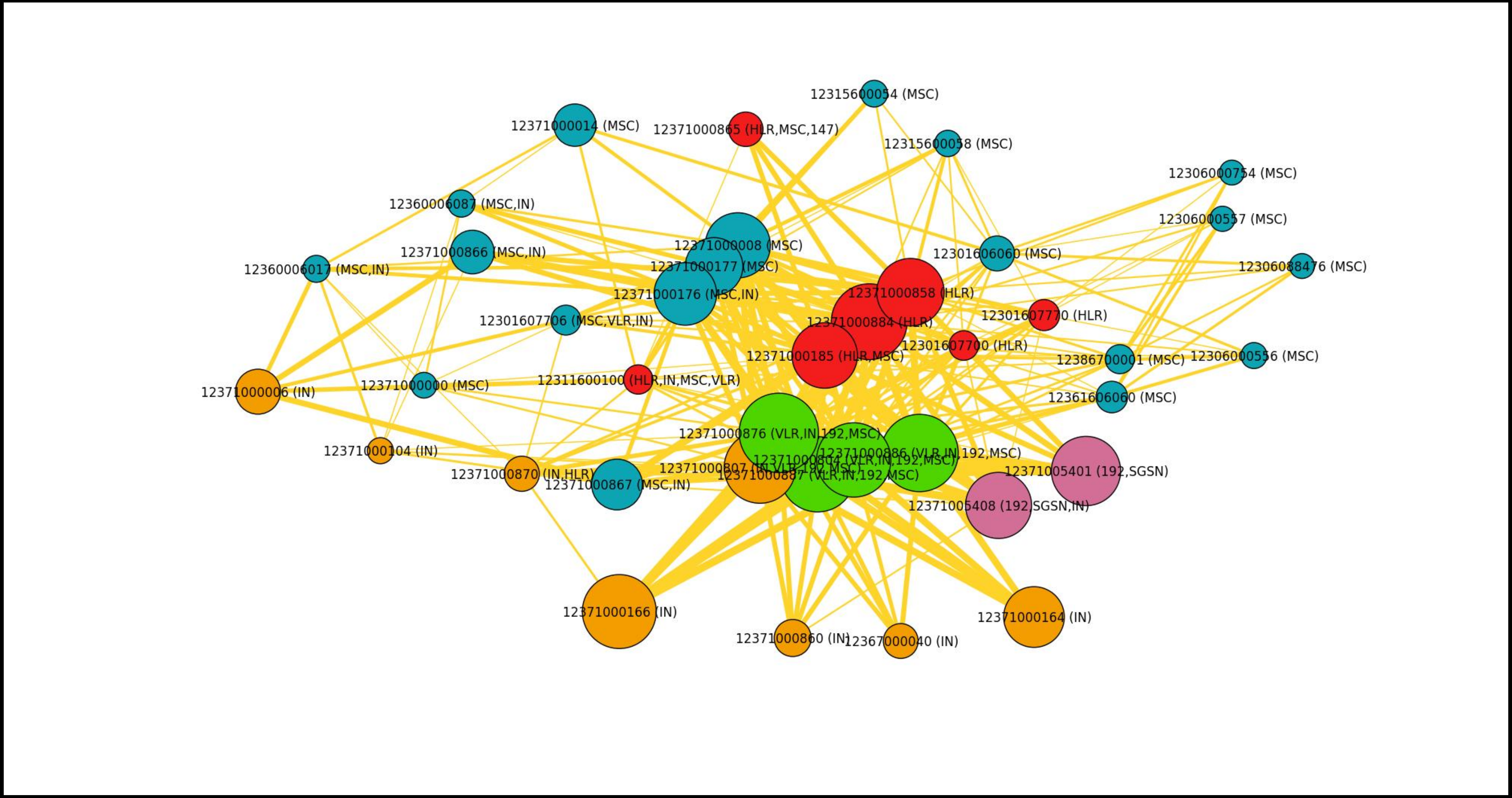
P1 Security
Priority One Security

Hacking Telco equipment
The HLR/HSS

Laurent Ghigonis

Security researcher at P1 Security

What are we talking about ?



A mobile network operator Core Network

Network passive capture showing Global Titles

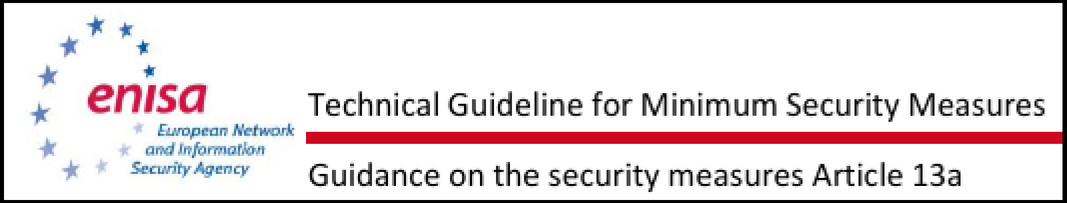
Mobile Operators

- Conveys the majority of voice communications worldwide
- Conveys our data
- Conveys growing M2M traffic
- Emergency systems notifications uses it

=> We now rely on it and we have some security expectations

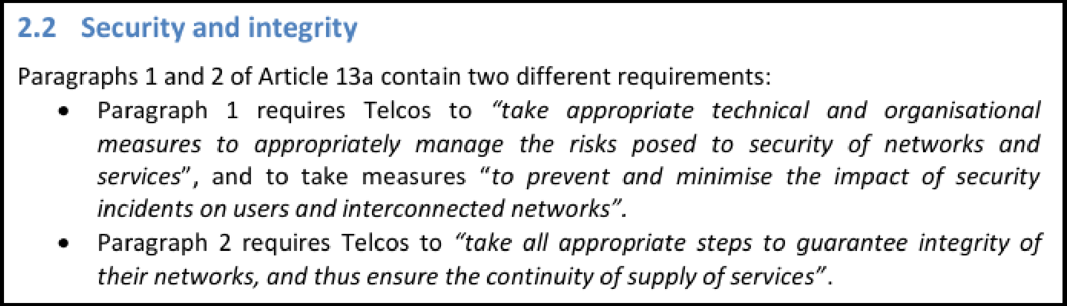
Mobile Operators and governance

- In Europe



Technical Guideline for Minimum Security Measures

Guidance on the security measures Article 13a

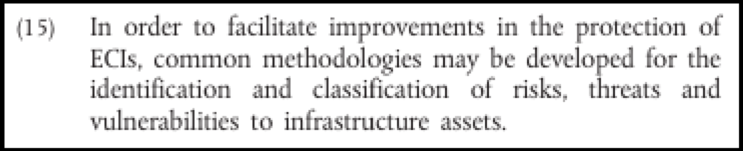


2.2 Security and integrity

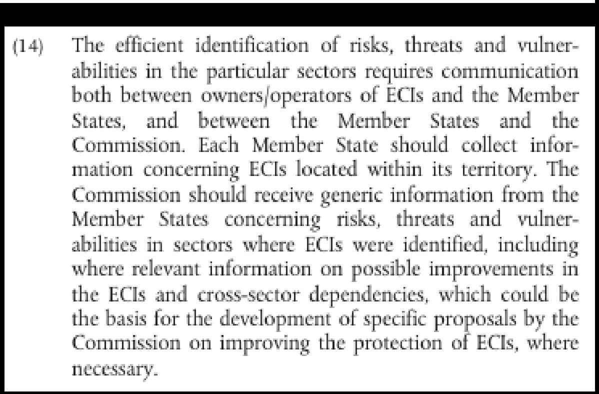
Paragraphs 1 and 2 of Article 13a contain two different requirements:

- Paragraph 1 requires Telcos to *"take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services"*, and to take measures *"to prevent and minimise the impact of security incidents on users and interconnected networks"*.
- Paragraph 2 requires Telcos to *"take all appropriate steps to guarantee integrity of their networks, and thus ensure the continuity of supply of services"*.

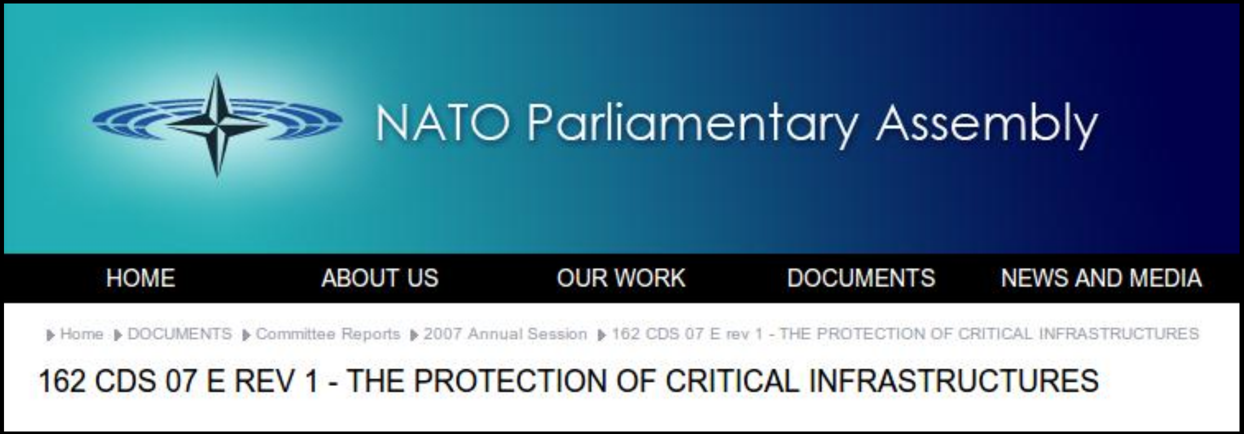
European Commission



(15) In order to facilitate improvements in the protection of ECIs, common methodologies may be developed for the identification and classification of risks, threats and vulnerabilities to infrastructure assets.



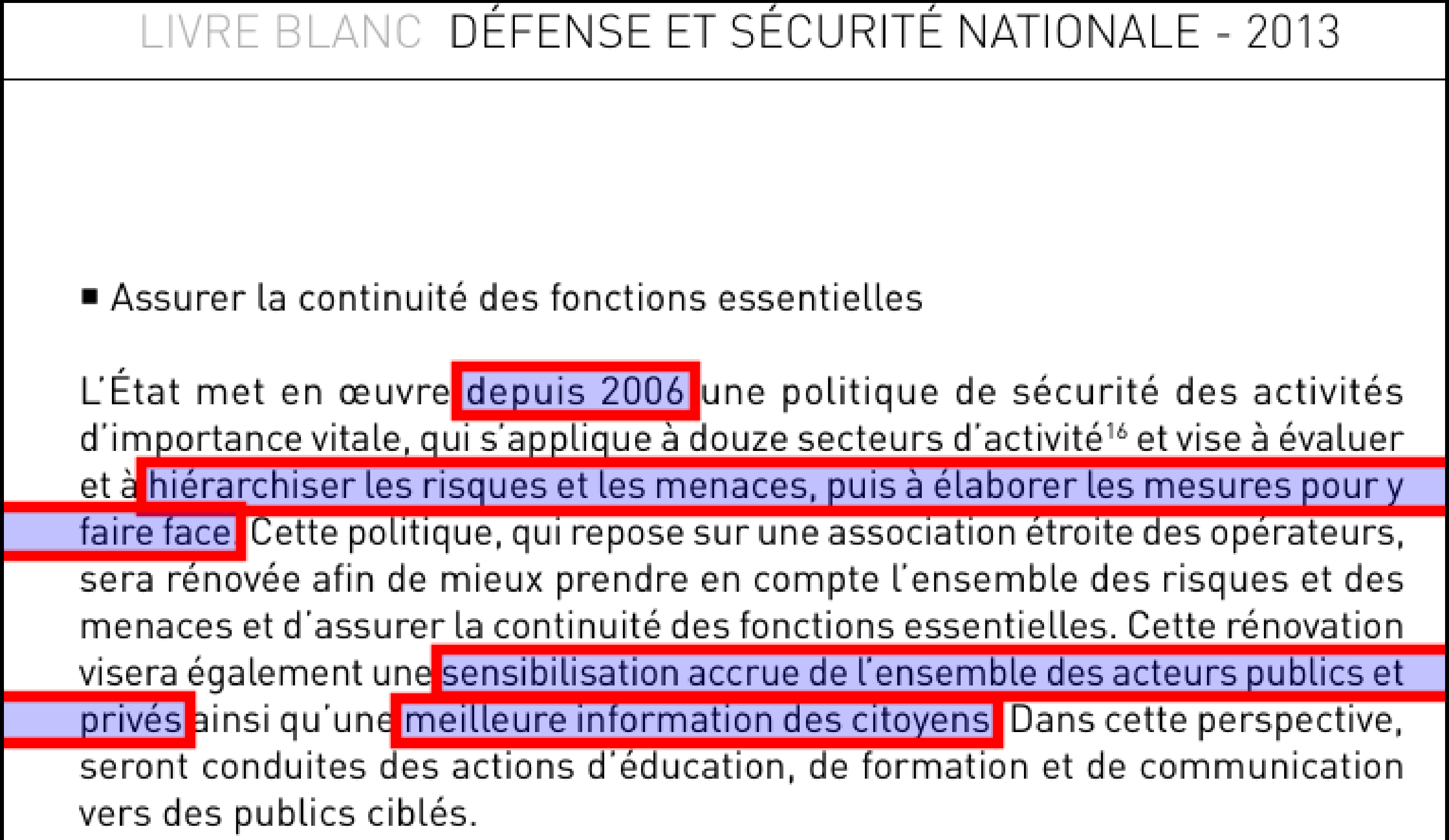
(14) The efficient identification of risks, threats and vulnerabilities in the particular sectors requires communication both between owners/operators of ECIs and the Member States, and between the Member States and the Commission. Each Member State should collect information concerning ECIs located within its territory. The Commission should receive generic information from the Member States concerning risks, threats and vulnerabilities in sectors where ECIs were identified, including where relevant information on possible improvements in the ECIs and cross-sector dependencies, which could be the basis for the development of specific proposals by the Commission on improving the protection of ECIs, where necessary.


NATO Parliamentary Assembly
HOME
ABOUT US
OUR WORK
DOCUMENTS
NEWS AND MEDIA
Home ▸ DOCUMENTS ▸ Committee Reports ▸ 2007 Annual Session ▸ 162 CDS 07 E rev 1 - THE PROTECTION OF CRITICAL INFRASTRUCTURES

162 CDS 07 E REV 1 - THE PROTECTION OF CRITICAL INFRASTRUCTURES

Mobile Operators and governance

- In France



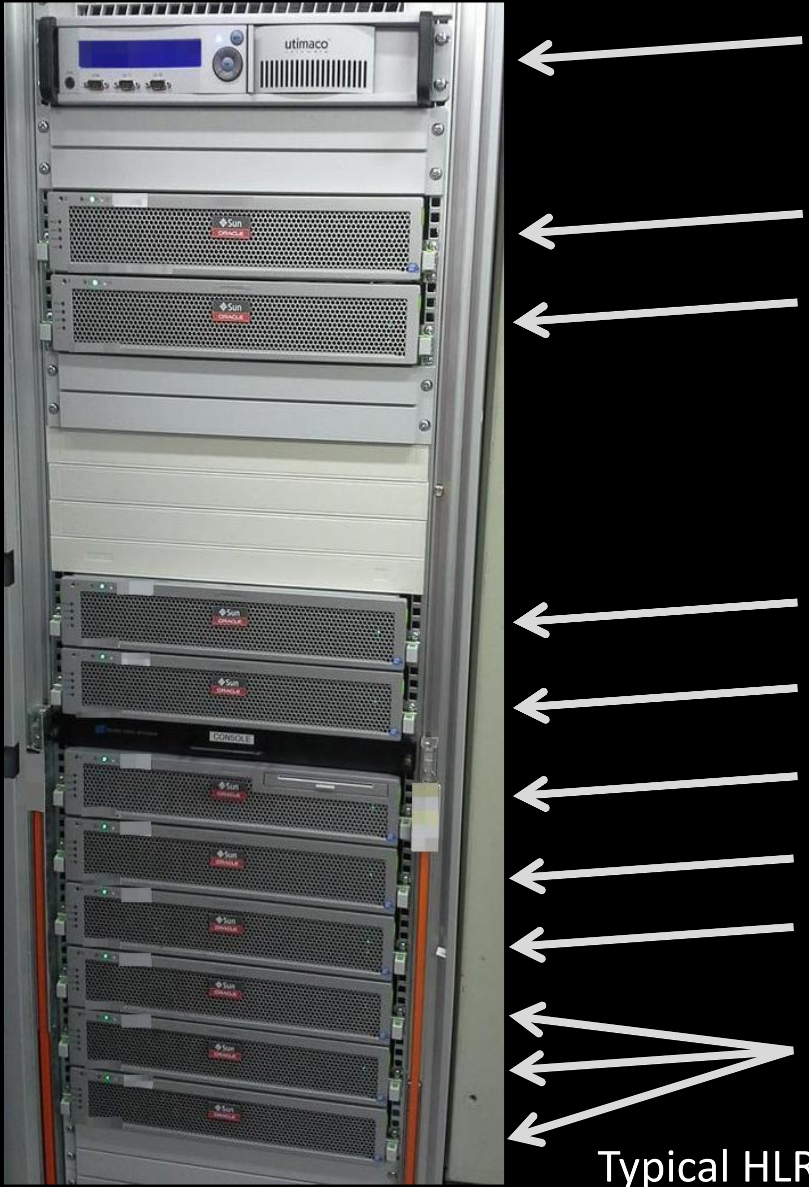
LIVRE BLANC DÉFENSE ET SÉCURITÉ NATIONALE - 2013

- Assurer la continuité des fonctions essentielles

L'État met en œuvre depuis 2006 une politique de sécurité des activités d'importance vitale, qui s'applique à douze secteurs d'activité[16] et vise à évaluer et à hiérarchiser les risques et les menaces, puis à élaborer les mesures pour y faire face. Cette politique, qui repose sur une association étroite des opérateurs, sera rénovée afin de mieux prendre en compte l'ensemble des risques et des menaces et d'assurer la continuité des fonctions essentielles. Cette rénovation visera également une sensibilisation accrue de l'ensemble des acteurs publics et privés ainsi qu'une meilleure information des citoyens. Dans cette perspective, seront conduites des actions d'éducation, de formation et de communication vers des publics ciblés.

Lets check the reality …

The Witness : An HLR/HSS



AuC HSM

HLR Front End

HSS Front End

Provisioning DSA

Routing DSA

Install Server

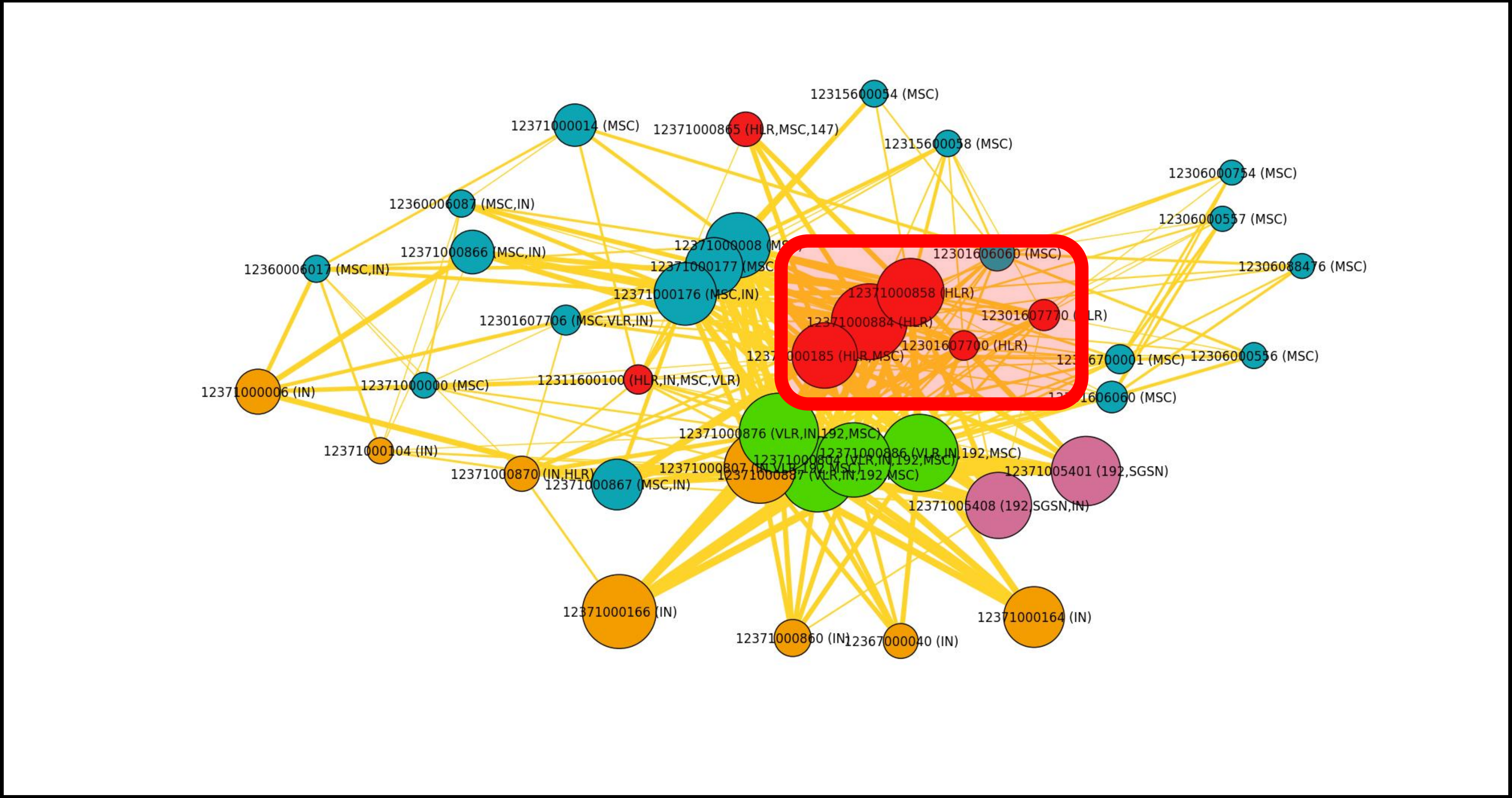
Admin

Provisioning Gateway

3 Back Ends

Typical HLR/HSS in use in operator Core Network

HLR/HSS in Mobile Core Network

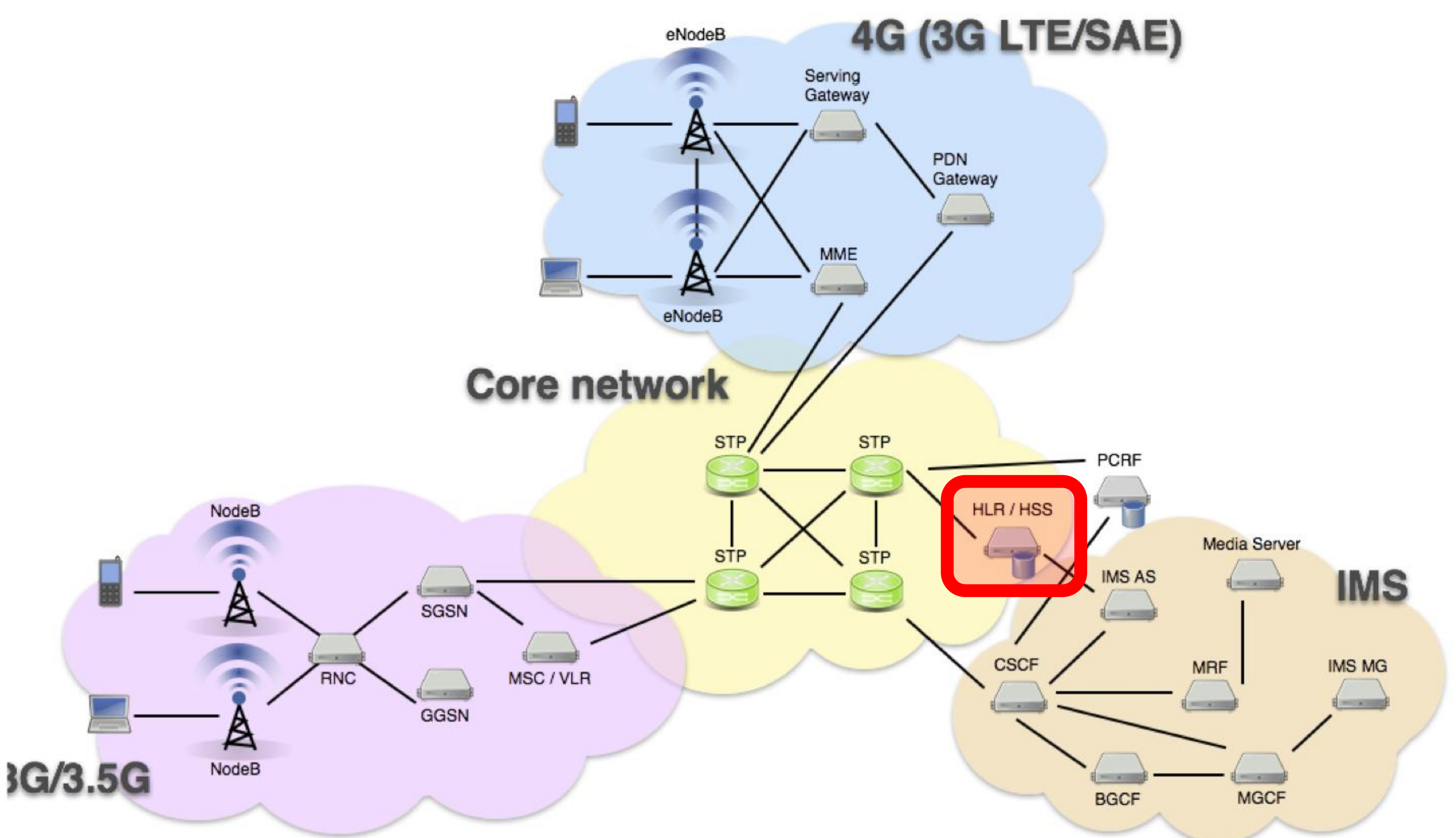


A mobile network operator Core Network

Network passive capture showing Global Titles

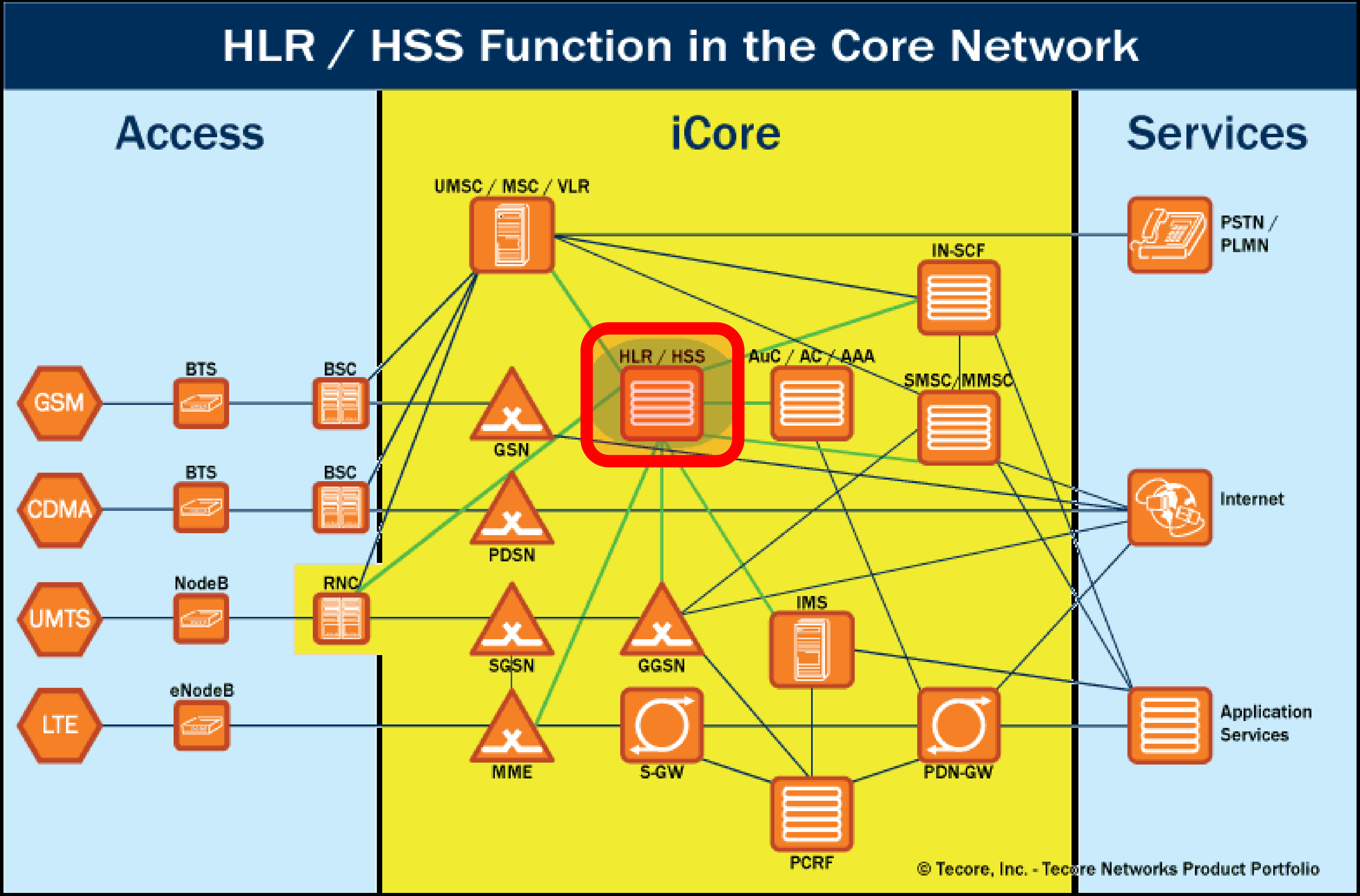
HLR/HSS in Mobile Core Network

Telecom network architecture



P1 Security
Priority One Security

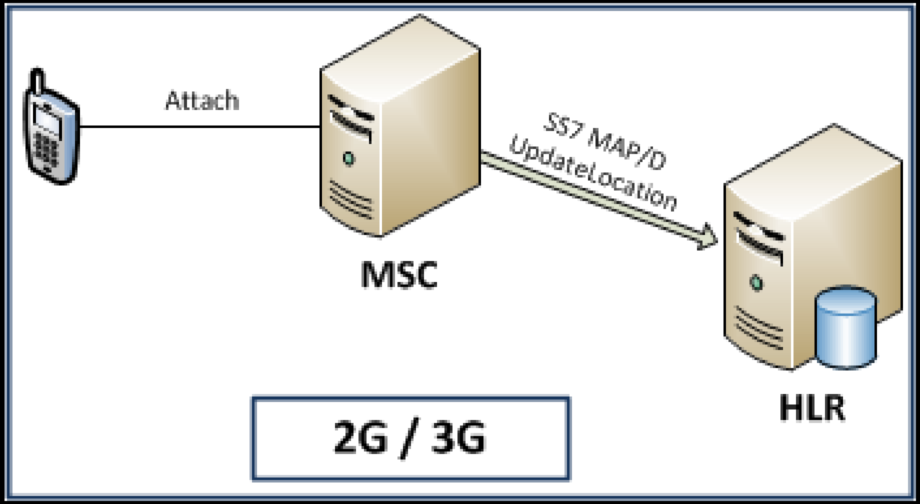
HLR/HSS in Mobile Core Network

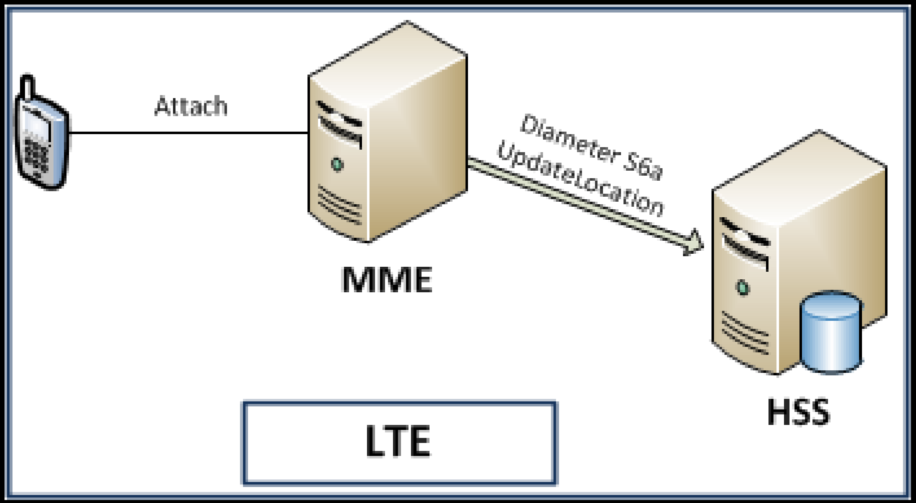


HLR/HSS in Mobile Core Network

- HLR is used in all 2G Operator Network
- HSS is used in all 3G/4G Operator Network
- Stores customer data
  - Subscriber identifier (IMSI)
  - Subscriber encryption keys
  - Subscriber approximate location
  - Subscriber SIM plan options
- Critical to the operator
  - HLR down == Network down, no calls possible

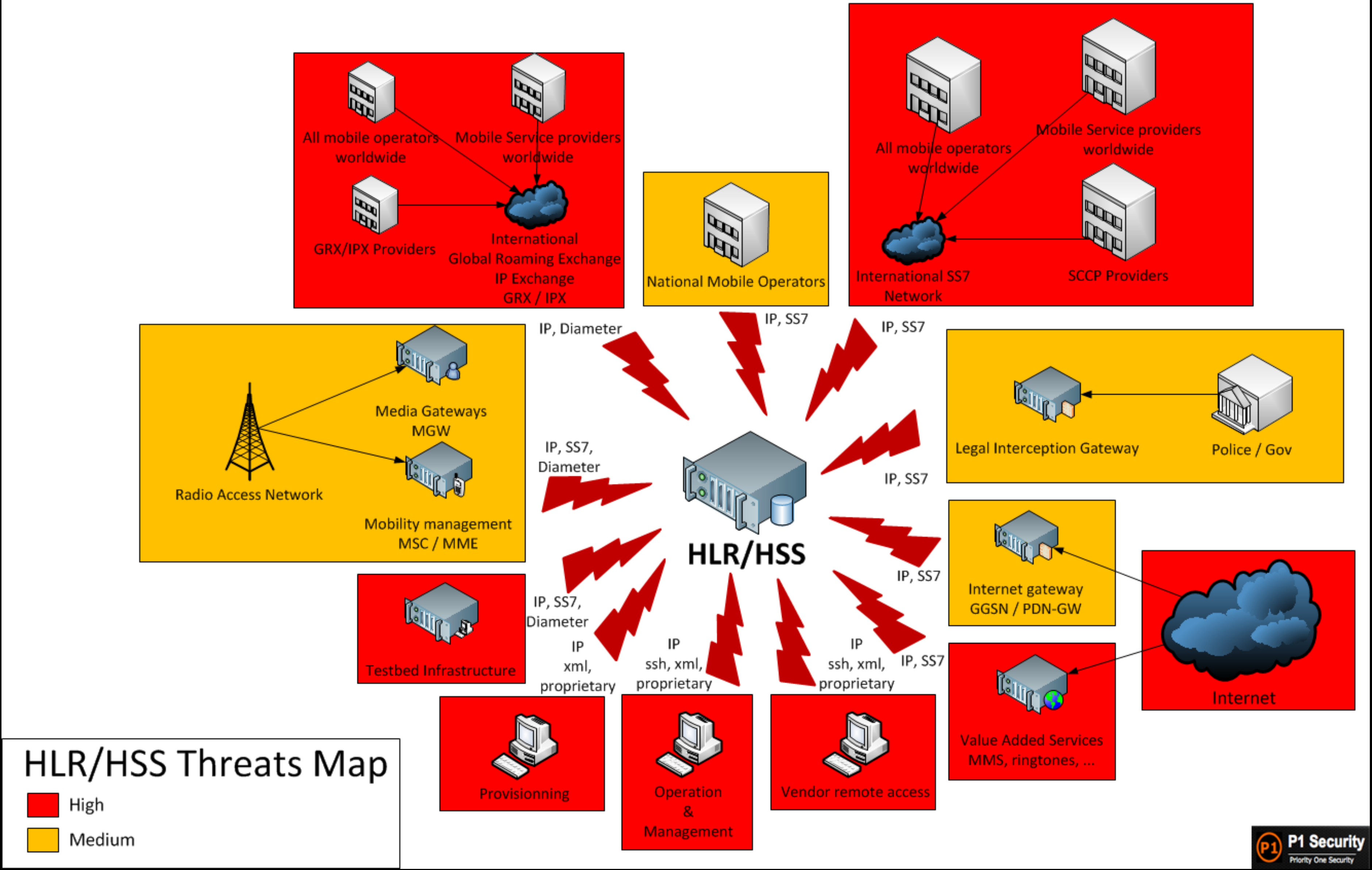
HLR/HSS in Mobile Core Network





HLR/HSS receiving subscriber location update from the operator SS7/Diameter signaling links

Lets make it talk …


All mobile operators worldwide
Mobile Service providers worldwide
GRX/IPX Providers
International Global Roaming Exchange IP Exchange GRX / IPX
National Mobile Operators
All mobile operators worldwide
Mobile Service providers worldwide
SCCP Providers
International SS7 Network
IP, Diameter
IP, SS7
IP, SS7
Radio Access Network
Media Gateways MGW
Mobility management MSC / MME
IP, SS7, Diameter
Legal Interception Gateway
Police / Gov
IP, SS7
HLR/HSS
IP, SS7
Internet gateway GGSN / PDN-GW
Internet
Testbed Infrastructure
IP, SS7, Diameter
IP xml, proprietary
IP ssh, xml, proprietary
IP ssh, xml, proprietary
IP, SS7
Value Added Services MMS, ringtones, ...
Provisionning
Operation & Management
Vendor remote access

HLR/HSS Threats Map

🟥 High

🟨 Medium

Plan

HLR/HSS Robustness assessment

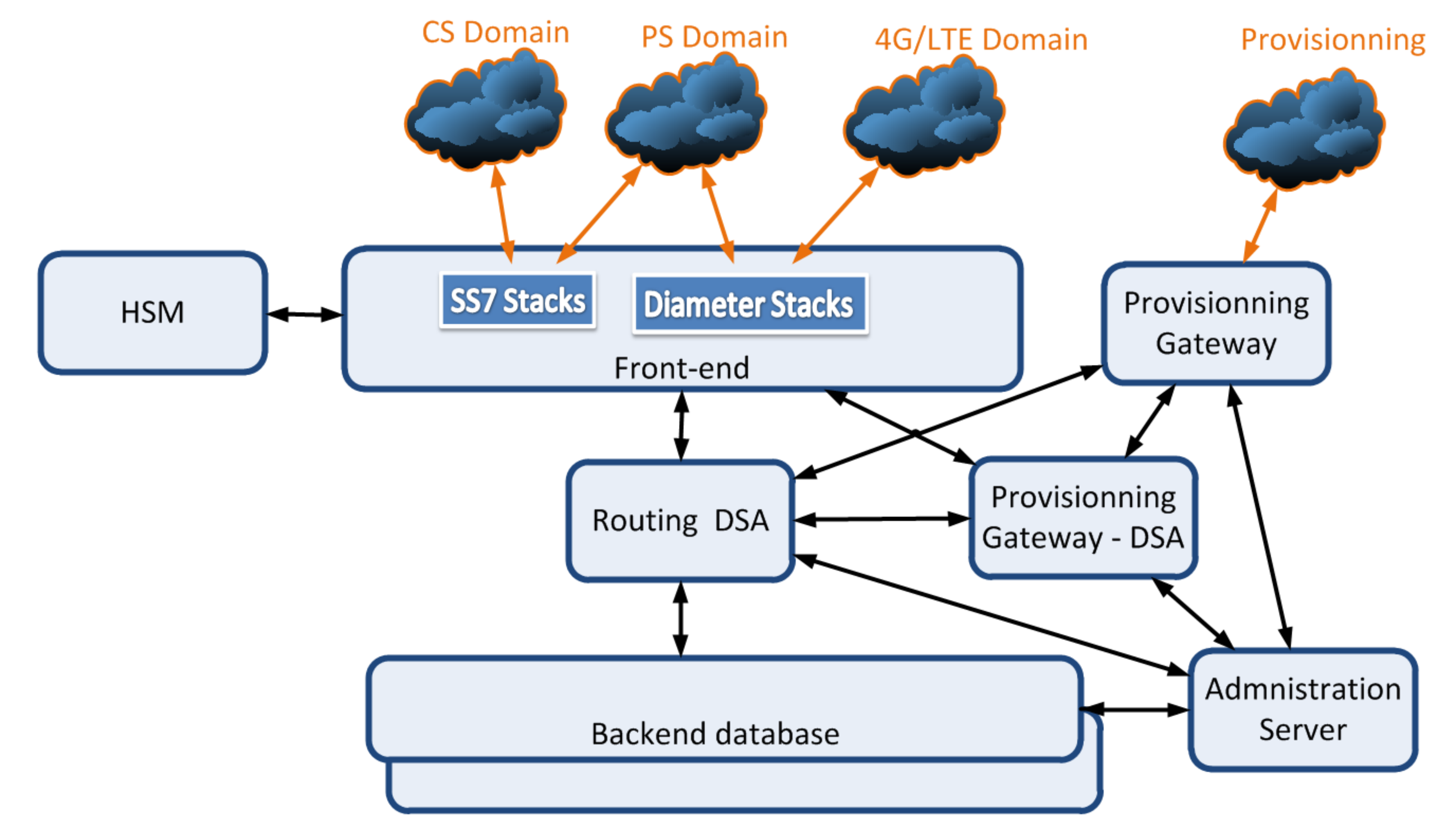
- Virtualization
  - Virtualization and instrumentation
- System Analysis
  - Localroot, Framework complexity
- Network Fuzzing
  - SS7 Protocols
- Binaries Reverse
  - More vulns

HLR/HSS Virtualization

No, it’s not ATCA / NFV

P1 Security
Priority One Security

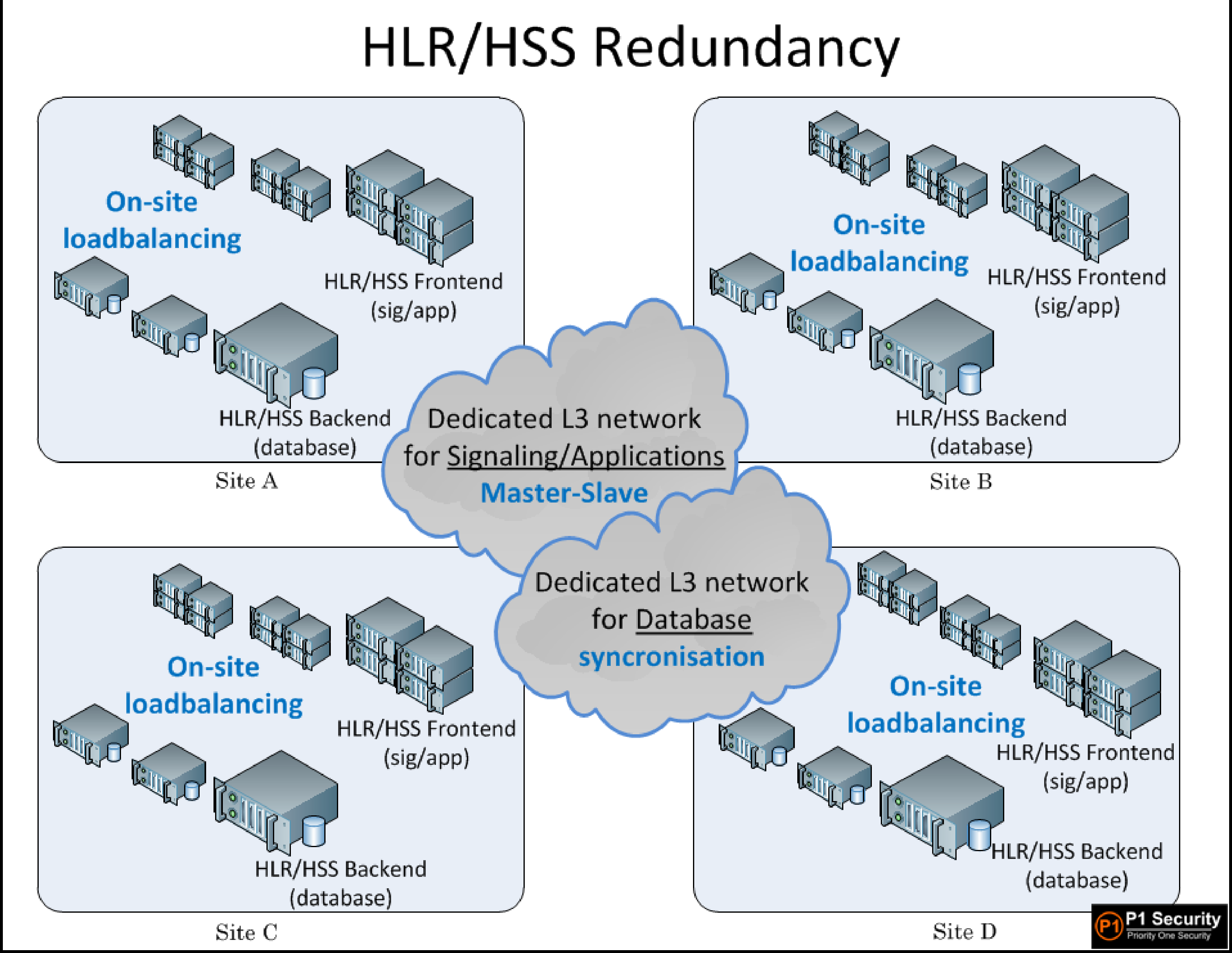
An HLR/HSS is an ecosystem



An HLR/HSS is an ecosystem

- HLR + HSS Front-end
- HLR Administration server
- Application/Database routing servers
- HLR Backend/Database (multiple)
- HSM (Hardware Security Module) for keys

HLR/HSS is never alone


HLR/HSS Redundancy
On-site loadbalancing
HLR/HSS Frontend (sig/app)
HLR/HSS Backend (database)
Site A
On-site loadbalancing
HLR/HSS Frontend (sig/app)
HLR/HSS Backend (database)
Site B
Dedicated L3 network for Signaling/Applications
Master-Slave
Dedicated L3 network for Database
syncronisation
On-site loadbalancing
HLR/HSS Frontend (sig/app)
HLR/HSS Backend (database)
Site C
On-site loadbalancing
HLR/HSS Frontend (sig/app)
HLR/HSS Backend (database)
Site D
P1 Security
Priority One Security

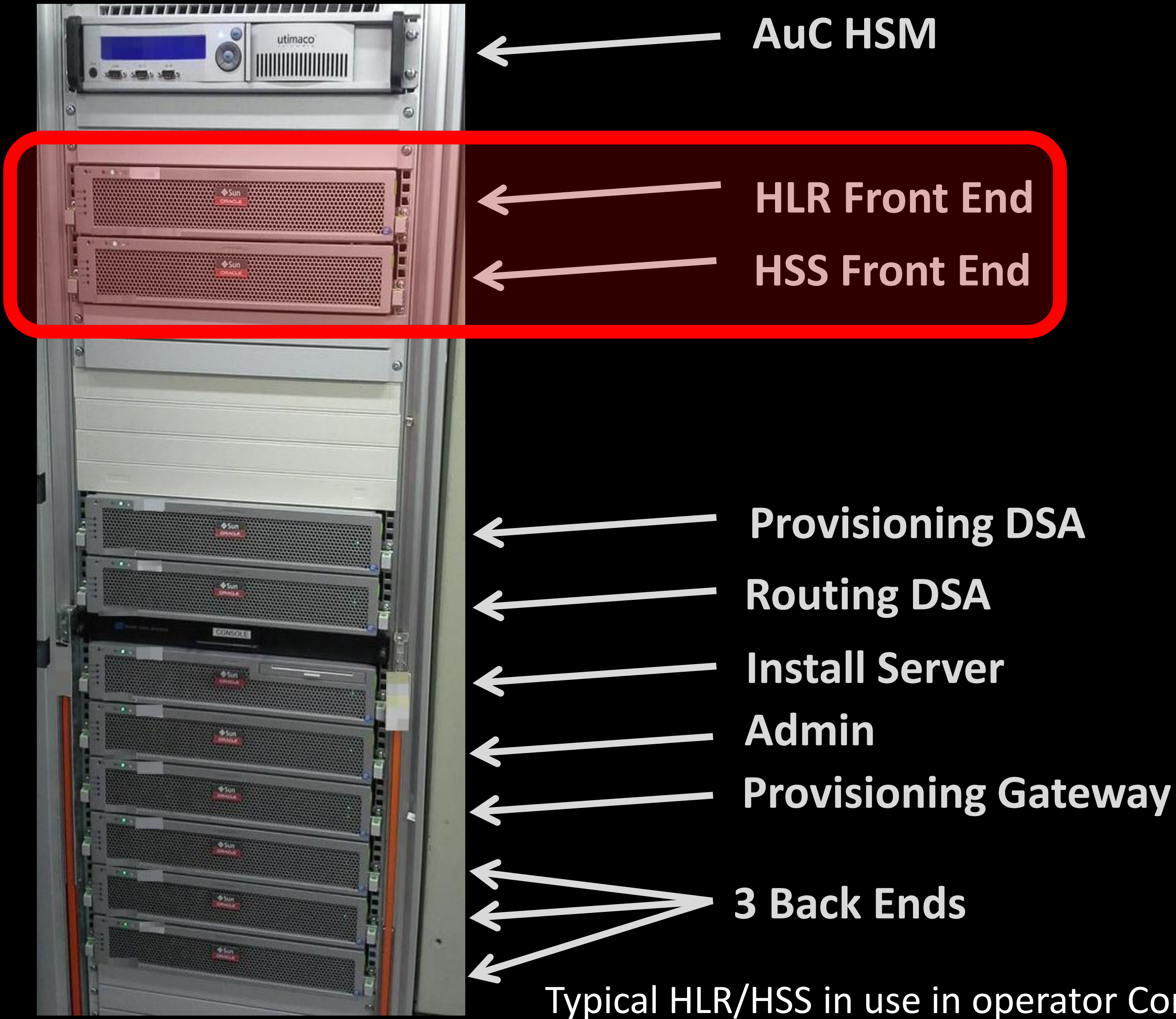
Where to start

- Most exposed from the outside

  => HLR/HSS Front-end

  - Receives SS7/Diameter traffic
    - Telecom network stacks
  - Receives provisioning requests
  - Connected to the HSM

Where to start



AuC HSM

HLR Front End

HSS Front End

Provisioning DSA

Routing DSA

Install Server

Admin

Provisioning Gateway

3 Back Ends

Typical HLR/HSS in use in operator Core Network

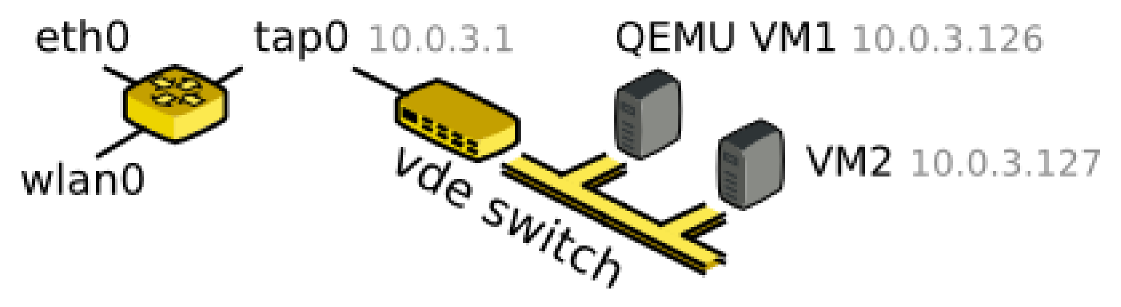
Virtualization of HLR/HSS
Frontend

Original Equipment Manufacturer

- Specs of the real equipment
  - i386 / **x64** / Sparc
  - **Solaris** / CentOS
  - 32 GB of RAM
  - CPU 16 Cores
  - TB hard drive + External SAN

Qemu/KVM

- Faster than VirtualBox
- More flexible
- Tweak code to add more network interfaces
- VDE Switch for networking



Qemu/KVM

```
qemu-system-x86_64                                                                                             \
            -machine type=pc,accel=kvm:tcg -pidfile ./myhlr.pid                                                \
            -m 7.2g -smp 4 -drive file=/dev/mapper/lvm-vm--myhlr,cache=none                                    \
            -vnc 127.0.0.1:2,password,tls,lossy -display curses -rtc base=localtime,driftfix=slew              \
            -net vde,vlan=1,sock=/home/vm-kvm/myhlr/vde-myhlr.ctl -net nic,vlan=1,macaddr=52:54:00:00:10:01    \
            -net vde,vlan=2,sock=/home/vm-kvm/myhlr/vde-myhlr.ctl -net nic,vlan=2,macaddr=52:54:00:00:10:02    \
            -net vde,vlan=3,sock=/home/vm-kvm/myhlr/vde-myhlr.ctl -net nic,vlan=3,macaddr=52:54:00:00:10:02    \
            -net vde,vlan=4, sock=/home/vm-kvm/myhlr/vde-myhlr.ctl -net nic,vlan=4,macaddr=52:54:00:00:10:02   \
            -net vde,vlan=5,sock=/home/vm-kvm/myhlr/vde-myhlr.ctl -net nic,vlan=5,macaddr=52:54:00:00:10:02    \
            -net vde,vlan=6,sock=/home/vm-kvm/myhlr/vde-myhlr.ctl -net nic,vlan=6,macaddr=52:54:00:00:10:02    \
            -net vde,vlan=7,sock=/home/vm-kvm/myhlr/vde-myhlr.ctl -net nic,vlan=7,macaddr=52:54:00:00:10:02    \
            -net vde,vlan=8,sock=/home/vm-kvm/myhlr/vde-myhlr.ctl -net nic,vlan=8,macaddr=52:54:00:00:10:02    \
            -net vde,vlan=9,sock=/home/vm-kvm/myhlr/vde-myhlr.ctl -net nic,vlan=9,macaddr=52:54:00:00:10:02    \
            -net vde,vlan=10,sock=/home/vm-kvm/myhlr/vde-myhlr.ctl -net nic,vlan=10,macaddr=52:54:00:00:10:02  \
            -net vde,vlan=11,sock=/home/vm-kvm/myhlr/vde-myhlr.ctl -net nic,vlan=11,macaddr=52:54:00:00:10:02  \
            -net vde,vlan=12,sock=/home/vm-kvm/myhlr/vde-myhlr.ctl -net nic,vlan=12,macaddr=52:54:00:00:10:02
```

- Physical partition for disk
  - Do not use disk file on host btrfs
    - super slow
    - ext4 is ok
  - http://www.linux-kvm.org/page/Tuning_KVM
- Curses output
- Improvements: serial terminal

Qemu/KVM

- Solaris 10
  - Qemu/KVM ok for x64
  - Fails for SPARC
- Stock kernel
  - /kernel
  - /usr/kernel
- Custom kernel modules
  - For Telecom Signaling [Signalware]
- Uses grub
- Failsafe mode

Inside the machine

- ZFS filesystem
- Solaris 10
- Everything is installed via packages
- Multiple Oracle databases
  - Even on HLR/HSS Front-end only
- A lot of Middleware framework to start the actual network stacks / applications
- Telco stacks: based on Ulticom Signalware
- The OS expects its precious network cards

System Analysis

The filesystem

- ZFS = Filesystem + Volume manager
- ZFS pool (often mirrored)
  - ZFS root pool
    - 100-200GB usually enough
    - Prepare free space for system/processes dump
  - ZFS Dump pool
    - Should be more than size of your RAM
  - ZFS SWAP pool
    - Should be more that size of your RAM

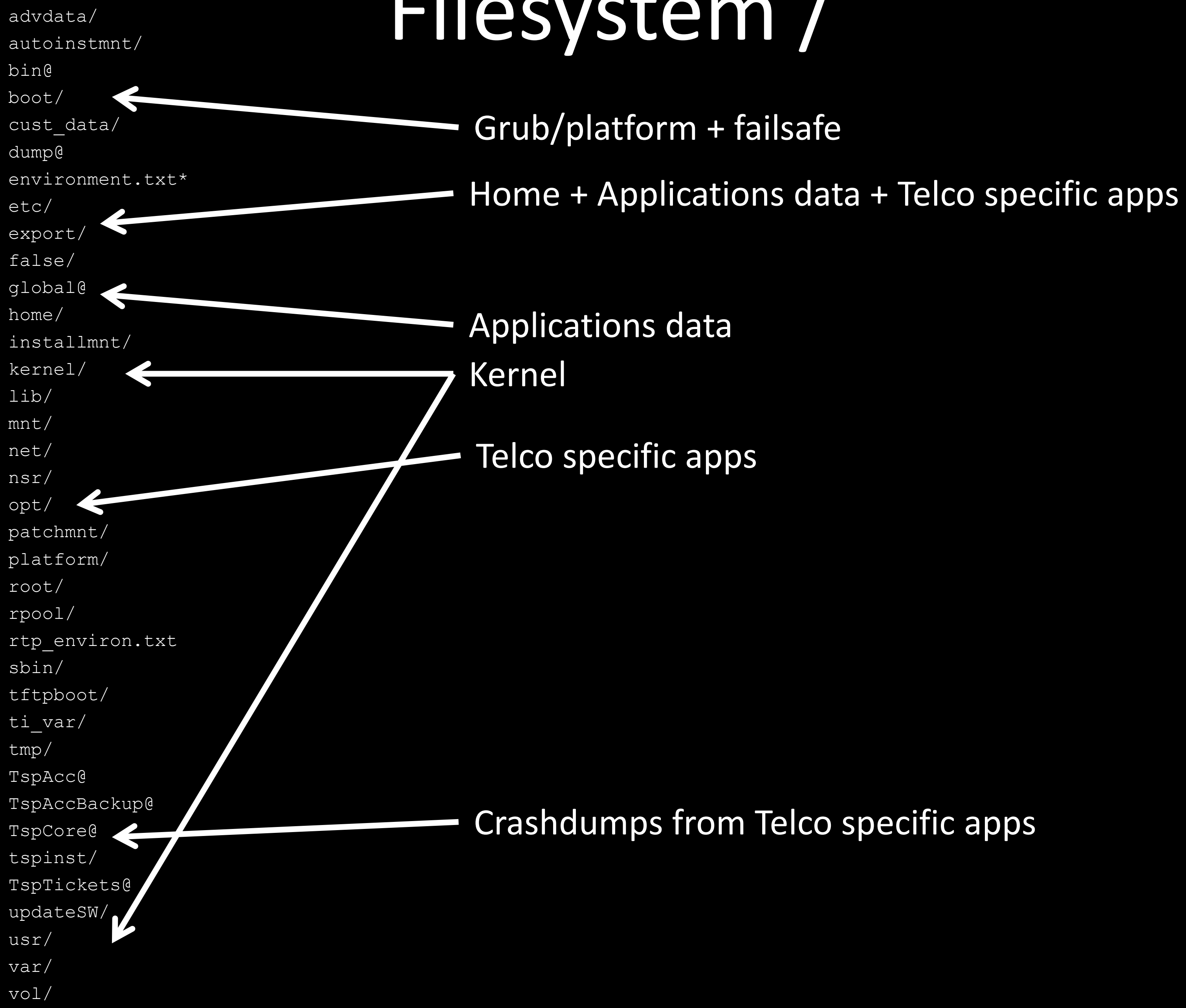
The filesystem

- ZFS offers good resilience against data corruption, and is very picky when there is too much corruption
  - You can't recover when filesystem is too much broken
  - You can try

```
$ zdb -e -p /dev/dsk/c0t3d0p0 -F -X -AAA -dd rpool 1
$ zpool import -f -F -X 19485729304958623456 mypool
$ zpool import -o readonly=on -o autoreplace=on -o
failmode-continue -m -N -f -F -X 19485729304958623456
mypool
```

- If it fails
  - Code your own tool by modifying ZOL http://zfsonlinux.org/

Filesystem /



```
advdata/
autoinstmnt/
bin@
boot/
cust_data/
dump@
environment.txt*
etc/
export/
false/
global@
home/
installmnt/
kernel/
lib/
mnt/
net/
nsr/
opt/
patchmnt/
platform/
root/
rpool/
rtp_environ.txt
sbin/
tftpboot/
ti_var/
tmp/
TspAcc@
TspAccBackup@
TspCore@
tspinst/
TspTickets@
updateSW/
usr/
var/
vol/
```

Grub/platform + failsafe

Home + Applications data + Telco specific apps

Applications data

Kernel

Telco specific apps

Crashdumps from Telco specific apps

Some packages installed

```
application SMAWrtp
        Telecommunication Service Platform (TSP) Base Package

application OMNI
        Signalware System

application S6U-4
        Signalware System

application OMNI-C7X
        Signalware C7 Extensions

application INTPahacu
        AC Utimaco HSM
```

Low hanging fruits

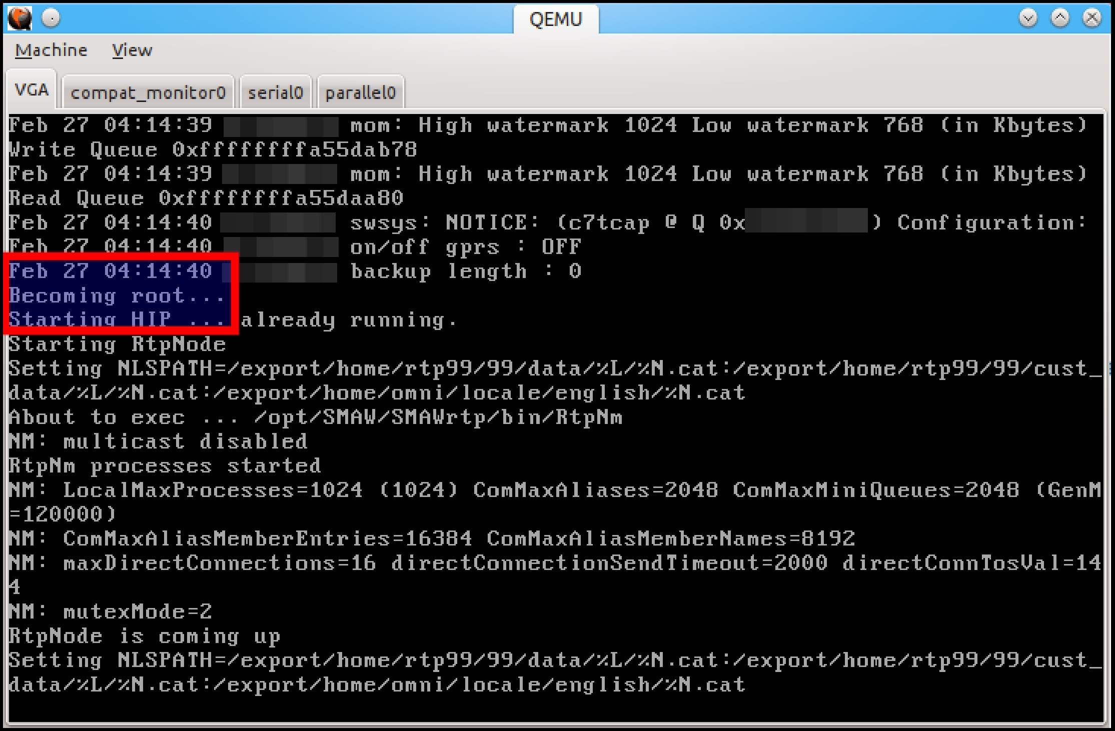
- SUID executables
  - SUID Total: 162 (155 binaries, 7 scripts)
  - SUID Root: 142 (137 binaries, 5 scripts)

- Signalware

Boot process

“becoming root”

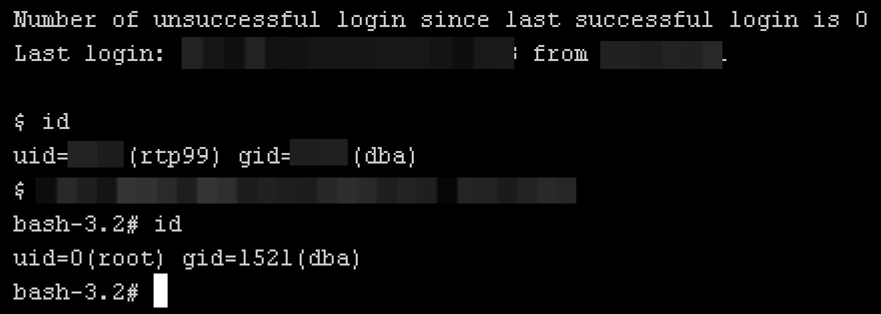
by Design



```
Feb 27 04:14:39 [redacted] mom: High watermark 1024 Low watermark 768 (in Kbytes)
Write Queue 0xfffffffa55dab78
Feb 27 04:14:39 [redacted] mom: High watermark 1024 Low watermark 768 (in Kbytes)
Read Queue 0xfffffffa55daa80
Feb 27 04:14:40 [redacted] swsys: NOTICE: (c7tcap @ Q 0x[redacted]) Configuration:
Feb 27 04:14:40 [redacted] on/off gprs : OFF
Feb 27 04:14:40 [redacted] backup length : 0
Becoming root...
Starting HIP ... already running.
Starting RtpNode
Setting NLSPATH=/export/home/rtp99/99/data/%L/%N.cat:/export/home/rtp99/99/cust_
data/%L/%N.cat:/export/home/omni/locale/english/%N.cat
About to exec ... /opt/SMAW/SMAWrtp/bin/RtpNm
NM: multicast disabled
RtpNm processes started
NM: LocalMaxProcesses=1024 (1024) ComMaxAliases=2048 ComMaxMiniQueues=2048 (GenM
=120000)
NM: ComMaxAliasMemberEntries=16384 ComMaxAliasMemberNames=8192
NM: maxDirectConnections=16 directConnectionSendTimeout=2000 directConnTosVal=14
4
NM: mutexMode=2
RtpNode is coming up
Setting NLSPATH=/export/home/rtp99/99/data/%L/%N.cat:/export/home/rtp99/99/cust_
data/%L/%N.cat:/export/home/omni/locale/english/%N.cat
```

Local roots

- Of course, we often find multiple local roots
- Some are really too easy (one command):



```
Number of unsuccessful login since last successful login is 0
Last login: [redacted] from [redacted].

$ id
uid=[redacted](rtp99) gid=[redacted](dba)
$ [redacted]
bash-3.2# id
uid=0(root) gid=1521(dba)
bash-3.2#
```

Example of Telco network stack: NSN TSP / RTP + Ulticom Signalware

- TSP + RTP framework are found on NSN NT-HLR
  - Found in many European and Worldwide operators
  - Very similar to Apertio OneHLR
- TSP: Telco Server Platform (Ericsson) / Telco Service Platform (NSN, others, generic name)
- RTP: Resilient Telco Platform (NSN)

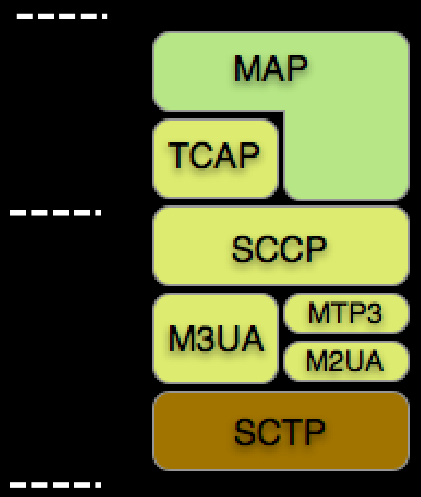
Example of Telco network stack: NSN TSP / RTP + Ulticom Signalware

- SS7 Protocol handling

TSP Framework [NSN]
Handles TCAP and MAP services
[Java executables, uses C libraries]

Signalware stack [Ulticom]
Handles SCTP, M3UA, SCCP, TCAP
[kernel modules and userland binaries]

RTP Framework [NSN]
Starts all Telco specific applications
[Shell scripts and binaries]

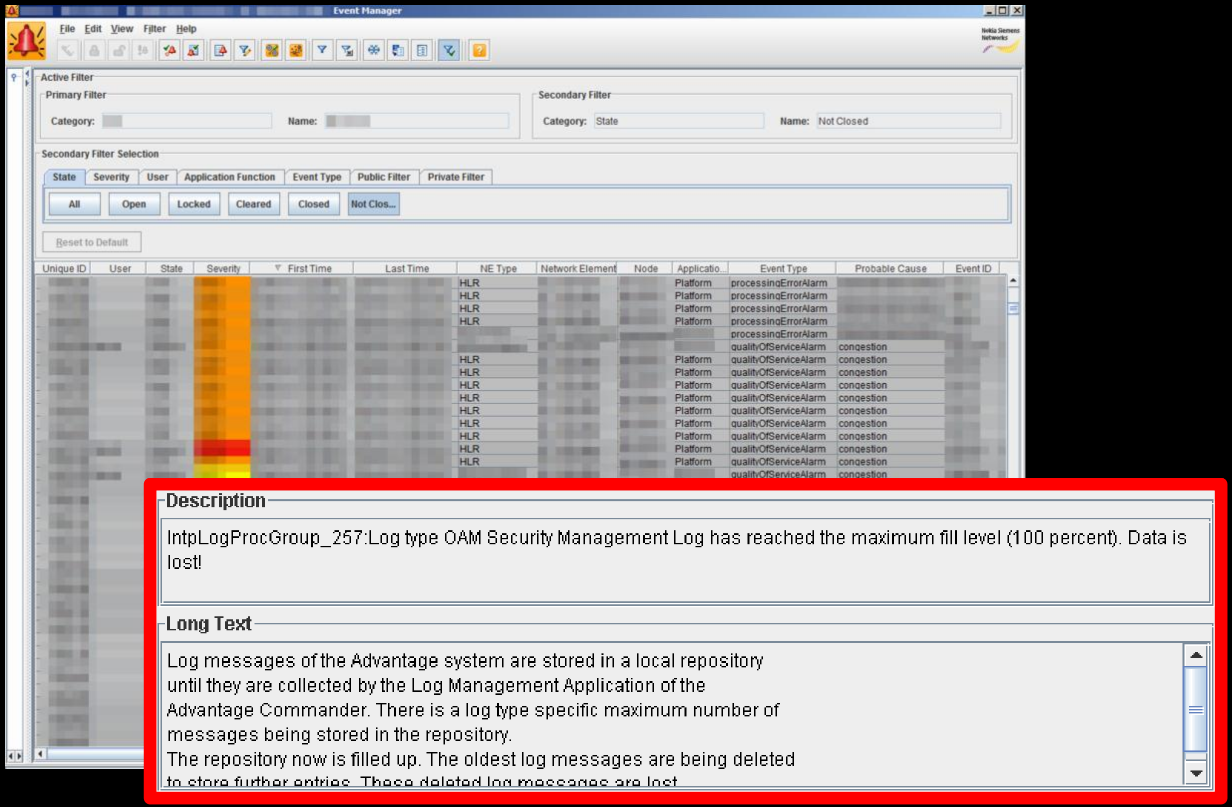


Reminder: SS7 stack

Network Fuzzing

Fuzzing SS7: M3UA

- Example: Flooding badly handled
  - Leads to alerts flooding in OSS
  - Leads to loss of previous alerts !
  - P1VID#799



Primary Filter: Category: [redacted] Name: [redacted]

Secondary Filter: Category: State Name: Not Closed

Unique ID	User	State	Severity	First Time	Last Time	NE Type	Network Element	Node	Applicatio...	Event Type	Probable Cause	Event ID
[redacted]		[redacted]	🟧	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	processingErrorAlarm	[redacted]	[redacted]
[redacted]		[redacted]	🟧	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	processingErrorAlarm	[redacted]	[redacted]
[redacted]		[redacted]	🟧	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	processingErrorAlarm	[redacted]	[redacted]
[redacted]		[redacted]	🟧	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	processingErrorAlarm	[redacted]	[redacted]
[redacted]		[redacted]	🟧	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	processingErrorAlarm	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	🟧	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	qualityOfServiceAlarm	congestion	[redacted]
[redacted]		[redacted]	🟧	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	qualityOfServiceAlarm	congestion	[redacted]
[redacted]		[redacted]	🟧	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	qualityOfServiceAlarm	congestion	[redacted]
[redacted]		[redacted]	🟧	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	qualityOfServiceAlarm	congestion	[redacted]
[redacted]		[redacted]	🟧	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	qualityOfServiceAlarm	congestion	[redacted]
[redacted]		[redacted]	🟧	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	qualityOfServiceAlarm	congestion	[redacted]
[redacted]		[redacted]	🟧	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	qualityOfServiceAlarm	congestion	[redacted]
[redacted]		[redacted]	🟧	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	qualityOfServiceAlarm	congestion	[redacted]
[redacted]	[redacted]	[redacted]	🟥	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	qualityOfServiceAlarm	congestion	[redacted]
[redacted]		[redacted]	🟧	[redacted]	[redacted]	HLR	[redacted]	[redacted]	Platform	qualityOfServiceAlarm	congestion	[redacted]
[redacted]	[redacted]	[redacted]	🟨	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	qualityOfServiceAlarm	congestion	[redacted]

Description

IntpLogProcGroup_257:Log type OAM Security Management Log has reached the maximum fill level (100 percent). Data is lost!

Long Text

Log messages of the Advantage system are stored in a local repository until they are collected by the Log Management Application of the Advantage Commander. There is a log type specific maximum number of messages being stored in the repository.
The repository now is filled up. The oldest log messages are being deleted to store further entries. These deleted log messages are lost

Fuzzing SS7: SCCP

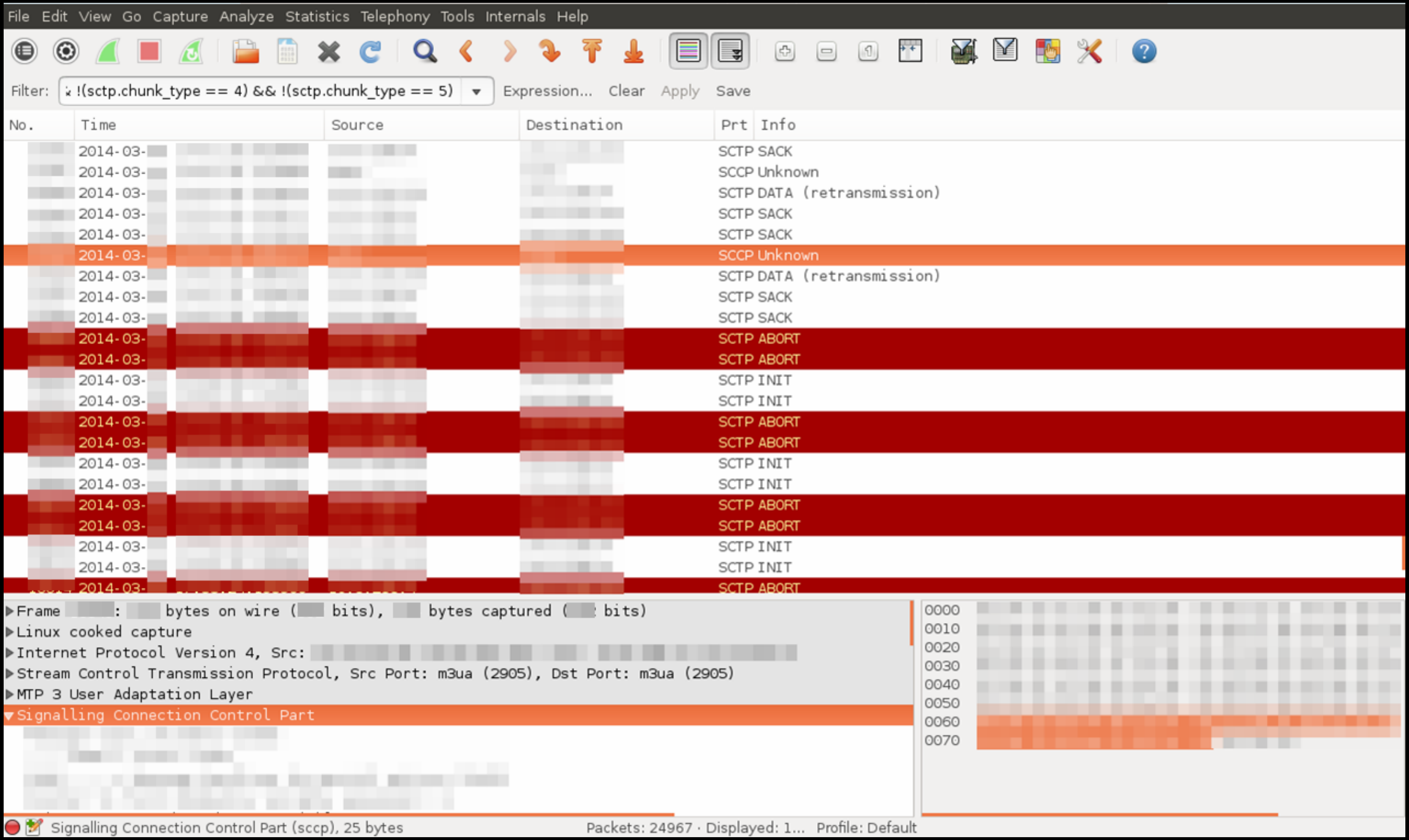
- Example result: 1 specific MSU repeated 2 times causes DoS of all Signaling Interconnections
  - HLR is down during 2 minutes
  - Total Denial of Service of the network
  - Nobody can receive calls in the whole country

```
core 'core.xxx' of 15477:   /export/home/xxx
 01 msu_processing ()
 02 msg_distribution ()
 03 main ()
 04 _start ()
```

  - If the attack is repeated, the DoS is permanent during the attack
  - P1VID#773

So long for the critical infrastructure …

Fuzzing SS7: SCCP


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

Filter: !(sctp.chunk_type == 4) && !(sctp.chunk_type == 5)

```
No.         Time                     Source       Destination  Prt Info
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP SACK
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCCP Unknown
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP DATA (retransmission)
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP SACK
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP SACK
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCCP Unknown
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP DATA (retransmission)
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP SACK
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP SACK
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP ABORT
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP ABORT
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP INIT
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP INIT
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP ABORT
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP ABORT
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP INIT
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP INIT
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP ABORT
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP ABORT
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP INIT
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP INIT
[redacted]  2014-03-[redacted]       [redacted]   [redacted]       SCTP ABORT
```

```
▶Frame [redacted]: [redacted] bytes on wire ([redacted] bits), [redacted] bytes captured ([redacted] bits)
▶Linux cooked capture
▶Internet Protocol Version 4, Src: [redacted]
▶Stream Control Transmission Protocol, Src Port: m3ua (2905), Dst Port: m3ua (2905)
▶MTP 3 User Adaptation Layer
▼Signalling Connection Control Part
   [redacted]
```

```
0000  [redacted]
0010  [redacted]
0020  [redacted]
0030  [redacted]
0040  [redacted]
0050  [redacted]
0060  [redacted]
0070  [redacted]
```

Signalling Connection Control Part (sccp), 25 bytes   Packets: 24967 · Displayed: 1...   Profile: Default

Fuzzing SS7: MAP

- Example results: 1 specific MSU causes MAP process crashes
  - 5 MSU/second makes HLR totally unresponsive to any other MAP Query
    - Total Denial of Service of the network
    - Nobody can receive calls in the whole country
  - 1 MSU/second makes HLR totally drop 50% of other MAP Queries
    - Network is highly perturbed
    - 50% of the called in the whole country are failing
  - P1VID#772

Fuzzing Diameter

- Process Crash with 1 specific manually crafted MSU

Logs do not even report process crash.

Neither the OSS Alerts.

Application logs:

```
Services_Esm_Log_Message: vc_Priority=LOG_ERR, vc_MessageInformation=ESM:
Service could not be processed correctly,
vc_AdditionalInformation=Reason: xxxxxxxxx data unavailable, Message Type:
S6a-xxxxxxxxx
Services_Esm_Log_Message: vc_Priority=LOG_ERR, vc_MessageInformation=ESM:
Service could not be processed correctly,
vc_AdditionalInformation=Reason: xxxxxxxxx data unavailable, Message Type:
S6a-xxxxxxxxx
UTC Tue Sep  3 01:20:44 2013 Services_Esm_Log_Message: vc_Priority=LOG_ERR,
vc_MessageInformation=ESM: Service could not be processed correctly,
vc_AdditionalInformation=Reason: xxxxxxxxx data unavailable, Message Type:
S6a-xxxxxxxxx
Services_Esm_Log_Message: vc_Priority=LOG_ERR, vc_MessageInformation=ESM:
Service could not be processed correctly,
vc_AdditionalInformation=Reason: xxxxxxxxx data unavailable, Message Type:
S6a-xxxxxxxxx
```

Behind that, process core dumps are created…

P1VID#718

Does redundancy saves you ?

- No !

- Same N front-ends == same crashes
- Messages just needs to be sent N times

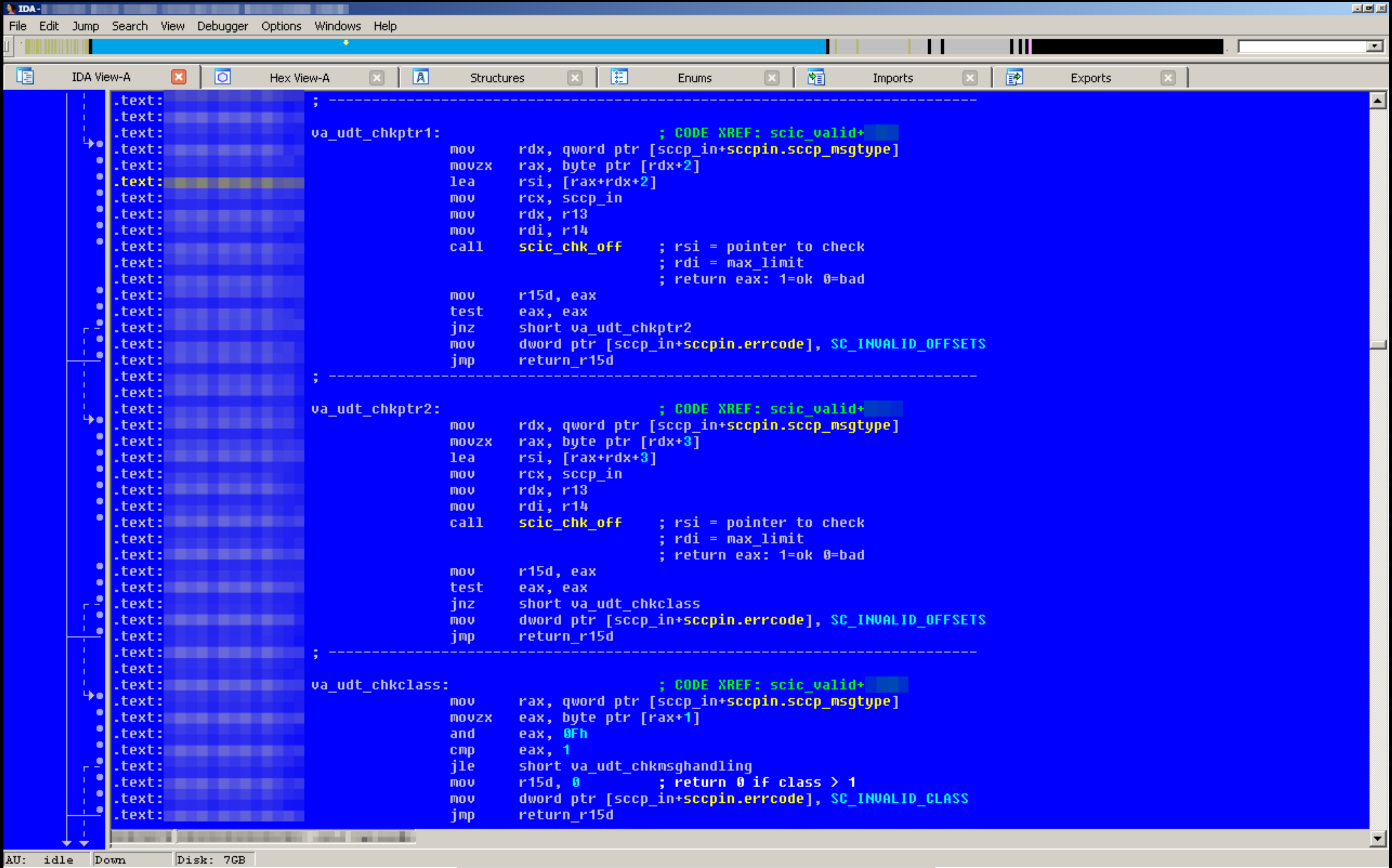
Binaries reverse

Often, too much help…

- Binaries not stripped
  - Debug symbols / function names / … available
- No anti-debug mechanism
- Libraries headers on production machines
  - Great help in understanding the internals
- Large documentation about internals on production machines
  - Great help in understanding the internals
- Updated binaries and previous binaries both on production machines
  - Binary diff to track issues fixed

Signalware Kernel modules

- Example: Parsing of SCCP header



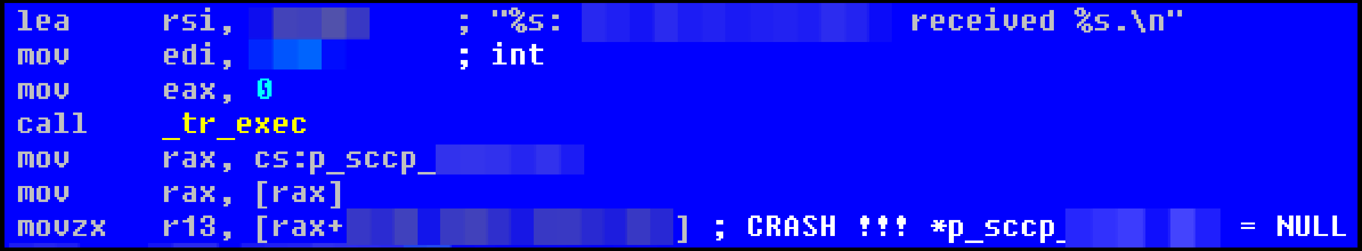
```
.text:[redacted]   ; ---------------------------------------------------------------------------
.text:
.text:             va_udt_chkptr1:                         ; CODE XREF: scic_valid+[redacted]
.text:                             mov     rdx, qword ptr [sccp_in+sccpin.sccp_msgtype]
.text:                             movzx   rax, byte ptr [rdx+2]
.text:                             lea     rsi, [rax+rdx+2]
.text:                             mov     rcx, sccp_in
.text:                             mov     rdx, r13
.text:                             mov     rdi, r14
.text:                             call    scic_chk_off    ; rsi = pointer to check
.text:                                                     ; rdi = max_limit
.text:                                                     ; return eax: 1=ok 0=bad
.text:                             mov     r15d, eax
.text:                             test    eax, eax
.text:                             jnz     short va_udt_chkptr2
.text:                             mov     dword ptr [sccp_in+sccpin.errcode], SC_INVALID_OFFSETS
.text:                             jmp     return_r15d
.text:             ; ---------------------------------------------------------------------------
.text:
.text:             va_udt_chkptr2:                         ; CODE XREF: scic_valid+[redacted]
.text:                             mov     rdx, qword ptr [sccp_in+sccpin.sccp_msgtype]
.text:                             movzx   rax, byte ptr [rdx+3]
.text:                             lea     rsi, [rax+rdx+3]
.text:                             mov     rcx, sccp_in
.text:                             mov     rdx, r13
.text:                             mov     rdi, r14
.text:                             call    scic_chk_off    ; rsi = pointer to check
.text:                                                     ; rdi = max_limit
.text:                                                     ; return eax: 1=ok 0=bad
.text:                             mov     r15d, eax
.text:                             test    eax, eax
.text:                             jnz     short va_udt_chkclass
.text:                             mov     dword ptr [sccp_in+sccpin.errcode], SC_INVALID_OFFSETS
.text:                             jmp     return_r15d
.text:             ; ---------------------------------------------------------------------------
.text:
.text:             va_udt_chkclass:                        ; CODE XREF: scic_valid+[redacted]
.text:                             mov     rax, qword ptr [sccp_in+sccpin.sccp_msgtype]
.text:                             movzx   eax, byte ptr [rax+1]
.text:                             and     eax, 0Fh
.text:                             cmp     eax, 1
.text:                             jle     short va_udt_chkmsghandling
.text:                             mov     r15d, 0         ; return 0 if class > 1
.text:                             mov     dword ptr [sccp_in+sccpin.errcode], SC_INVALID_CLASS
.text:                             jmp     return_r15d
```

Signalware Kernel modules

- Kernel modules signaling parsing is robust
- IPC to communicate with userland binaries
- Complexity leads to other type of errors
  - Logic errors
  - Race conditions
  - Slow handling of some types of MSUs

Signalware userland binaries

- Parsing less robust (less tested)
- Example logic error due to IPC / Framework complexity:



```
lea     rsi, [redacted]          ; "%s: [redacted]  received %s.\n"
mov     edi, [redacted]          ; int
mov     eax, 0
call    _tr_exec
mov     rax, cs:p_sccp_[redacted]
mov     rax, [rax]
movzx   r13, [rax+[redacted]] ; CRASH !!! *p_sccp_[redacted] = NULL
```

Null pointer dereference

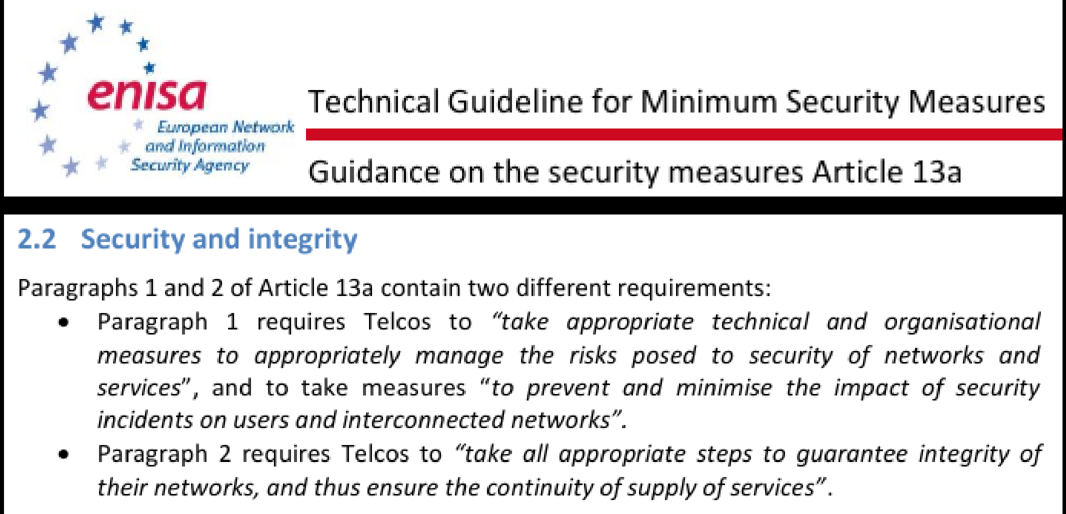
Can be triggered from the International SS7 network

So verdict ?

So verdict ?

- Misconceptions!
  - No crashes on a Critical Core Network Element
    - FAIL
  - Robustness against network attacks
    - FAIL
    - Redundancy != Robust, attack kills Front-end one by one
  - Modern
    - Depends, but from what we see there is much room for improvement

Mobile Operators and governance



enisa
European Network and Information Security Agency

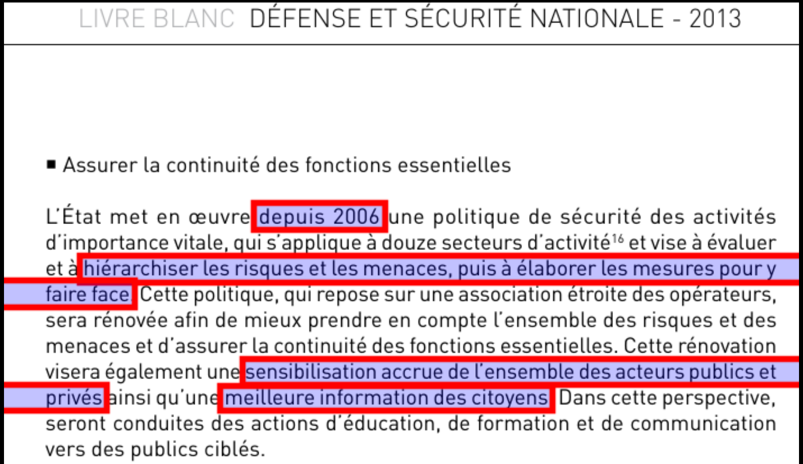
Technical Guideline for Minimum Security Measures

Guidance on the security measures Article 13a

2.2 Security and integrity

Paragraphs 1 and 2 of Article 13a contain two different requirements:

- Paragraph 1 requires Telcos to *"take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services"*, and to take measures *"to prevent and minimise the impact of security incidents on users and interconnected networks"*.
- Paragraph 2 requires Telcos to *"take all appropriate steps to guarantee integrity of their networks, and thus ensure the continuity of supply of services"*.



LIVRE BLANC DÉFENSE ET SÉCURITÉ NATIONALE - 2013

- Assurer la continuité des fonctions essentielles

L'État met en œuvre depuis 2006 une politique de sécurité des activités d'importance vitale, qui s'applique à douze secteurs d'activité[16] et vise à évaluer et à hiérarchiser les risques et les menaces, puis à élaborer les mesures pour y faire face. Cette politique, qui repose sur une association étroite des opérateurs, sera rénovée afin de mieux prendre en compte l'ensemble des risques et des menaces et d'assurer la continuité des fonctions essentielles. Cette rénovation visera également une sensibilisation accrue de l'ensemble des acteurs publics et privés ainsi qu'une meilleure information des citoyens. Dans cette perspective, seront conduites des actions d'éducation, de formation et de communication vers des publics ciblés.

- Reality on Threats analysis: Maybe
- Reality of Telco equipment security: Very bad
- Public information: Very bad
- Telco private sector information: Didn't see impact

Consequences

- Mobile Network crashes for unknown publicly available reason
- Spying on phone calls / customer activities from a single point (Core Network) is relatively easy
- Fraud

Recommendations

- Secure SDLC (Secure Software Development Life Cycle)
  - Design
  - Implementation
  - Testing
    - Especially for vendors custom stacks/services TCAP/MAP parsing bugs leading to overflows, …
- Vendors security audits (HLR isolated)
  - System audit
  - Network audit
- Testbed audits (HLR in environment)
  - System audit
  - Network audit
  - Before deploying to production

Recommendations: securing the OS

- Use Solaris Zones to split services: P1VID#764
- Use Solaris Audit mechanism: P1VID#765
- Authenticate the hardware
  - To prevent emulation
- Use the latest OS protections against exploitation
  - Solaris 11 has ASLR
  - Use custom Linux kernel
- Use a firewall **by default** on the machine itself
- …

Recommendations: OSS

- Make it faster !
  - People should be able to use it to react when under attack
  - E.g. NSN @vantage commander
- Need access to all low-level network traffic for forensics

Recommendations: For the operators

- Push the vendors to fix the bugs
- Some of the attacks we discovered can be filtered
  - Operators do not have to wait for bugs to be fixed
  - Filter at perimeter boundaries (typically STP / Router)
  - Depends on STP / Router models and security “features”
    - Sometime filtering options are charged by vendor
- It is possible to filter also at the SCCP provider level

To be continued

- Telecom Network Elements security is low
  - We tested multiple Network Element types/models, from different vendors
- Vendors, Governments and security researchers have work to do
- Vulnerability disclosure in security critical infrastructure is scarce
  - Dangerous ?
  - Not if there is collaboration

Other aspects of Telecom Security

- We talked here about equipment security
  - It’s a work in progress, and only HLR/HSS
  - Mainly Network Equipment Vendor responsibility
- Also consider
  - Other Network Elements security
  - GRX / IPX / SCCP Providers security
  - Deployment security (passwords policies, filtering…), Operator responsability
  - Telecom Network Fraud (SS7 spoofing, Call/SMS Spoofing, …), Operator responsability

References

Governance literature on critical infrastructure:

- European level
  - 2007:
    http://www.nato-pa.int/default.asp?COM=1165&LNG=0
  - 2012
    http://www.nato.int/cps/en/natolive/news_88054.htm?selectedLocale=en
  - 2013
    http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm
    http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf
- France
  - 2012
    http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000026638421&dateTexte=&categorieLien=id
  - 2013
    http://www.gouvernement.fr/gouvernement/livre-blanc-2013-de-la-defense-et-de-la-securite-nationale

That’s it, please react.

Thank you

laurent@p1sec.com

http://www.p1sec.com