS

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



Legacy GPRS / UMTS

- GRX
- TLD / Domain .gprs
- Quite monolithic:
  - APN
  - RAI
    - rai<RAI>. mnc08. mcc204.gprs
- Only APNs and “some” network element

IMS DNS

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

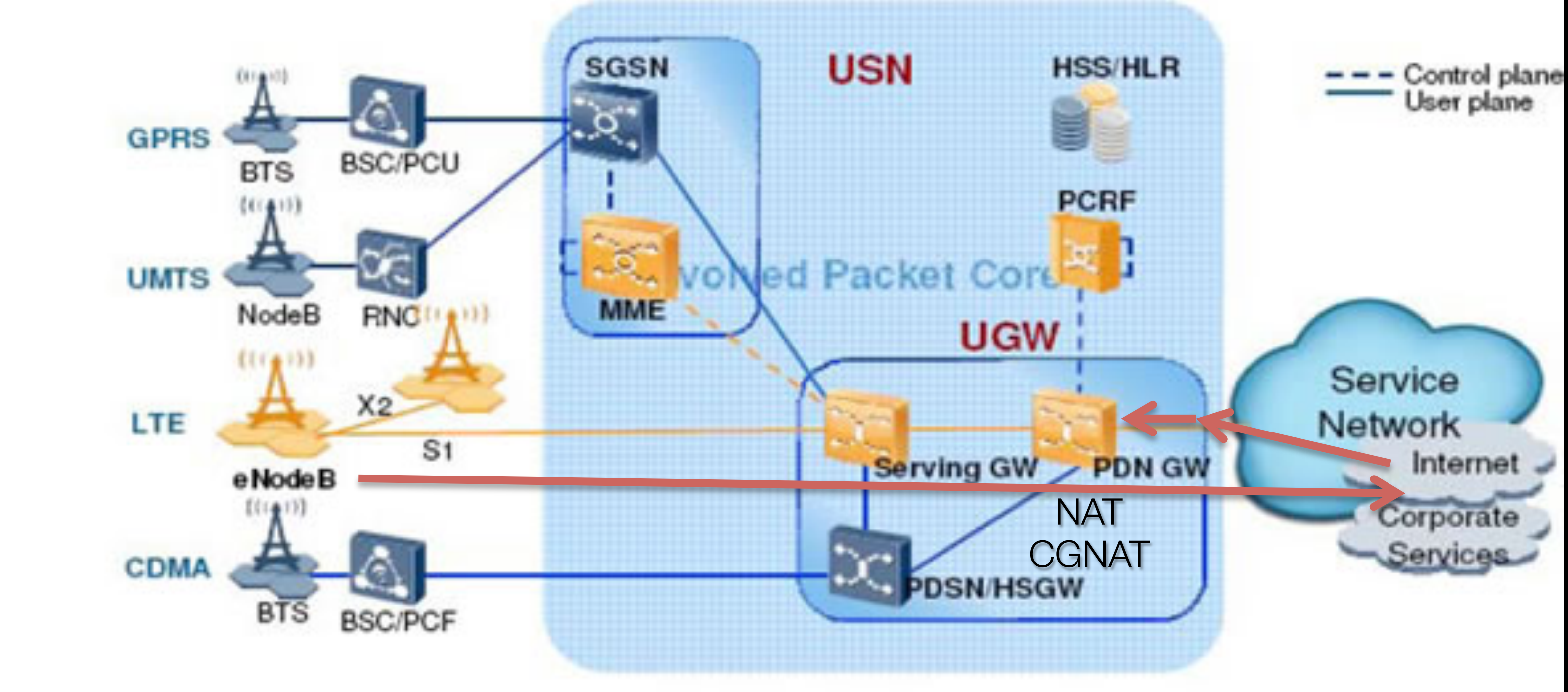
LTE EPC DNS

- Same as IMS DNS but extended
- Supports and lists most SAE EPC Network Elements
  - MME
  - SGW
- Examples

```
mmec<MMEC>.mmegi<MMEGI>.mme.epc.mnc99.mcc208.3gppnetwork.org
```

Pwning from LTE mobile

- Infrastructure Reverse path protection
- LTE Mobile data access
  - RFC1918 leaks (Sometime)
  - Datacom IP infrastructure access (Now more often)



Source: 3GPP.org

Pwning from external: Direct MML access from Internet

- Pwning 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	

Auditor bias #4: Testbed is always more secure

- Testbed is more secure than production
  - Legacy impact
  - Scalability impact
- Audit is often only permitted in testbed
  - Liability
  - Potential for Denial of Service
- Result
  - Attackers advantage
  - Production goes untested

Auditor bias #4: Testbed is always more secure

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

Technical Capacity & Knowledge issue

- Who
  - Can audit all new LTE protocols and legacy protocols
  - Has expertise on the architectures & 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 standardization 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 2013! Unbelievable!
  - Some are getting proactive

Contact:

Philippe.Langlois@p1sec.com
http://www.p1sec.com

THANKS!

SEE YOU AT:
HACKITO ERGO SUM – MAY 2-4 2013
PARIS, FRANCE

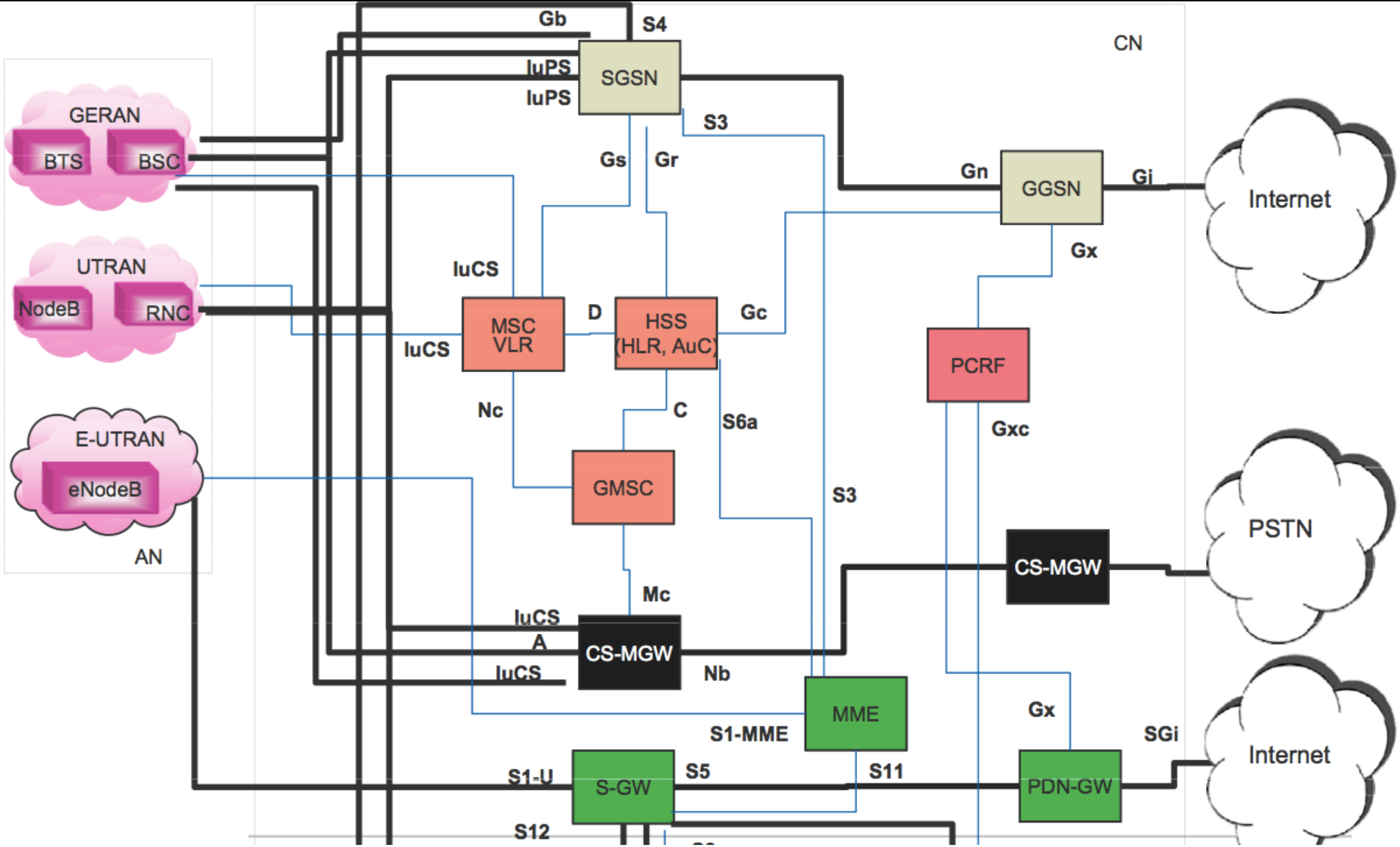
BACKUP SLIDES

Interfaces

P1 Security
Priority One Security

Interface	Endpoints	
S6a	MME	HSS
S6d	HSS	vSGSN (Rel 8)
S13	MME	EIR
S9	hPCRF	vPCRF
Rx	PCRF	AF, P-CSCF
Gx	PGW	PCRF
Gy	PGW	OCF
Gz	PGW	OFCF
Cx	I/S-CSCF	HSS
Sh	AF, IP-SM-GW	HSS
Rf	P/I/S-CSCF, AF	OFCF
Ro	S-CSCF, AF	OCF
Rc	OCF	ABMF
Re	OCF	RF

LTE Network



GERAN
BTS
BSC
UTRAN
NodeB
RNC
E-UTRAN
eNodeB
AN
CN
Gb
S4
IuPS
IuPS
SGSN
S3
Gs
Gr
Gn
GGSN
Gi
Internet
Gx
IuCS
IuCS
MSC
VLR
D
HSS
(HLR, AuC)
Gc
PCRF
Nc
C
S6a
Gxc
GMSC
S3
PSTN
CS-MGW
Mc
IuCS
A
CS-MGW
IuCS
Nb
MME
Gx
S1-MME
SGi
Internet
S1-U
S-GW
S5
S11
PDN-GW
S12

Previous LTE services & missions

- LTE Complete infrastructure audit
- Huawei LTE EPC Core Network audit & vulnerability research
- LTE CSFB infrastructure integration with legacy audit
  - both Diameter, S1, X2 and SS7 integration for CS FallBack
- Ericsson eNodeB audit and product security review
- Diameter security audit on LTE & IMS Core

LTE audit milestones

P1 Security
Priority One Security

1. External LTE testing, scan & audit (blackbox)
   – LTE new elements
   – Integration with legacy
2. LTE eRAN onsite audit
   – eNodeB, enrollment, configuration & PSR/PVR
   – OSS & OAM
3. LTE EPC Core Network audit
   – MME
   – S-GW & PDN GW
   – HSS
   – PCRF
4. MBSS – Minimum Baseline Security Standard
   – LTE eRAN: eNodeB, SeGW, OSS & enrollment servers
   – LTE EPC: MME, S-GW, PCRF, HSS, PDN GW, MSC Proxy

INTERFACES

Interfaces

P1 Security
Priority One Security

Interface	Endpoints	
S6a	MME	HSS
S6d	HSS	vSGSN (Rel 8)
S13	MME	EIR
S9	hPCRF	vPCRF
Rx	PCRF	AF, P-CSCF
Gx	PGW	PCRF
Gy	PGW	OCF
Gz	PGW	OFCF
Cx	I/S-CSCF	HSS
Sh	AF, IP-SM-GW	HSS
Rf	P/I/S-CSCF, AF	OFCF
Ro	S-CSCF, AF	OCF
Rc	OCF	ABMF
Re	OCF	RF

ADDRESSING IN LTE

Core Network: IP addresses everywhere

- Everything uses IP addresses
  – User: UE,
  – RAN: eNodeB, SeGW
  – EPC: MME, HSS, SGW, PGW
- IPv4
- IPv6 is actually really being supported

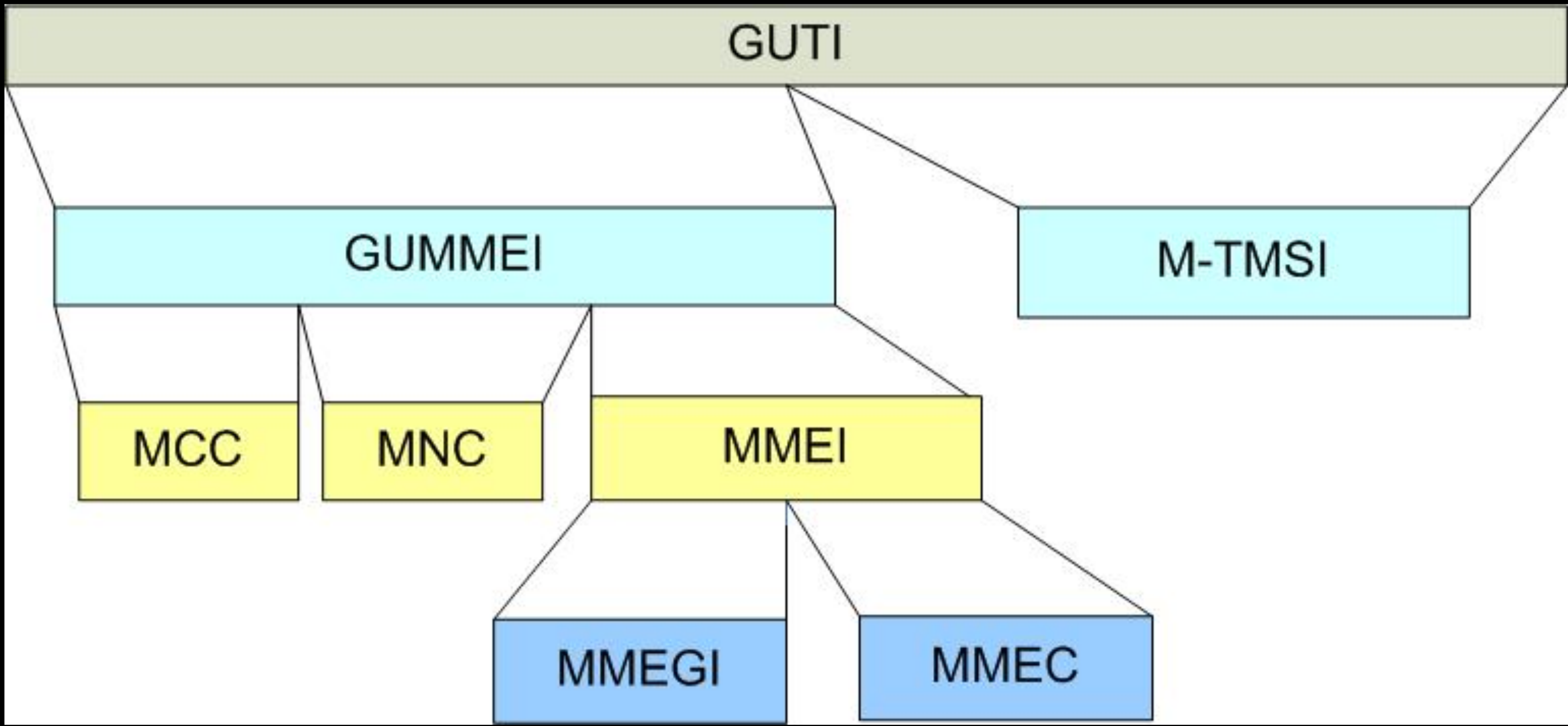
Telecom-specific addressing

- End user addresses:
  - GUTI,
  - IMSI,
  - …

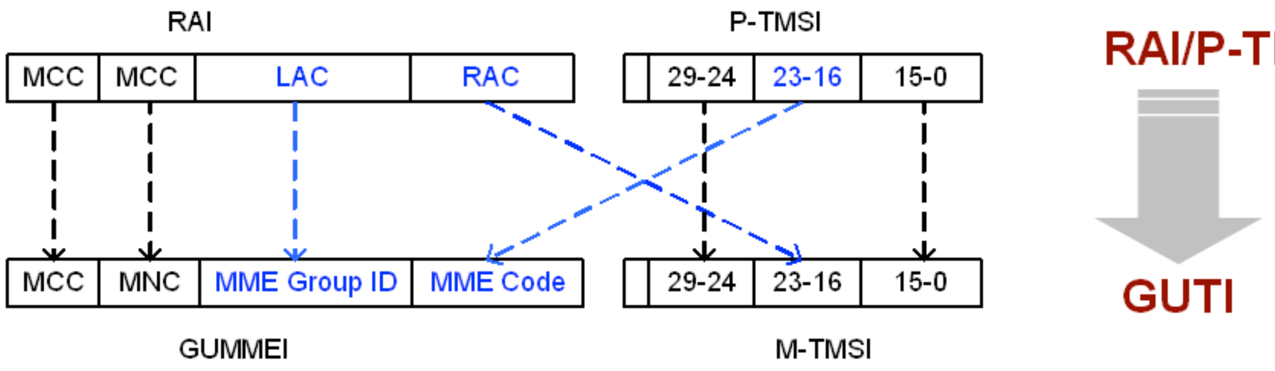
GUTI

- Globally Unique Temporary Identity (GUTI)
  - Allocated by the MME to the UE
- GUTI = GUMMEI + M-TMSI
  - GUMMEI = Globally Unique MME ID
    - GUMMEI = MNC + MCC + MMEI
      - MMEI = MMEGI + MMEC
        - » MMEGI = MME Group ID
        - » MMEC = MME Code
  - M-TMSI == MME TMSI
- GPRS/UMTS P-TMSI -> LTE M-TMSI
- S-TMSI = MMEC + M-TMSI

GUTI in Pictures



RAI/P-TMSI mapping to GUTI

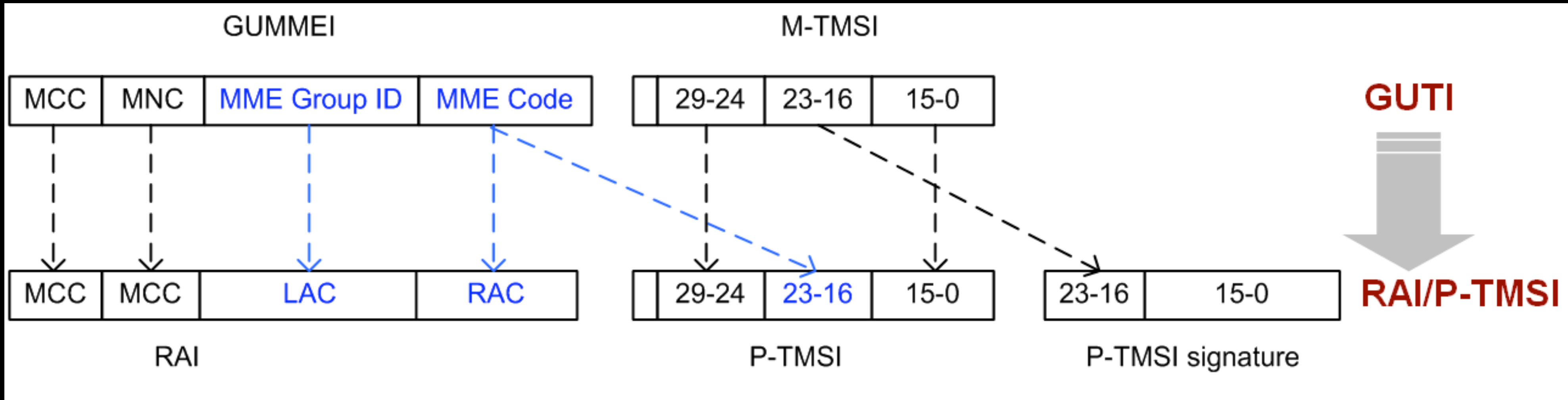


RAI: Routing Area Identity

P-TMSI: Packet Temperate Mobile Subscription Identity

GUTI: Globally Unique Temporary UE Identity

GUTI mapping to P-TMSI



TAC and RNC ID

RNC ID

Octets	8	7	6	5	4	3	2	1
1	MCC digit 2				MCC digit 1			
2	MNC digit 3				MCC digit 3			
3	MNC digit 2				MNC digit 1			
4	Location Area Code (LAC)							
5	Location Area Code (LAC)							
6	Routing Area Code (RAC)							
7 to 8	RNC ID							

eNodeB ID

Octets	8	7	6	5	4	3	2	1
1	MCC digit 2				MCC digit 1			
2	MNC digit 3				MCC digit 3			
3	MNC digit 2				MNC digit 1			
4	Spare				eNodeB ID			
5	eNodeB ID							
6	eNodeB ID							
7 to 8	Tracking Area Code (TAC)							

ADRESS MAPPING IN DNS

Legacy GPRS / UMTS

- GRX
- TLD / Domain .gprs
- Quite monolithic:
  - APN
  - RAI
    - rai<RAI>. mnc08. mcc204.gprs

P1 Security
Priority One Security

IMS DNS

- 3gppnetwork.org
- Supports
  - LAC
  - RAC
- Examples
  - rac<RAC>.lac<LAC>.mnc08.mcc204.gprs

P1 Security
Priority One Security

LTE EPC DNS

- Same as IMS DNS but extended
- Supports
  - MME
  - SGW
- Examples
  - mmec<MMEC>.mmegi<MMEGI>.mme.epc.mnc99.mcc208.3gppnetwork.org

TECHNOLOGY BACKGROUNDER

LTE Data Terminology

- GTP = GPRS Tunneling Protocol
- EPS = Evolved Packet Service, LTE data sessions
- EPC = Evolved Packet Core, the LTE core network
- APN = Access Point Name (same as 2G/3G)
- Bearer = PDP session, GTP Tunnel for a given used
- SeGW = Security Gateway, segments eNB / EPC
- SGW = Serving Gateway, like GGSN, connects to Internet

PDP Context vs. EPS Bearer

- UMTS and GPRS data session
  - Packet Data Protocol (PDP) Context
  - Attach (Alert SGSN) -> PDP Context Activation procedure
- LTE data session
  - Evolved Packet System (EPS) Bearer
    - Default EPS Bearer
    - Dedicated EPS Bearer
- Both use parameters:
  - Access Point Name (APN),
  - IP address type,
  - QoS parameters

LTE GTP = eGTP

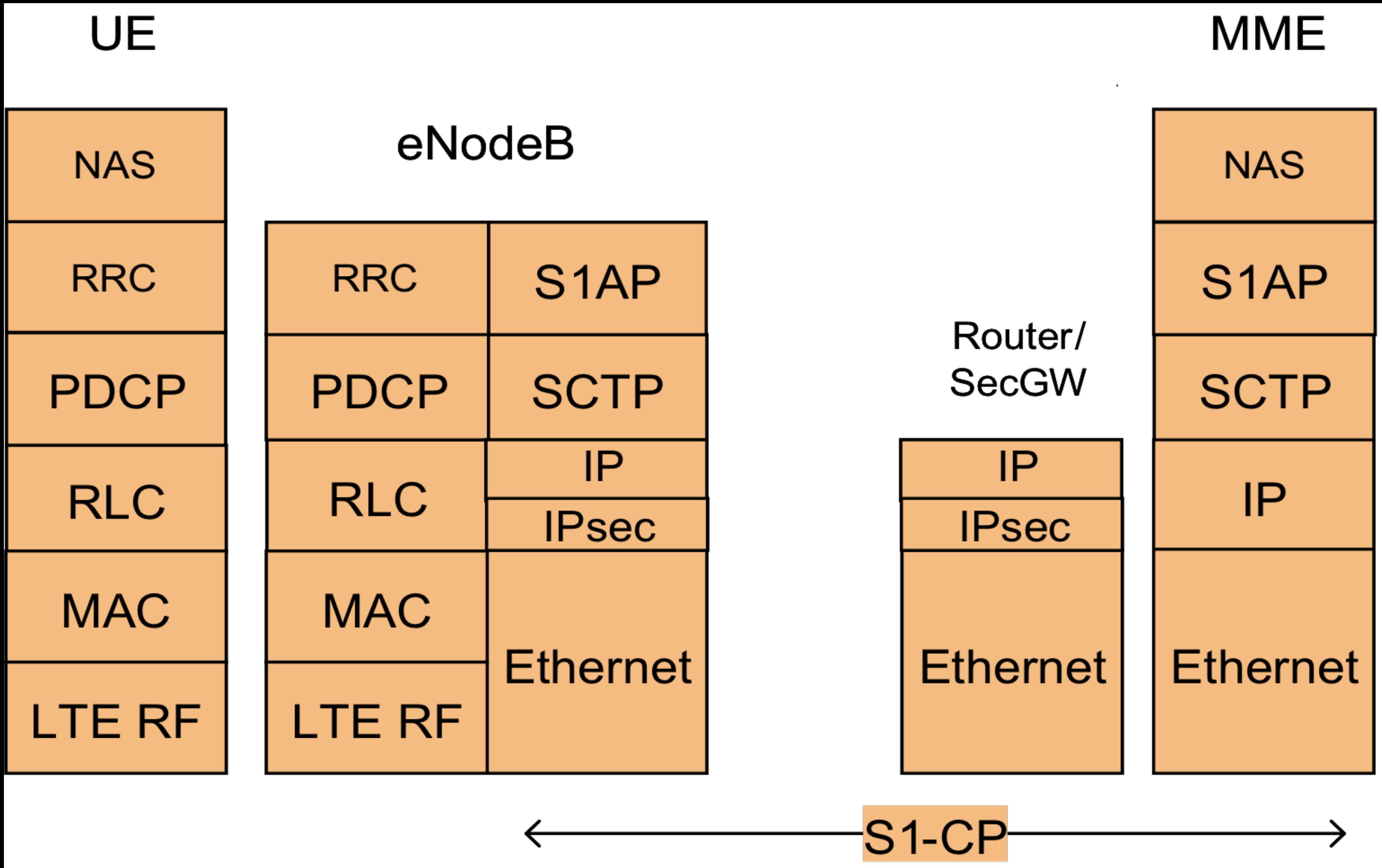
- GTP-U
- From eNodeB to PDN GW
  - PGW
  - aka Internet exit node
  - Used to be the GGSN

GTP-U

- udp/*2152*

LTE Control Plane: eNodeB-MME

P1 Security
Priority One Security

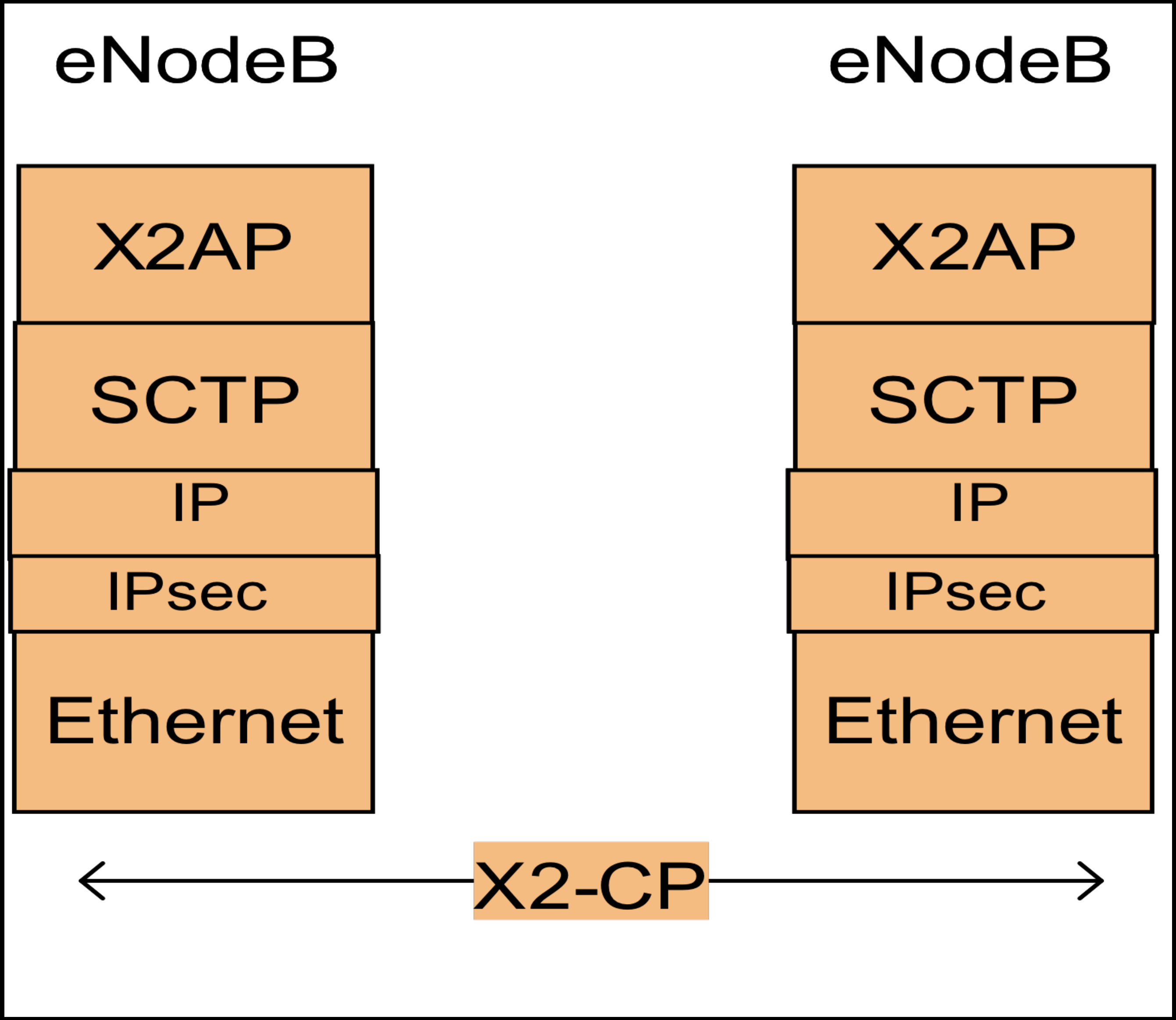


S1AP

- sctp/36412

LTE Control Plane: eNodeB-eNodeB

P1 Security
Priority One Security



X2AP

- sctp/36422

Protocol and port matrix

Communicating nodes		Protocol	Protocol ports	
Source	Destination		Source	Destination
eNodeB	S-GW	GTP-U/UDP	2152	2152
S-GW	eNodeB	GTP-U/UDP	2152	2152
eNodeB	eNodeB	GTP-U/UDP	2152	2152
eNodeB	MME	S1AP/SCTP	36422	36412
MME	eNodeB	S1AP/SCTP	36412	36422
eNodeB	eNodeB	X2AP/SCTP	36422	36422

All is ASN1

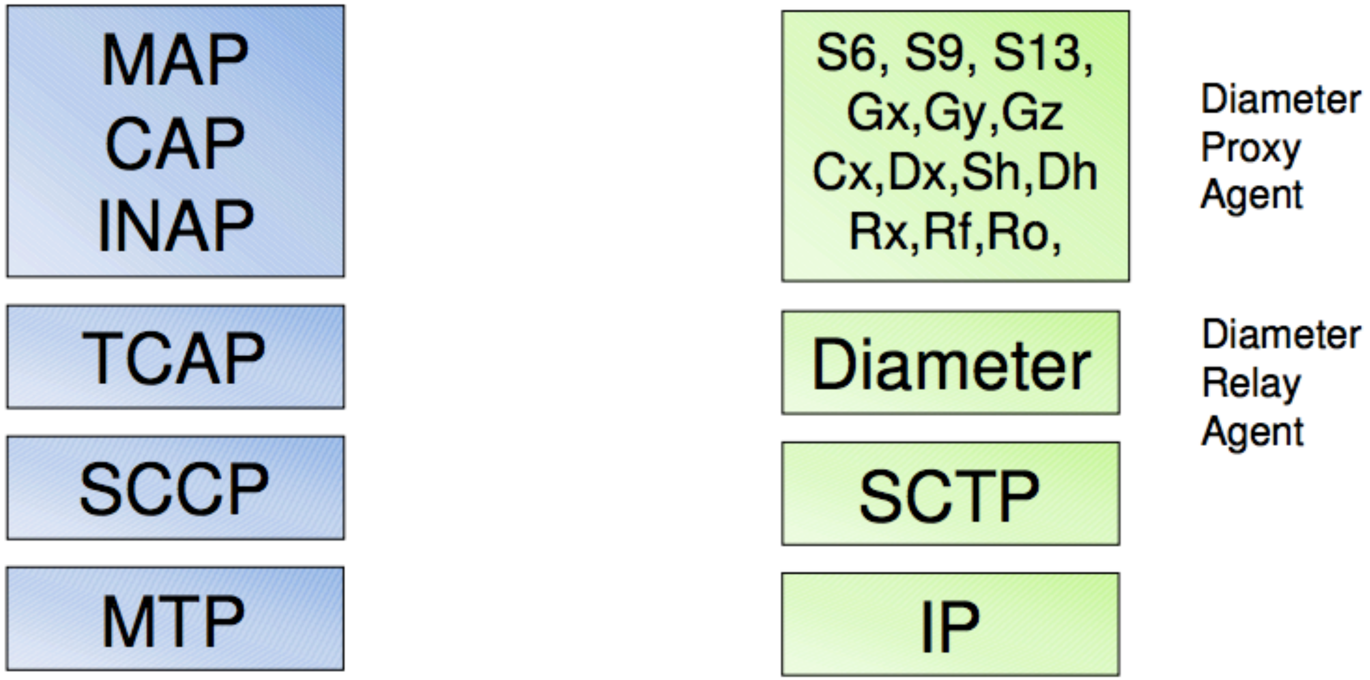
- All protocols described in ASN1
  - Different kind of Encoding
    - BER – Basic, standard TLV
    - PER – Packed,
      - Aligned (APER)
      - Unaligned (UPER)
  - Described in ITU and 3GPP standards
  - Require ASN1 “CLASS” keywords

LTE SIGNALING

Diameter Everywhere

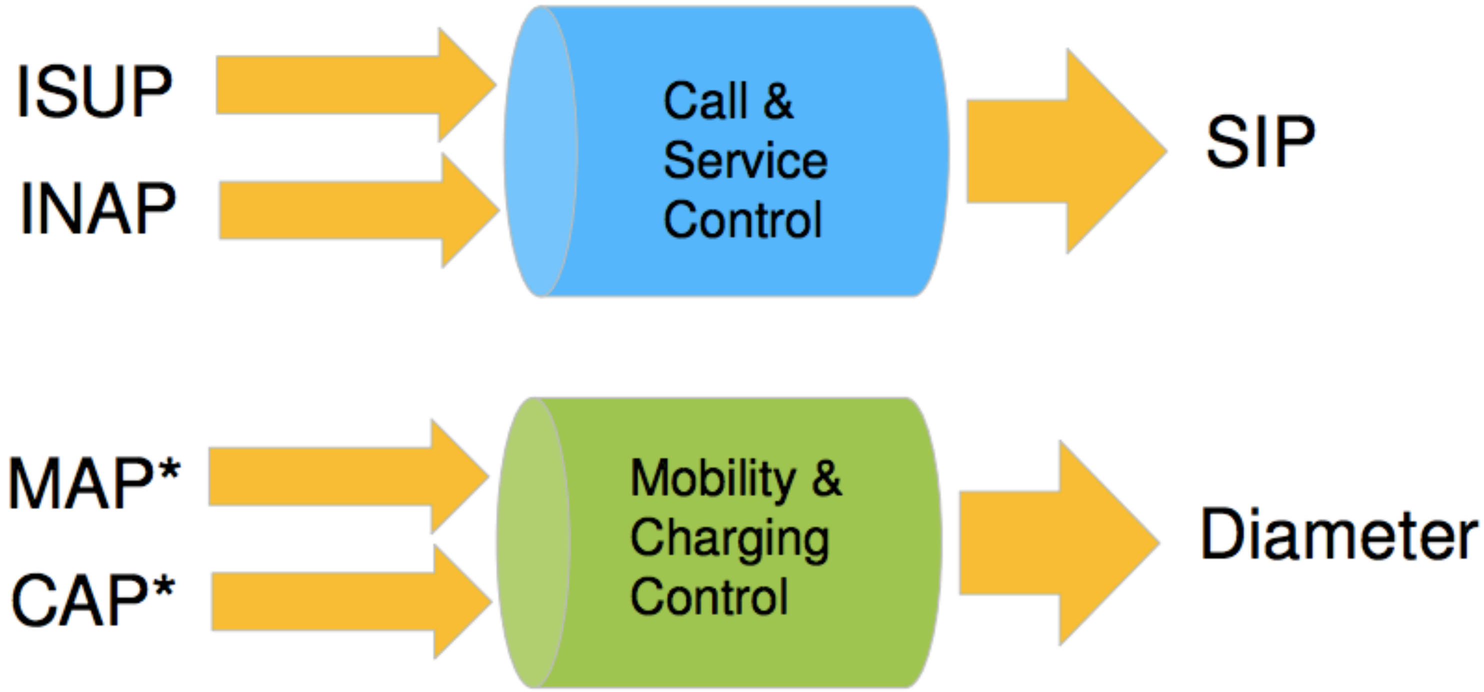
- Diameter replaces SS7 MAP
- DSR
  - Diameter Signaling Router

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

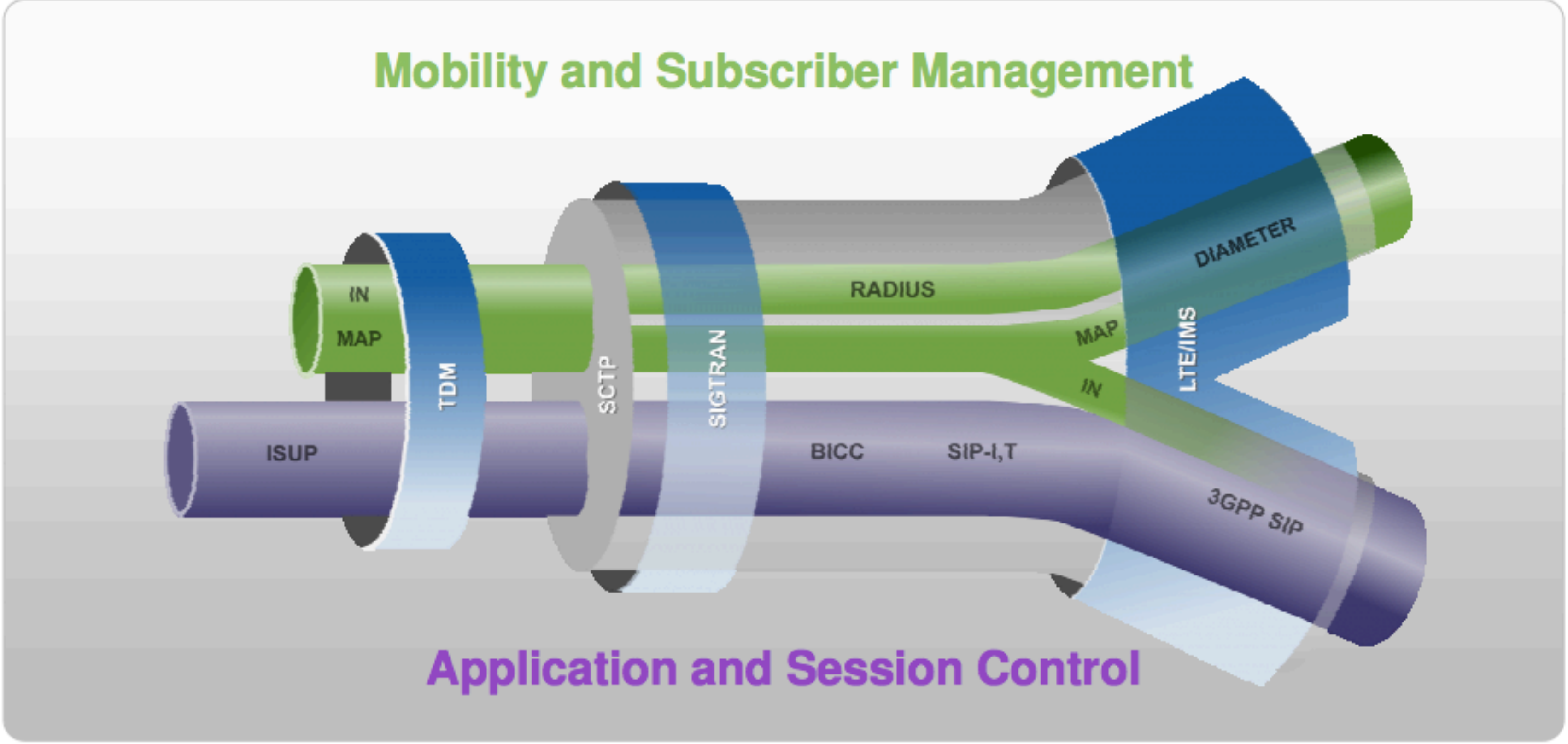


- CAP* - 2G/3G CAMEL prepaid functions in future via Diameter, VAS functions of CAMEL via SIP (= INAP)
- MAP* - AAA and mobility in future via Diameter, Messaging (SMS) via SIP

P1 Security
Priority One Security

Signaling Protocol Evolution

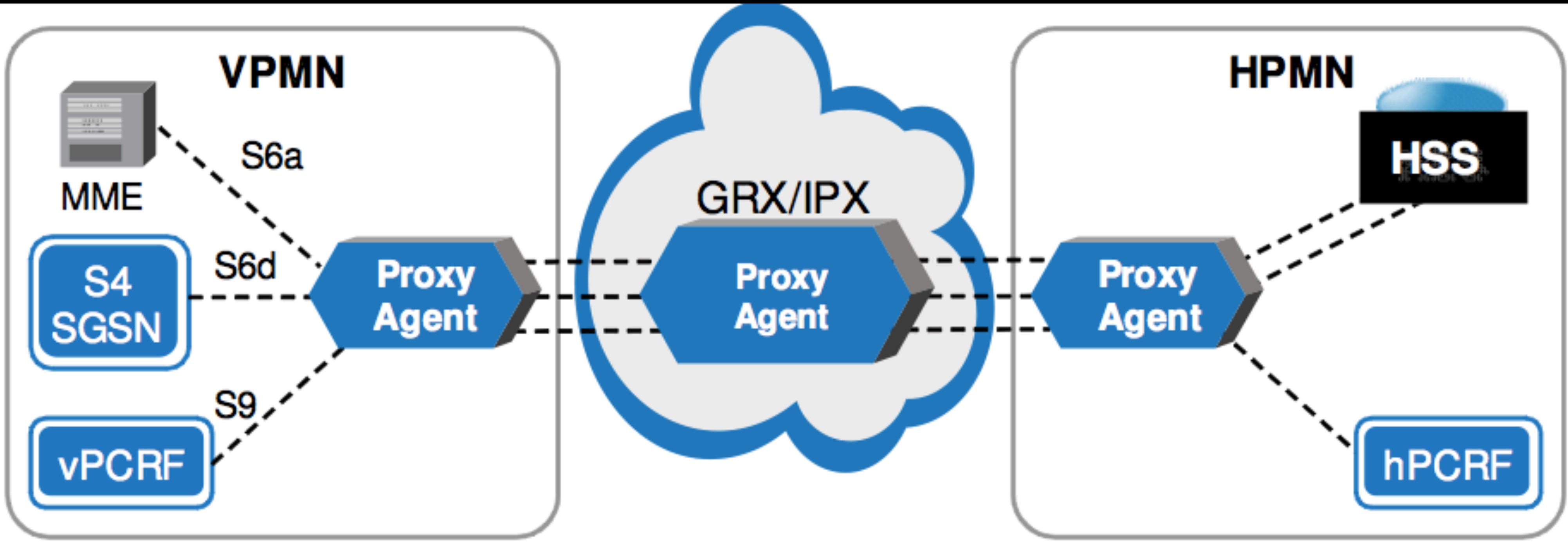
- Diameter and SIP become the dominant signaling protocols
- SCTP “point-to-point” connections remain



Security implication

- SCTP filtering to be generalized
- Benefit
  – SCTP is "config first" most of the time
- Threat
  – IP cloud is much more exploitation friendly
  – Attack techniques are known to many people
  – Compromise consequences are more far-reaching than SS7

Diameter Roaming



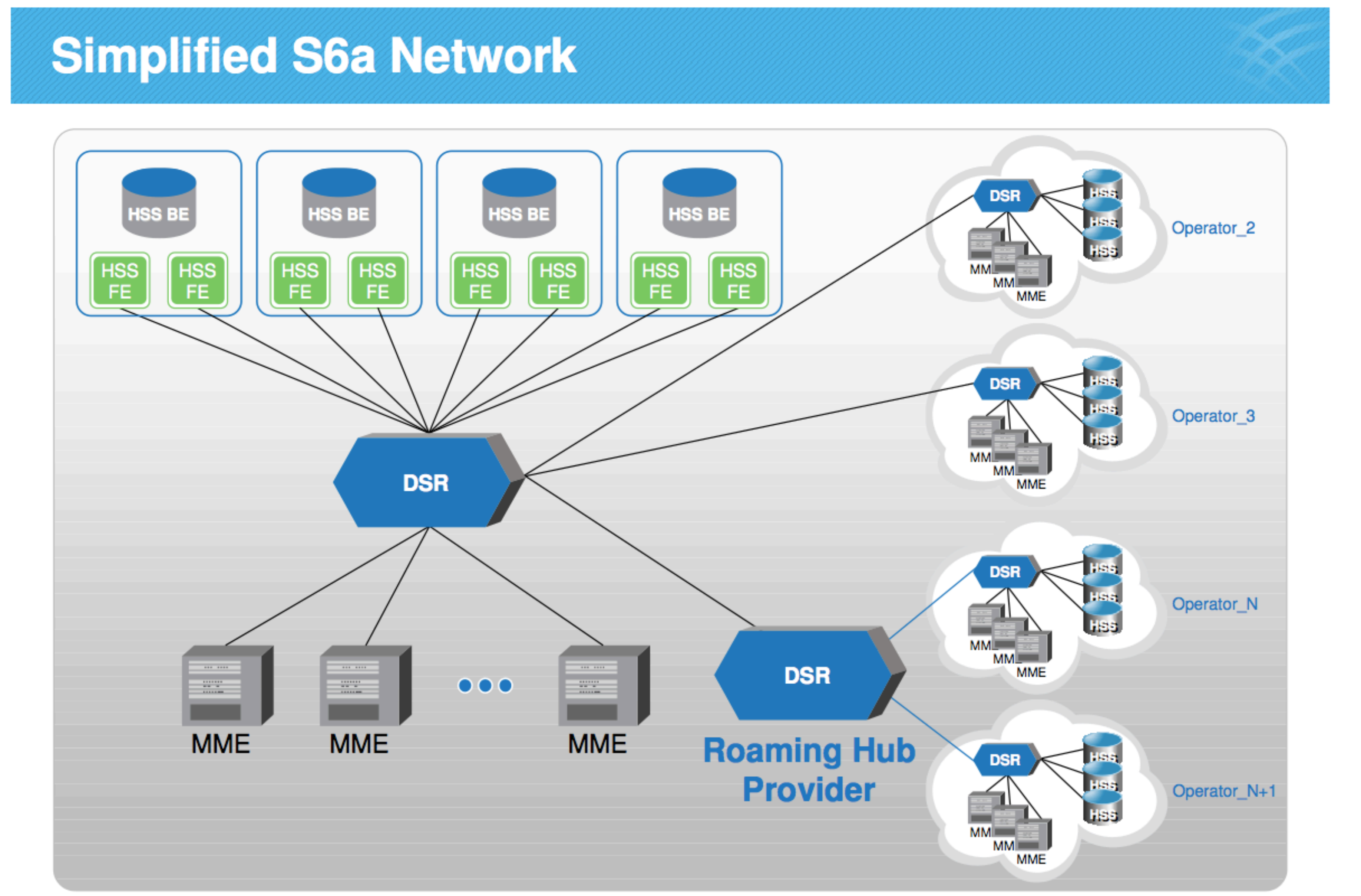
P1 Security
Priority One Security

Security routing and filtering in Diameter

- DSR
  - Define routing & filtering rules
- Discriminants Indicators
  - Destination-based:
    - Realm, Host, Application-ID
  - Origination-based:
    - Realm, Host, Application-ID
  - Command-Code
  - IMSIAddress

Future Diameter Routing & Filtering

P1 Security
Priority One Security



P1 Security
Priority One Security

Security & Vulnerability of EPC Roaming

- Filtering even more important
  - DSR filtering is not mature
- GRX problems amplified
  - Impact of the GRX/IPX/IMS/SAE EPC DNS infrastructure in Information Gathering
- Unique Identifier leaks much easier
  - Privacy consequences

P1 Security
Priority One Security

TESTING

Testing Security in an LTE Environment

- Two kind of environment
  - Testbed
  - Live (also called Production, Greenfield, Active)

P1 Security
Priority One Security

LTE Testbed Security testing

- Shielded testing
  - eNodeB antenna output connected to a cable
  - Cable arrives in test room
  - A “Shielded box” in test room is connected to cable
  - Phone / USB dongle is put inside the box for tests
  - USB cable goes out of the box toward the test PC
- No RF is polluting the spectrum
  - Enables pre-auction testing

Relationship to Vendors

P1 Security
Priority One Security

- Vendor usually prevent audit
  - By limiting information
  - By limiting access to Device Under Test
  - By limiting access to testbed
  - By threatening of potential problems, delays, responsibility, liability
- Most of the LTE testing can happen transparently
  - The vendor doesn't see the security audit team
  - Presented as normal operator qualification
  - Not presented as security audit
- Result only is presented when audit is finished

AUDITS

GTP

P1 Security
Priority One Security

- Endpoint discovery
- Illegal connection/association establishment
  - User identity impersonation
  - Fuzzing
- Leak of user traffic
  - to Core Network (EPC)
  - to LTE RAN

X2AP Audit

- Endpoint discovery
- Illegal connection/association establishment
  - Fuzzing
- Reverse engineering of proprietary extensions
- MITM

S1AP Audit

- Endpoint discovery
- Illegal connection/association establishment
  - Fuzzing
- Reverse engineering of proprietary extensions
- MITM
  - NAS injection

LTE EPC DNS Audit

- EPC DNS is important
- EPC DNS scanner
- Close to GRX / IMS

ATTACKS

User attacks: EPS Bearer Security Attacks

P1 Security
Priority One Security

- APN Bruteforcing
- IP Segmentation
  - accessing operators' RFC1918 internal networks
- GTP endpoint discovery
  - from within Bearer Data Session
- Secondary EPS Bearer Exhaustion/Flood load DoS
  - Max 11 to be tested
  - Repeat setup/teardown of connections
- PGW DiffServ testing
  - Scans the IP header DS bits (Differentiated Services) to see difference in treatment by PGW

P1 Security
Priority One Security

TOOLS

Basic audit tools

- LTE SIM card
- LTE USB Dongle
- LTE UE (User Equipment) = Phone
- RJ45 for Ethernet connection to EPC/EUTRAN
- Wireshark
- Sakis3G and evolutions for LTE support
- IPsec audit tool

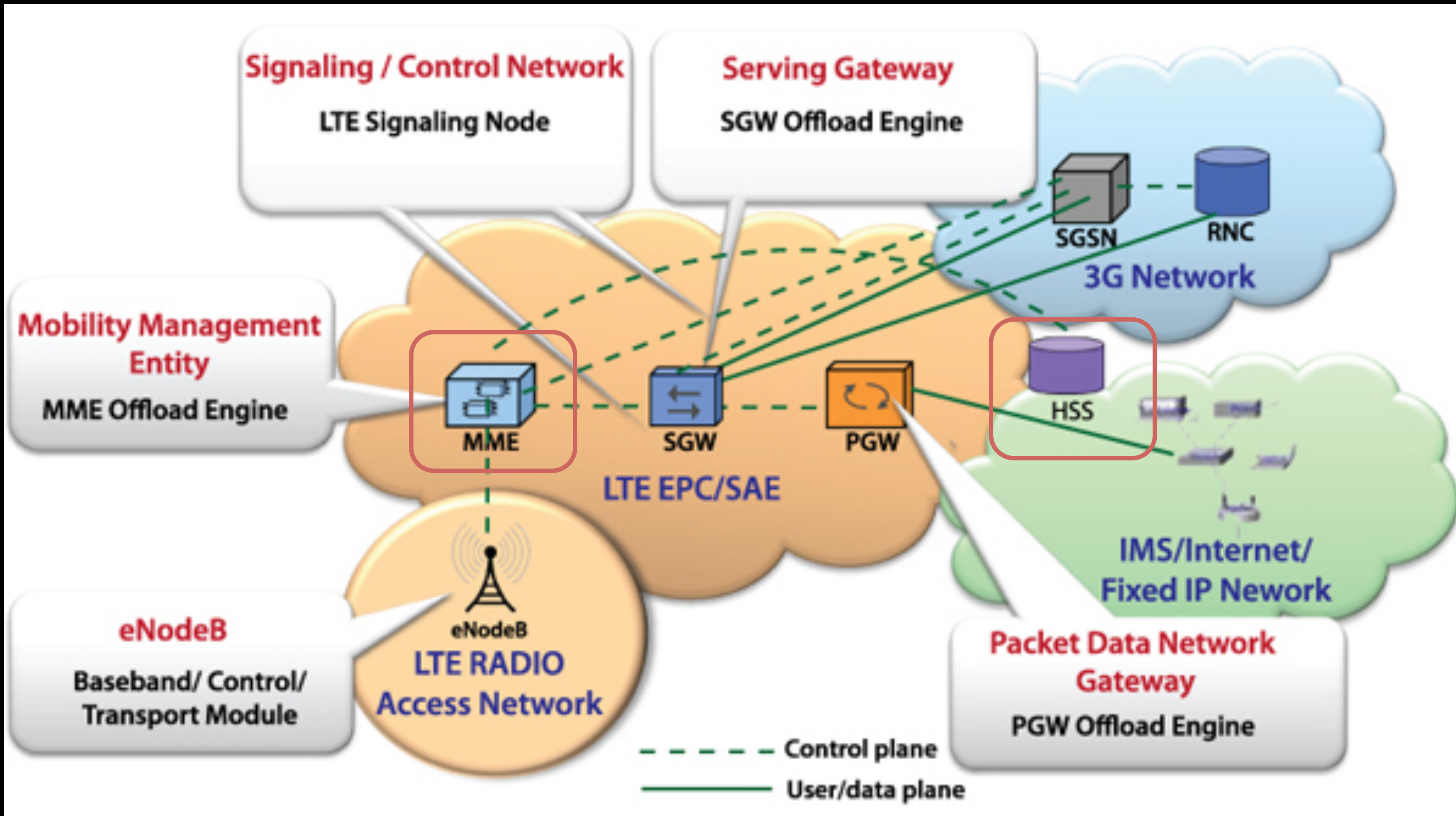
Ideal audit tools

- GTP protocol stack & fuzzer
- SCTP MITM tool & fuzzer
- Ethernet/ARP MITM tool (ettercap)
- S1AP protocol stack & fuzzer
- NAS protocol stack & fuzzer
- X2AP protocol stack & fuzzer
- Diameter protocol stack & fuzzer
- GRX, IMS, EPC DNS scanner

Virtualization targets

- Huawei
  - In progress
    - HSS
    - MSC Proxy
  - Potential
    - USN, Serving GW, PDN GW, MME
  - eHRS integrated node (MME, HSS, SGW, PGW, …)
    - Easier because one single node
- HP opportunity?

LTE Network Virtualization



Huawei ATCA vs. PGP

- OSTA 2.0
  - Linux based
    - OpenSuse 10.x or 11.x
    - Old, unpatched kernel
    - Proprietary extensions and SMP
  - Some FPGA based boards
  - Some OEM based integration (Switches AR40, Routers, …)
- PGP
  - Older architecture
  - More monolithic
  - Harder to replicate

P1 Security
Priority One Security

Hard problems

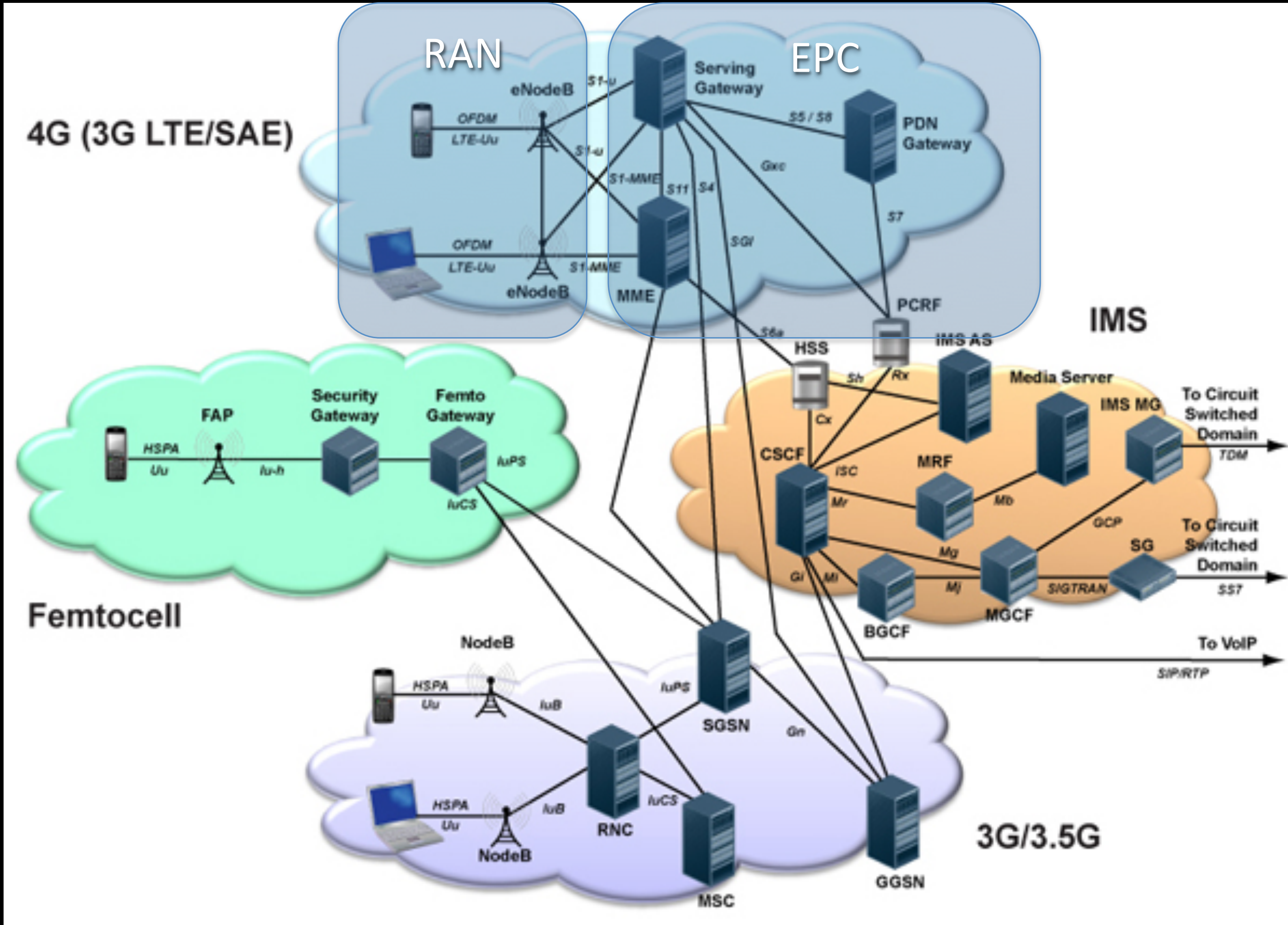
- Use same kernel (medium)
- Use licensing (medium)
- Load signed kernel modules (medium hard)
- Emulate FPGA and OEM integration (hard)
- Replicate network services / other NEs (hard)

HSS

- ATCA / OSTA 2.0
- Few external hardware
- Moderately easy
- Operation in progress
- Based on HSS_V900R003

Virtualizing in context (CSFB)

P1 Security
Priority One Security



P1 Security
Priority One Security

MSC Proxy

- ATCA / OSTA 2.0
- No external hardware
- Moderately easy
- Configuration with
  - existing SS7 SIGTRAN infrastructure
  - Diameter testbed

USN

- USN_V900R011C02SPC100
- Harder

Ericsson

- Difficult to deal with them
- Very protective
  - Access
  - Licensing
  - Documentation

P1 Security
Priority One Security

NSN

- Potentially easier than Ericsson
- Linux based (SGSN, …)
  - MontaVista
- Some security features

Cisco

- Some virtualization done
  - IOS 12.x
- Some virtualization needs hardware
  - Cisco 7200
  - Cisco ITP
  - Cisco GGSN
- Virtual networking
- Our technology for adapted virtualization

Our advantage so far

- Virtualize x86 with specific/signed kernels and modules
- Virtualize MIPS
- Emulation of specific hardware support
  - Kernel modules development
- Virtualize ARM Android based device
  - for customer simulation

Mobile + VAS virtualization

- Specific demand from customer
  - Virtualize x86 based server
  - Virtualize 10-20 Android clients
  - Simulate fraudulent transaction within this flow
  - Inject faults within repeated traffic

VIRTUALIZED SIGNALING FUZZING

Principle

- Proxies
  - M3UA Proxy
  - S1/X2 Proxy
  - Diameter Proxy
- Made transparent
  - SCTP Man in the Middle
  - Packet forwarding

LTE increases risks

- Financial theft
- Privacy theft
- Hacking of corporate users
- M2M impact of worms and attacks
- LTE Mobile broadband usage as main internet connection
- Protocols are untested and traditional fuzzer coverage is weak and shallow
- Network equipment is new and not as reliable as traditional network elements

Questions ?