

# 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

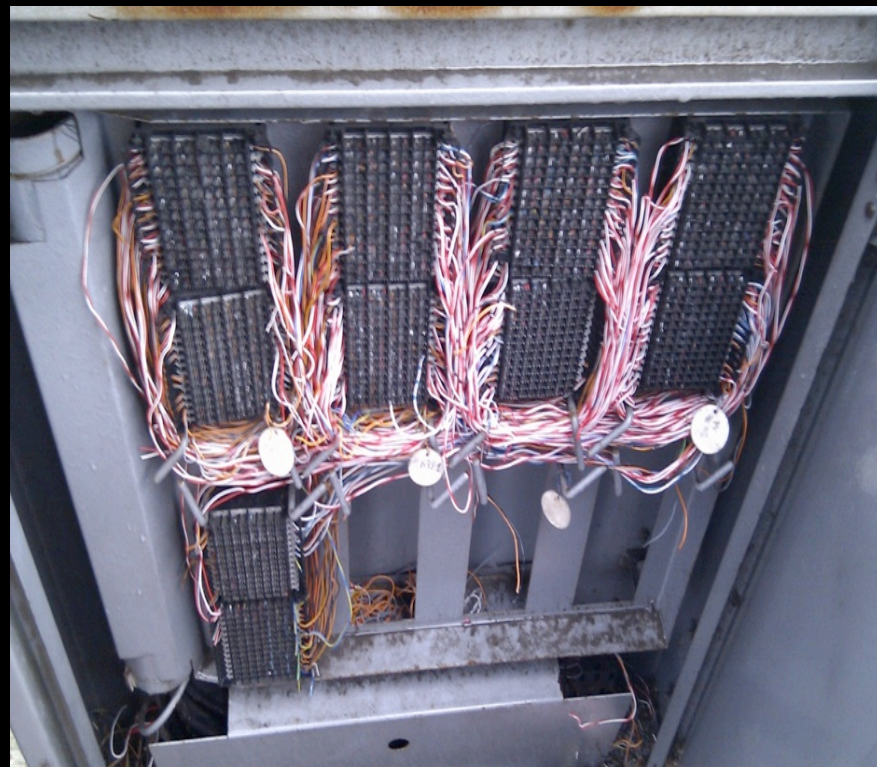
Prehistory



# Beige Box



+

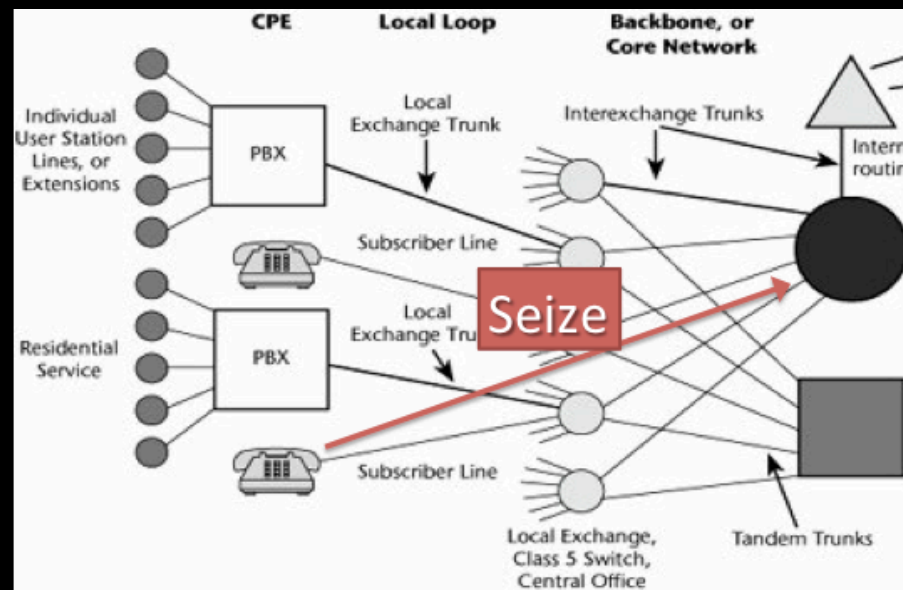


= ?

# Blue box: Kudos Captain!



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

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

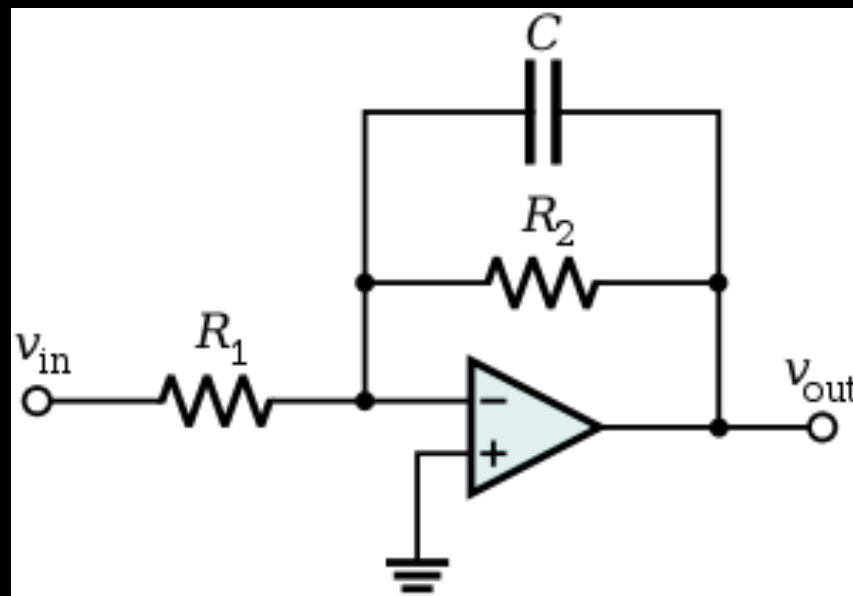
1980's

Legacy





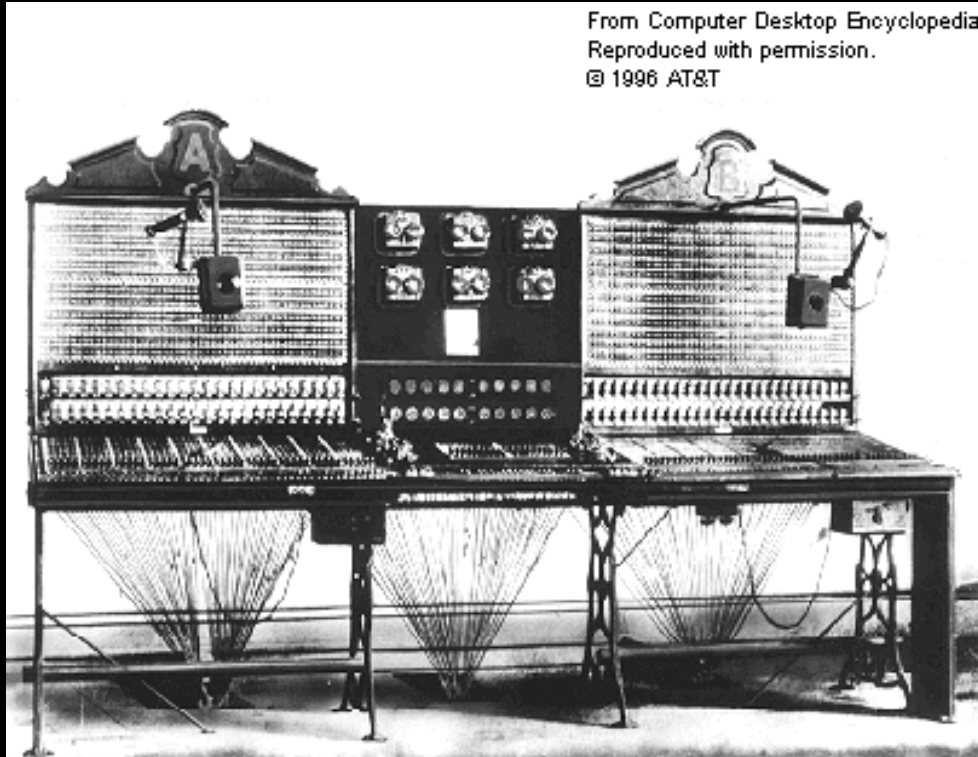
# Payphone attacks



- 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 !

Command Prompt

```
C:\Documents and Settings\user1>cd c:\tools
```

C:\tools>C:\tools>C:\tools>C:\tools>

**THC-SCAN.EXE**

TIME	STATISTIC	LOG WINDOW
Start » 19:14:23	Done : 1	19:14:23 Auto Saving DAT File ..
Now » 19:14:58	To Do : 9999	19:14:23 UnDialed : 10000
ETA » 20:27:08	Dials/H: 103	19:14:23 Excluded : 0
Timeout » 34/50	Carrier: 1	19:14:23 Done : 0
Rings » 0/6	Tones : 0	19:14:23 To Do : 10000
<b>FOUND!</b>	UMB : 0	19:14:23 Dialmask : 555XXXX
555-9686 CARRIER	Voice : 0	19:14:23 Scan Mode: Carrier
	Custom : 0	19:14:23 Dialing : undialed, bu
	Busy : 0	19:14:23 Scan started
	Others : 0	19:14:23 5559686 Connecting...
	2ndary : 0	

**MODEM WINDOW**

```
ATDT5559686
```

GREETINGS PROFESSOR FALKEN

HELLO

A STRANGE GAME.  
THE ONLY WINNING MOVE IS  
NOT TO PLAY.

HOW ABOUT A NICE GAME OF CHESS?

\* FINAL \* THC-SCAN v2.00 (c) 1995-98 by van Bommel/THC \* FINAL

# Telco maintenance modem access

```
ATDT01539422404
```

```
BUSY
```

```
ATDT01539422404
```

```
CONNECT 2400
```

```
AlphaServer 1000A 5/300 VMS Alpha V8.3 MSW,
```

```
Username: █
```

Shout a login/password! NOW!

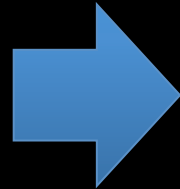
# Telco maintenance modem access (2)

- 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)

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



# 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 terminal)
1	Analog line



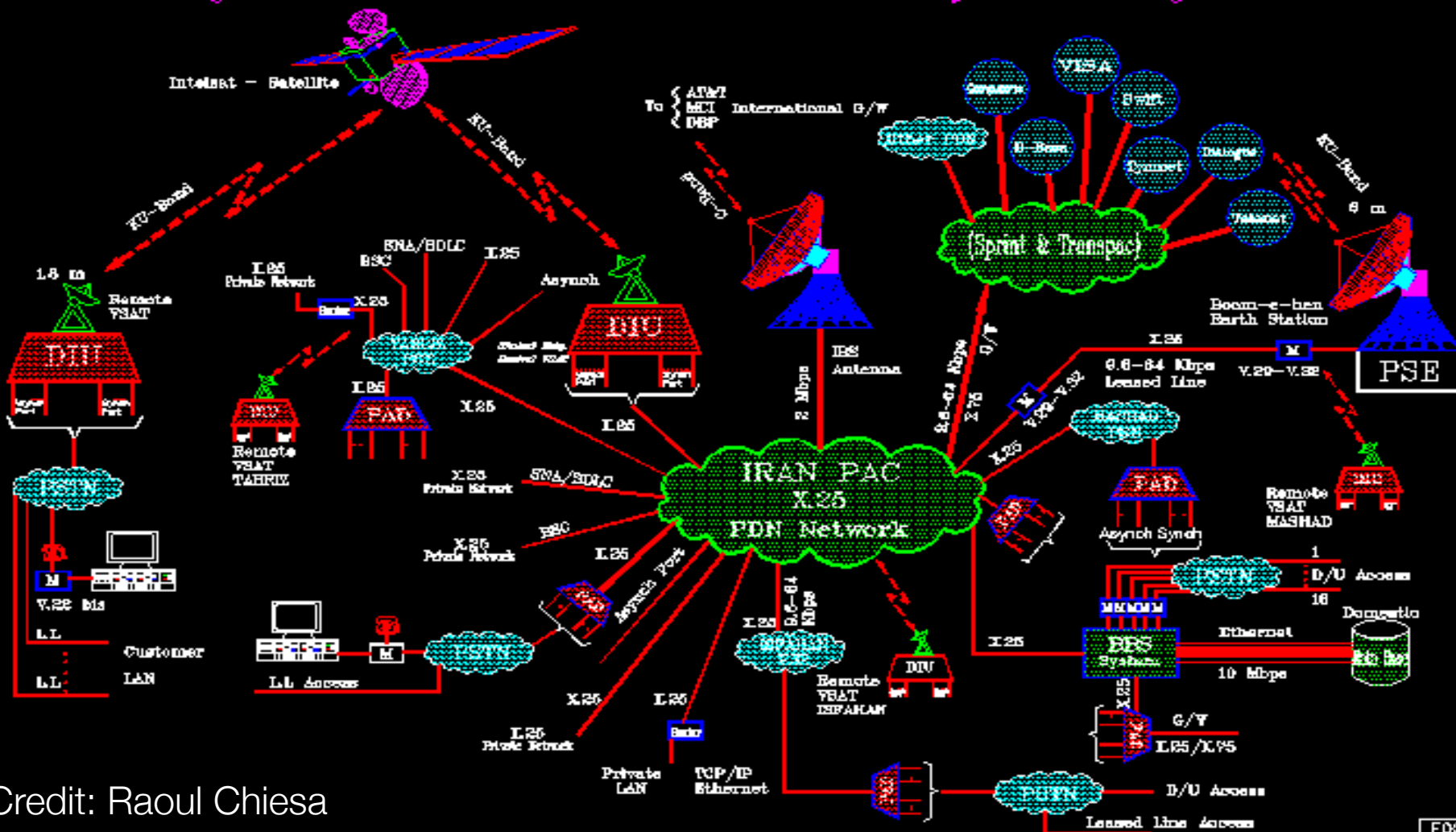
Millions of teenagers  
+ cheap modem and terminal  
+ eager to get cheap services  
= **What could possibly go wrong?**





# X25 networks

## Iran Packet Switched Public Data Network (Iranpac) *Integrated PDN & VSAT Network & Global Information System*



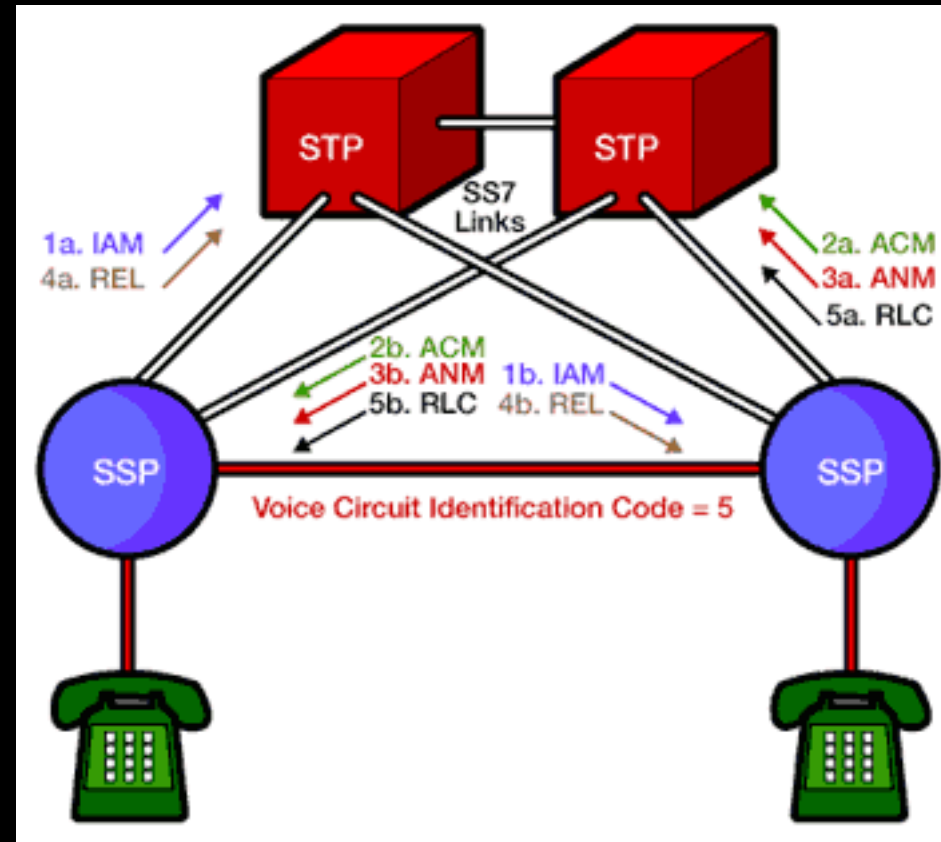
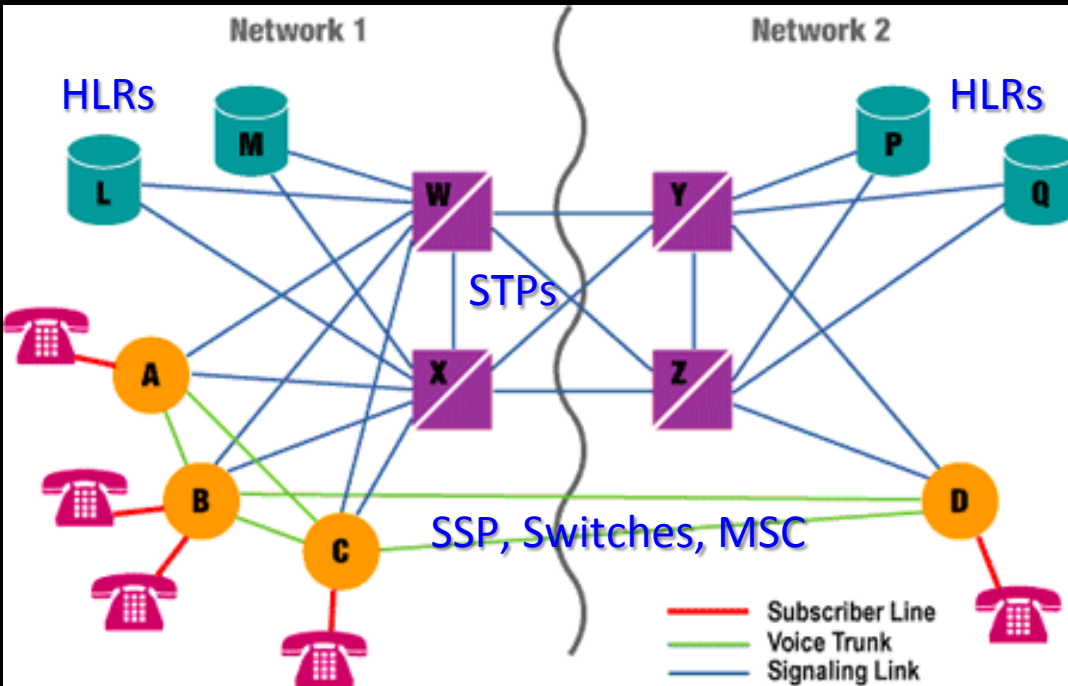
Credit: Raoul Chiesa

1990's

Golden Age



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



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

## 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)



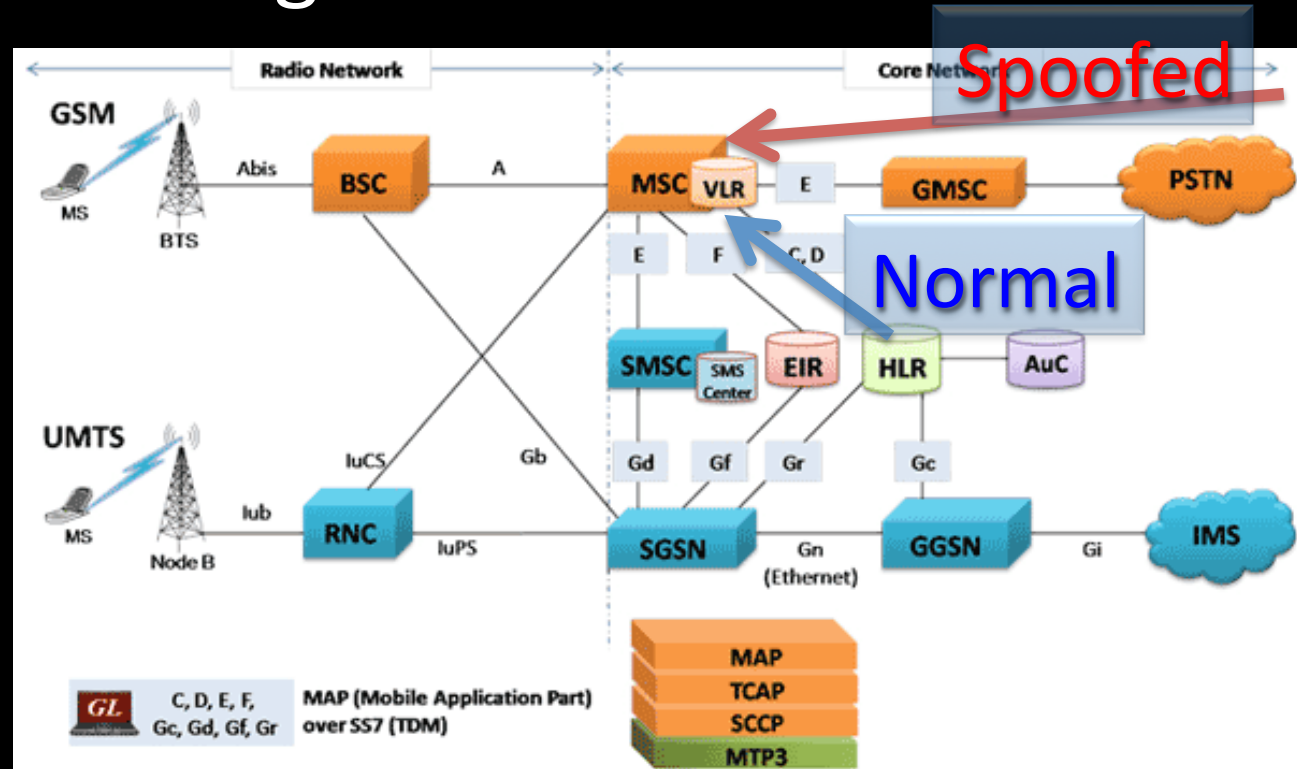
# SS7 ISUP IAM flood cause Denial of Service on MSC (3)

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 “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”

# 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)

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 “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

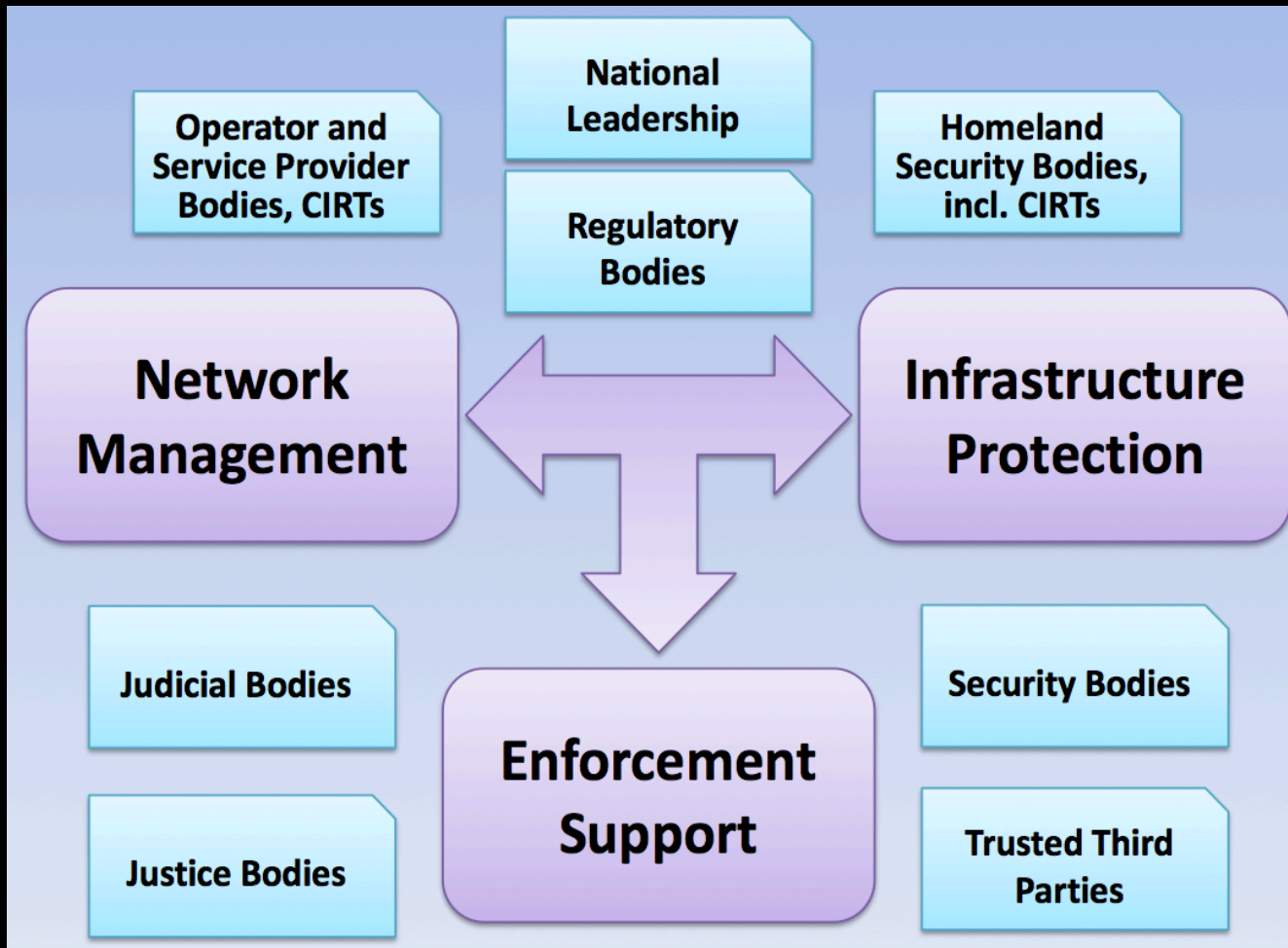
2000's

Momentum






# Interception Ecosystem



“Now we really understand security you know”

# Interception in the 1960's... evolved


**NEW** 

**NOW**  
*Telephone*  
**SURVEILLANCE**  
**WORK MADE EASY**

- ★ Makes telephone recordings automatically
- ★ No Attendant necessary
- ★ Adaptable to most any recorder
- ★ Can be used near or great distances from parent telephone
- ★ Now being used successfully by police and law enforcement agencies nationally

An Electronic Transistorized control unit for automatically controlling the manual operating functions of any standard sound recording machine to record sound from telephone line. Unit will operate from any recording machine which has sufficient torque to start in record position. Will work satisfactorily on any national or foreign telephone single or multiple line system. Recorder runs only when telephone is in use. Automatically starts when telephone is answered or used for calling. Automatically stops when telephone call is completed. May be used on off premise extension as distant as five miles from parent phone by direct parallel connections. Can also be used to detect numbers called by the click method. Cannot be detected or heard by parent phone. Operates from self-contained power supply 115 volt A.C. 60 cycle.

DESIGN PATENT 30220601



See your industrial Electronic Distributor or use the Readers Service card for catalogue and your nearest distributor.

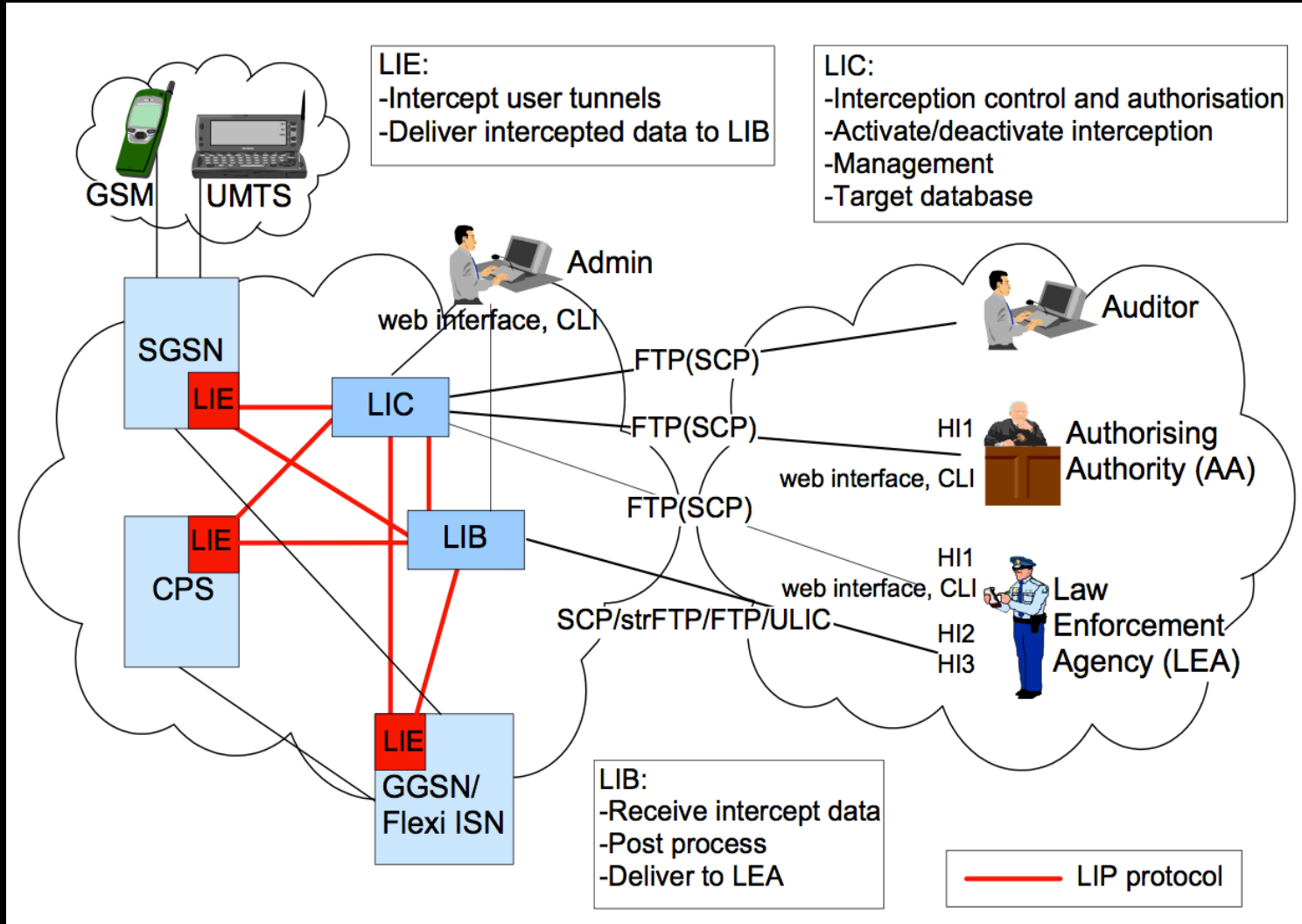
Export Division: **EMEC, Inc.**  
127 Grace St. Plainview, L.I., N.Y.

**NET PRICE**  
**\$79 95**

NOTE: Not intended for automatic telephone answering.



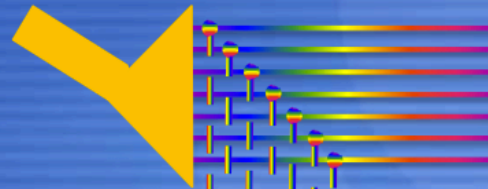
# Interception Overview



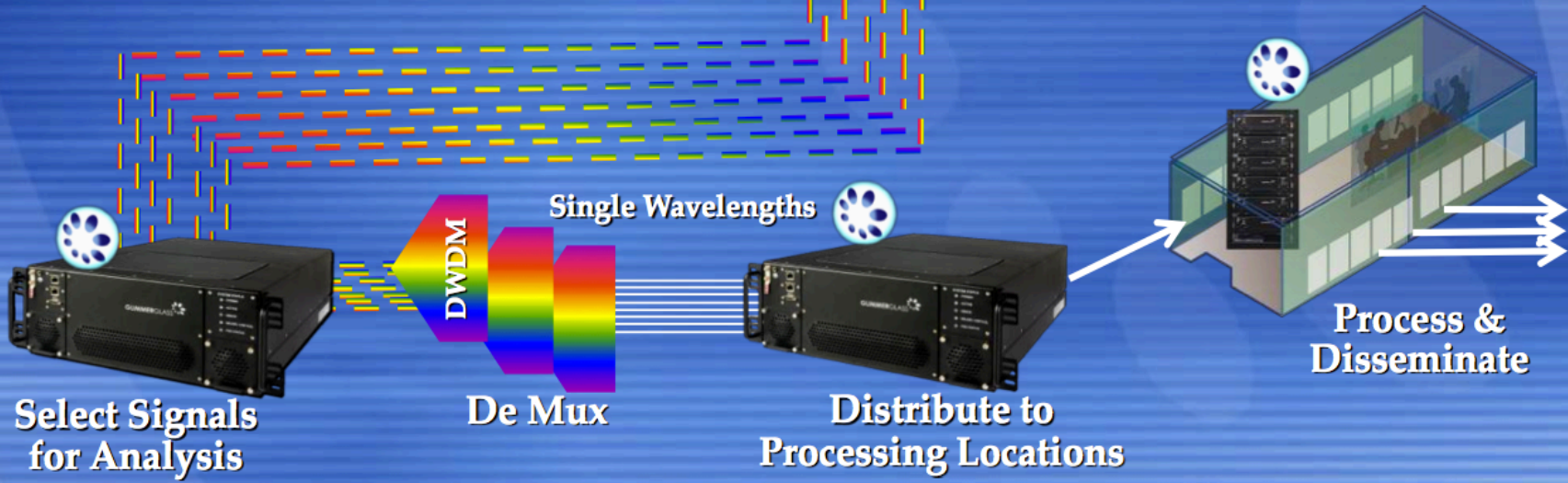
# Fiber Optics Interception

Targeted intercept of communications on behalf of a Law Enforcement Agency (LEA)

Carrier POP

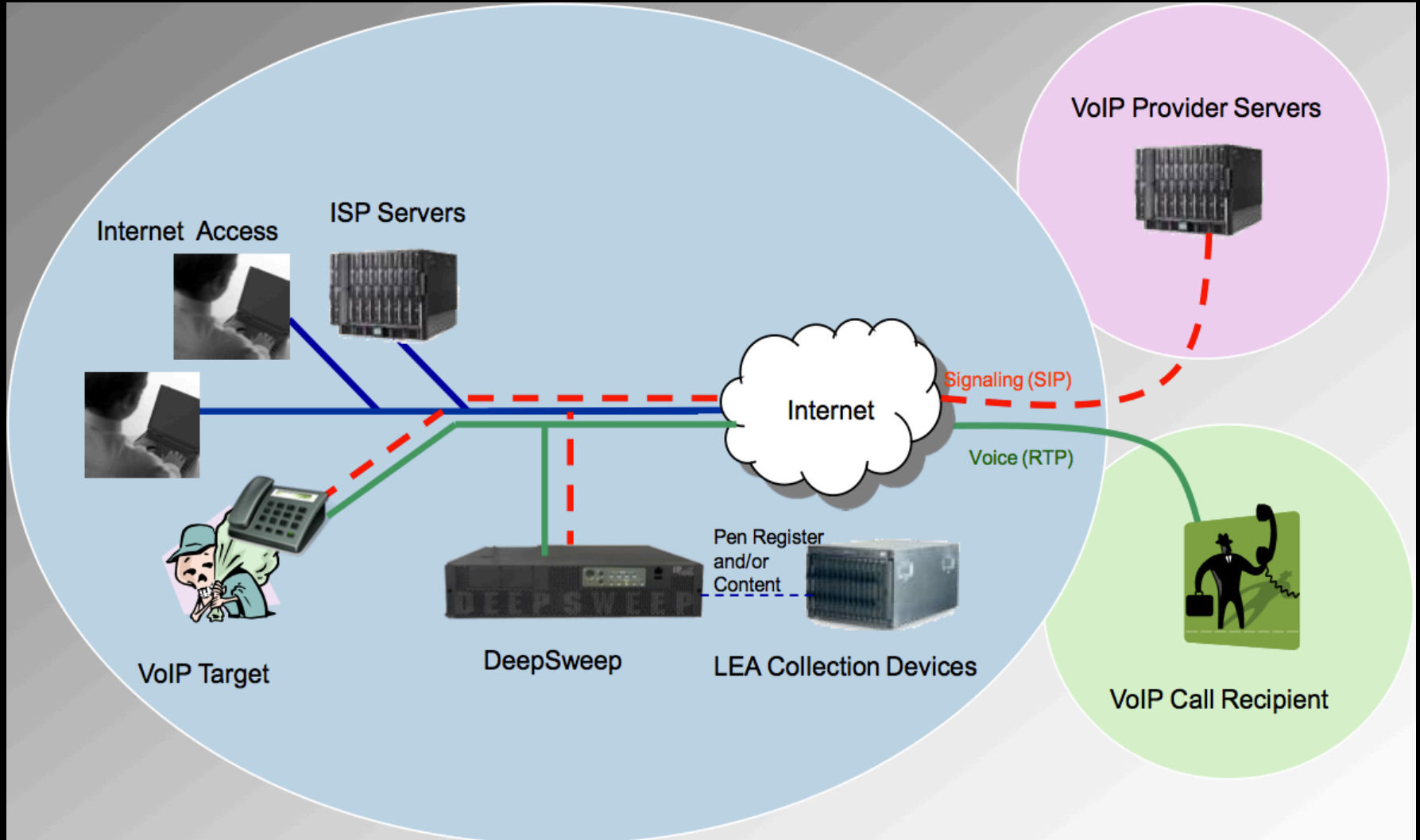


“Cooperation Point”



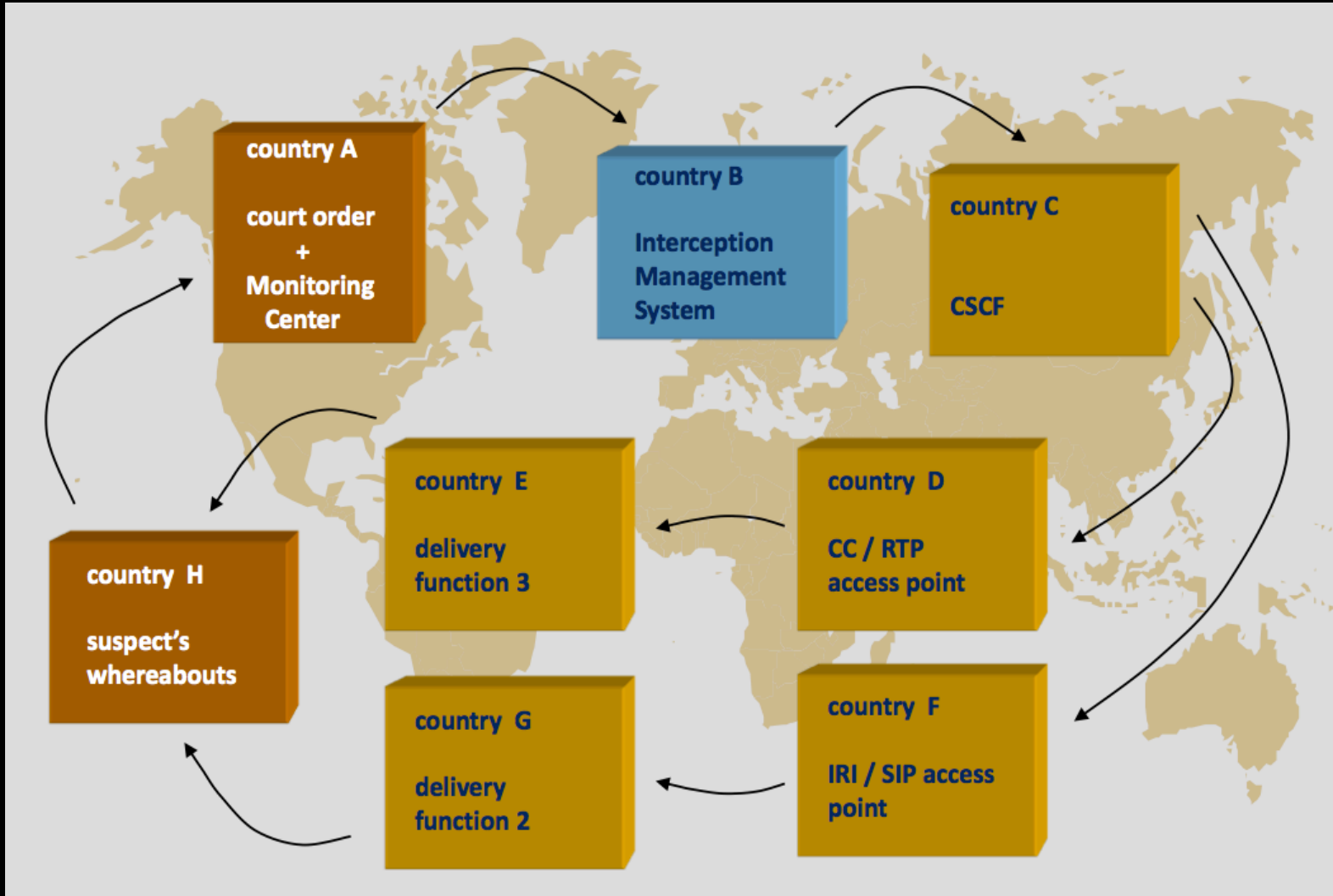
Oh, where is the judge?

# VoIP Interception

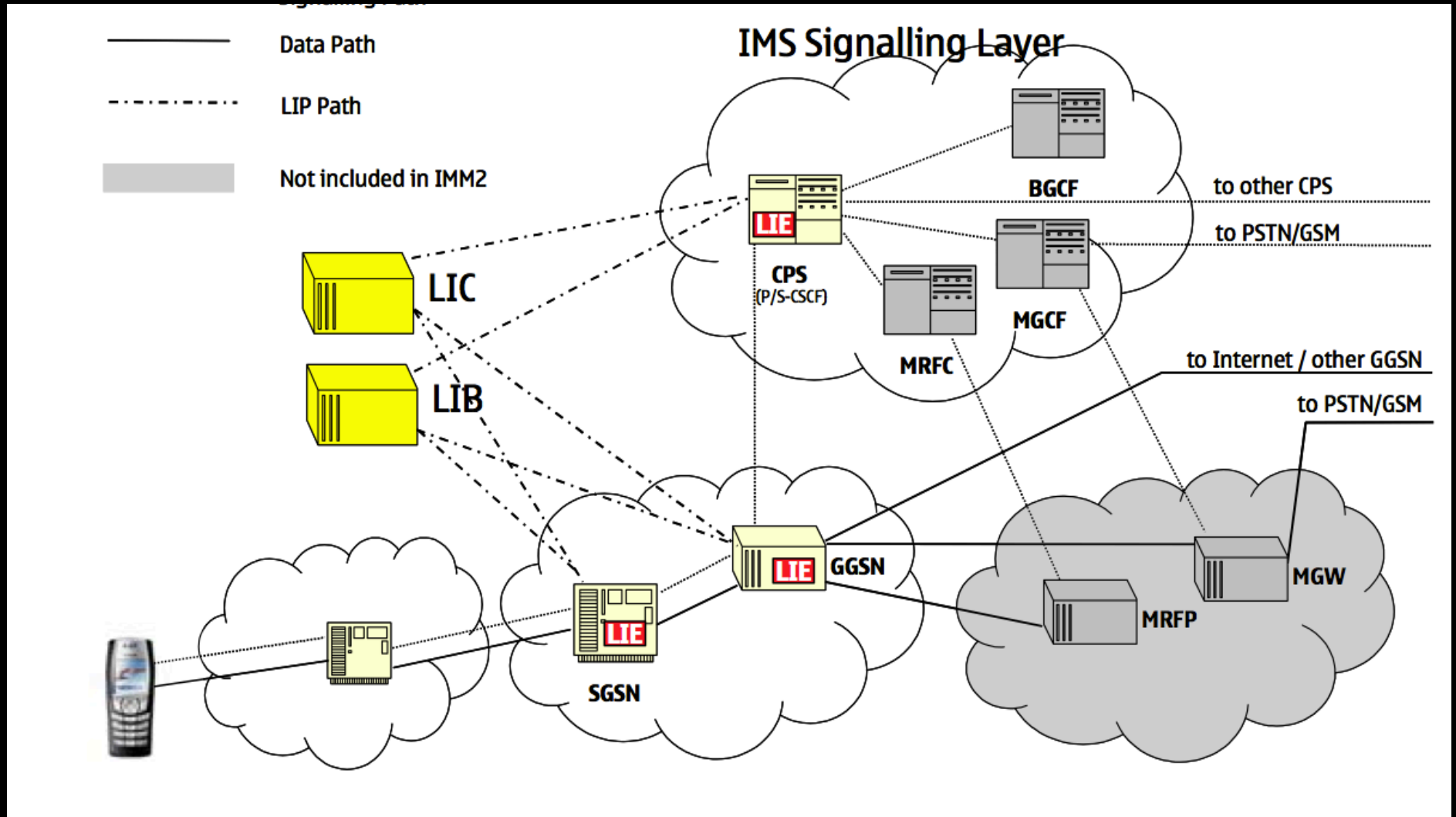




# VoIP Interception



# 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


### Smartphone 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



**ITALIANS**  
*Do it better!*

# Tactical Interception



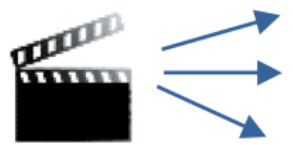
- Receiving/Intercepting
- Discretion for long-term intelligence
- Listening



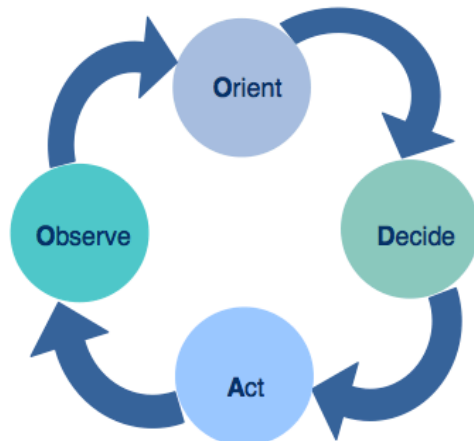
- Direction finding/Locating
- Mobility for tracking
- Recording /Replay
- Analysis



- Data base management
- Mapping/Simulations
- Targetting



- Locate
- Homing/Tracking
- Jamming/Neutralizing



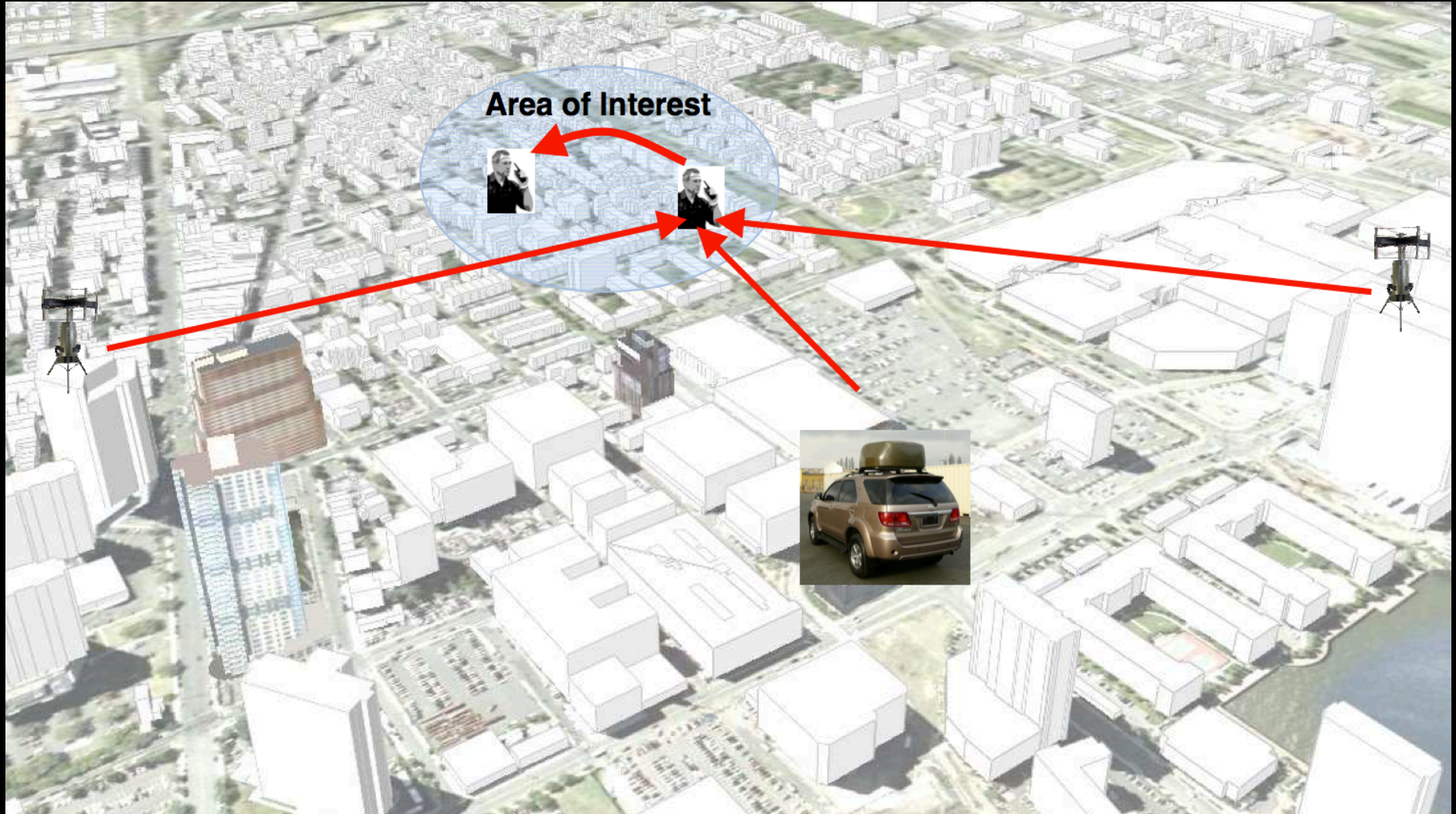


# Passive Interception System

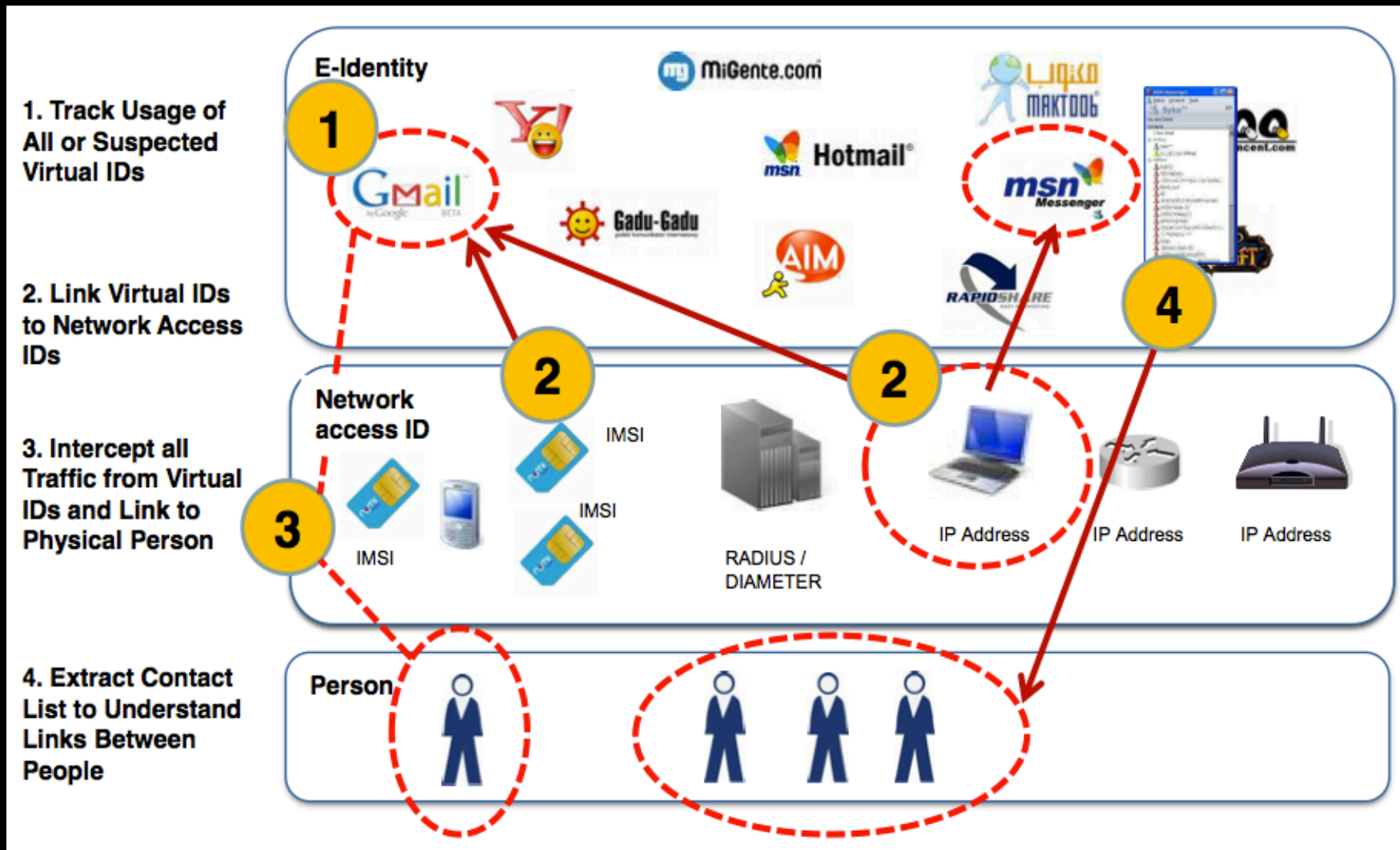




# Accurate Interception



# Virtual Identities to Real Persons





# POP / IMAP Interception

The screenshot displays a POP3 email client interface with a toolbar at the top containing icons for various functions like POP3, Delete, Search, and Account List. Below the toolbar is a table of email messages. The third message is selected, and its content is shown in a preview window. The email subject is "Football: Australia makes bid for 2018 World Cup".

No.	Date-Time	Account	Sender	Receiver	CC	Subject	Size	Similar Search	Whols
1.	2009-02-01 14:39:24	frankie	frankie@digi-fo...	frankie@digi-fo...		FW: U.S. needs Iran&#0...	82.31K		
2.	2009-02-01 14:39:24	frankie	decision@ed-sys...	frankie@ed-syst...	frankie@di...	FW: Govt rejects ultim...	172.85K		
3.	2009-02-01 14:39:24	frankie	frankie@ed-syst...	frankie@ed-syst...	frankie@di...	FW: Football: Australi...	126.43K		

The email preview window shows the following details:

- Subject: FW: Football: Australia makes bid for 2018 World Cup
- From: frankie <frankie@ed-system.sg>
- Date: 2/1/2009 2:08 PM
- To: frankie@ed-system.sg
- Cc: frankie@digi-forensics.com

The main body of the email contains the following text:

**Football: Australia makes bid for 2018 World Cup**

MELBOURNE: Australia have formally lodged their bid to host the 2018 or 2022 Fifa World Cup. Federation Australia (FFA) Chairman Frank Lowy said Sunday.

Initial expressions of interest to Fifa, the world governing body for the sport, are required by Monday.

"We have submitted Australia's expression of interest in hosting either the 2018 or 2022 World Cup," Lowy said in a statement.

Attachments include "Language.doc" and "pca\_fwz\_cpq2\_jpg\_b2000.jpg".

Red arrows indicate the flow of information from the email content to external lookup tools:

- An arrow points from the sender's email address (frankie@ed-system.sg) to a "who.is" website showing domain registration details for "hinet.net".
- Another arrow points from the "Src IP: 122.116.65.211" field in the email header to a "Query Result" section showing the IP address and its corresponding host: "HOST : 122-116-65-211 HINET - IP hinet.net".
- A third arrow points from the "Query Result" section to a Google Maps interface showing the geographical location of the IP address.

# Chat Interception

The screenshot displays an MSN account list with columns for No., Date-Time, Account, User Handle, Participants, Conversation, Count, and Similar Search. A red arrow points from the selected conversation (No. 15) to a detailed chat history window.

No.	Date-Time	Account	User Handle	Participants	Conversation	Count	Similar Search
9.	2008-09-22 09:56:23	VIC-TEST	diesis@ms62.hinet.net	dick691111@yahoo.com.tw	↓Conversation	20	
10.	2008-09-22 09:32:21	VIC-TEST	diesis@ms62.hinet.net	she0430@hotmail.com	↓Conversation	11	
11.	2008-09-22 09:10:59	VIC-TEST	diesis@ms62.hinet.net	shmily.d0613@msa.hinet.net	↓Conversation	48	
12.	2008-09-22 09:10:59	FLYY	shmily.d0613@msa.hinet.net	diesis@ms62.hinet.net	↓Conversation	48	
13.	2008-09-22 09:10:59	FLYY	shmily.d0613@msa.hinet.net	philip12129@hotmail.com	↓Conversation	8	
14.	2008-09-22 10:21:09	FLYY	shmily.d0613@msa.hinet.net	dick691111@yahoo.com.tw	↓Conversation	28	
15.	2008-07-02 10:43:23	192.168.1.13	wedetective@hotmail.com	wedetective2@hotmail.com	↓Conversation	7	
16.	2008-07-02 10:43:23	FRANKIE-PC	wedetective2@hotmail.com				

No.	Date-Time	User Handle	Type	Message	View started	Flash Time
1.	2008-07-02 10:40:06	wedetective2	Message	hello		
2.	2008-07-02 10:40:07	wedetective2	Message	good morning		
3.	2008-07-02 10:40:09	wedetective2	Message	how r u?		
4.	2008-07-02 10:40:19	wedetective1	Message	hi		
5.	2008-07-02 10:40:21	wedetective1	Message	I am fine		
6.	2008-07-02 10:40:22	wedetective1	Message	thank you		
7.	2008-07-02 10:40:42	wedetective1	File			
8.	2008-07-02 10:40:55	wedetective1	File	Customer Request Form.pdf		
9.	2008-07-02 10:42:21	wedetective1	Message	thank you!!		
10.	2008-07-02 10:42:29	wedetective2	Message	welcome		
11.	2008-10-12 20:50:40	wedetective1	Audio		2008-07-02 10:41:02	2008-07-02 10:41:28
12.	2008-10-12 20:50:40	wedetective1	Audio		2008-07-02 10:41:02	2008-07-02 10:41:28
13.	2008-10-12 20:50:40	wedetective1	Audio		2008-07-02 10:41:02	2008-07-02 10:41:28
14.	2008-10-12 20:50:40	wedetective1	Video		2008-07-02 10:41:02	2008-07-02 10:41:28

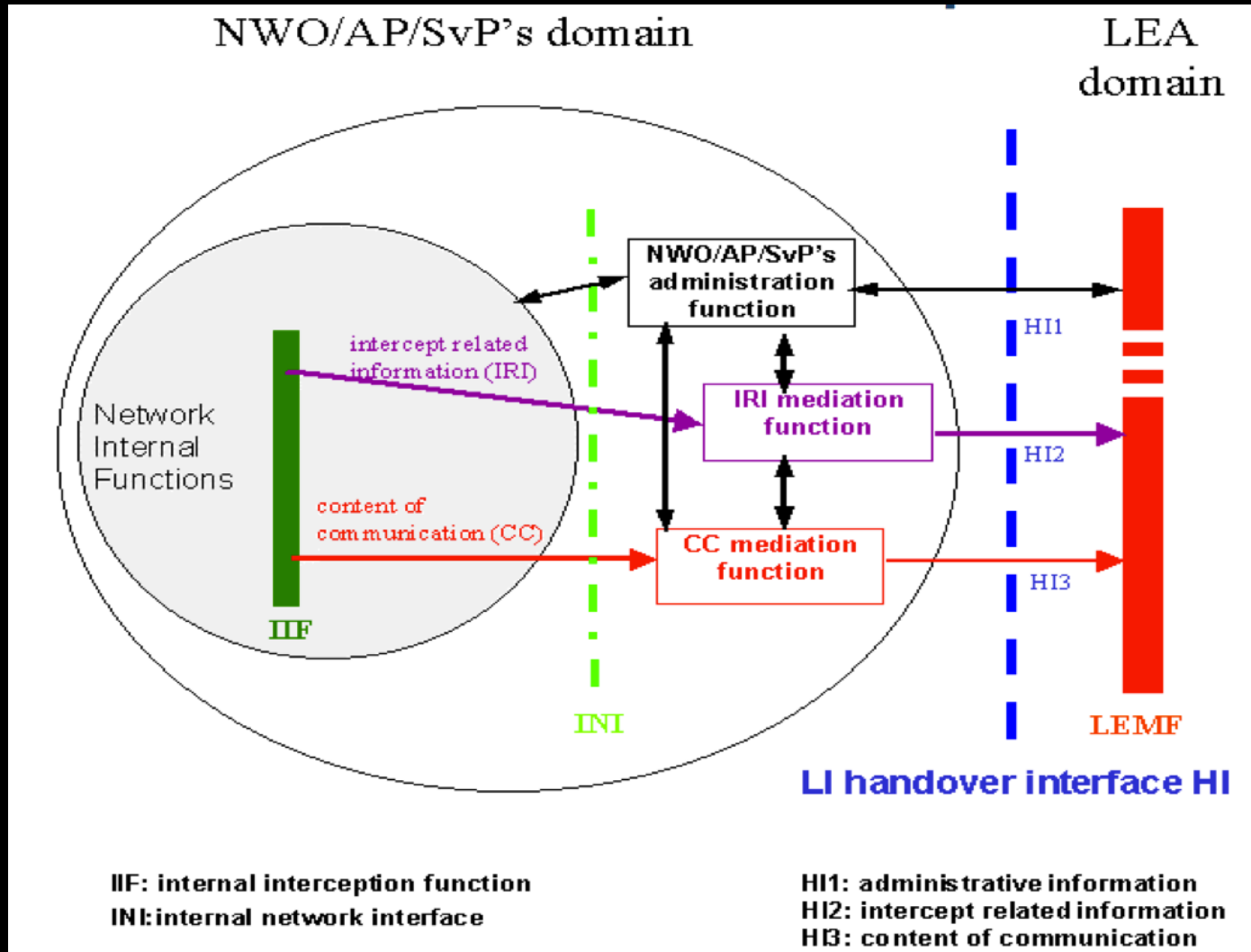
# Top 10 LEA Challenges

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,

A Jeopardy! game board with six columns and five rows. The columns are labeled with categories: ROMAN ART, ANIMALS, TV MDs, UNOFFICIAL STATE NICKNAMES, BERRY, BERRY GOOD, and AIN'T THAT AMERICA. The rows are labeled with dollar amounts: \$200, \$400, \$600, \$800, and \$1000. All cells in the board contain the same dollar amount as the row they are in, indicating that all questions in that row have the same value.

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

# 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, ...)

# Weapons of Mass Disruption



*When is an attack just “hacker mischief “ and when is it a matter of national security?*

*Is the cyber attack coordinated against a particular country or is it just a general attack?*

*How did the blueprints for our country’s top secret weapon system end up abroad?*

*Are disruptions at banks, electricity grids or airport navigation systems due to technical problems or is it a cyber attack?*

# Vodafone Femtocell intrusion

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

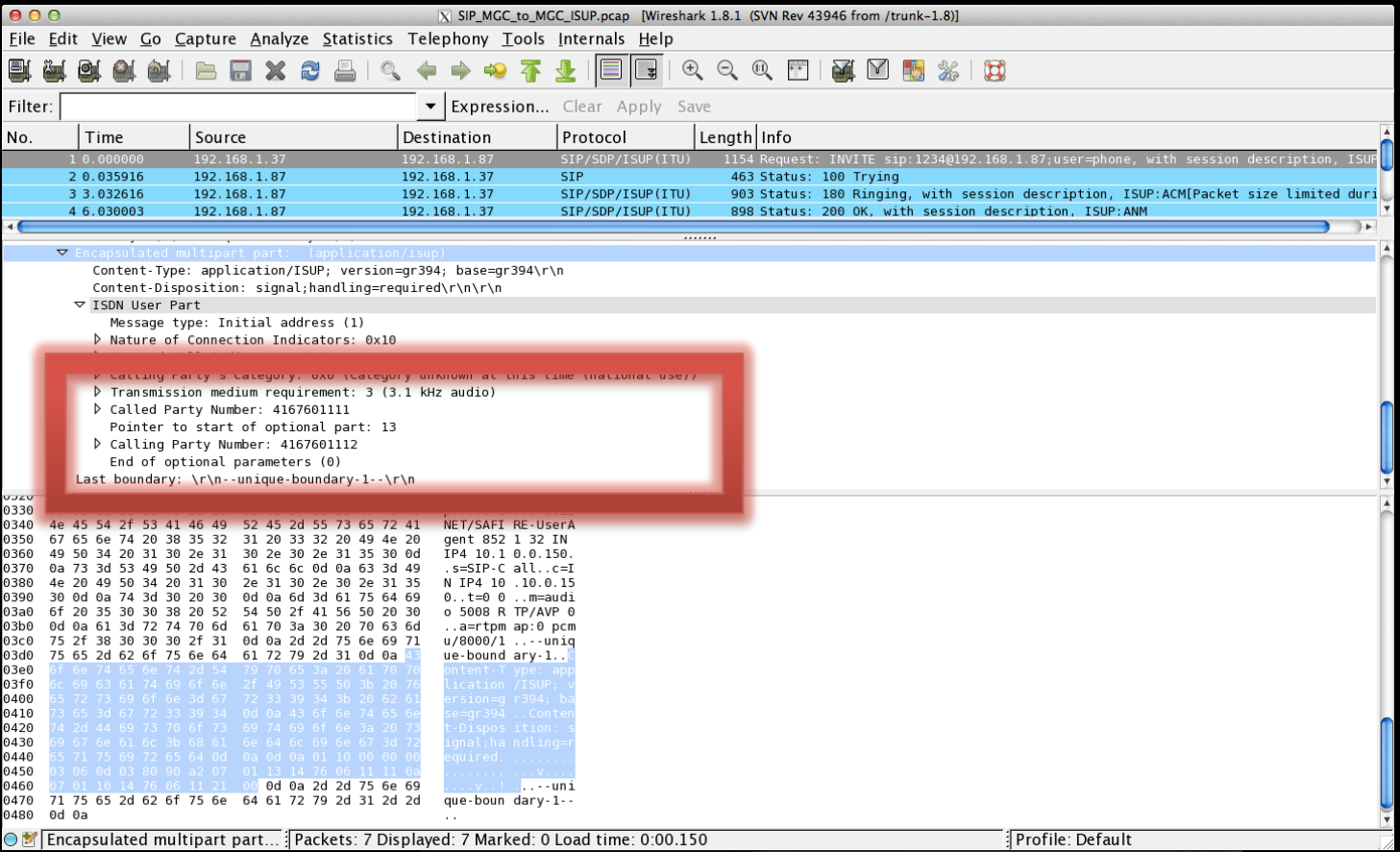




# VoIP catastrophes... just worse

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!”

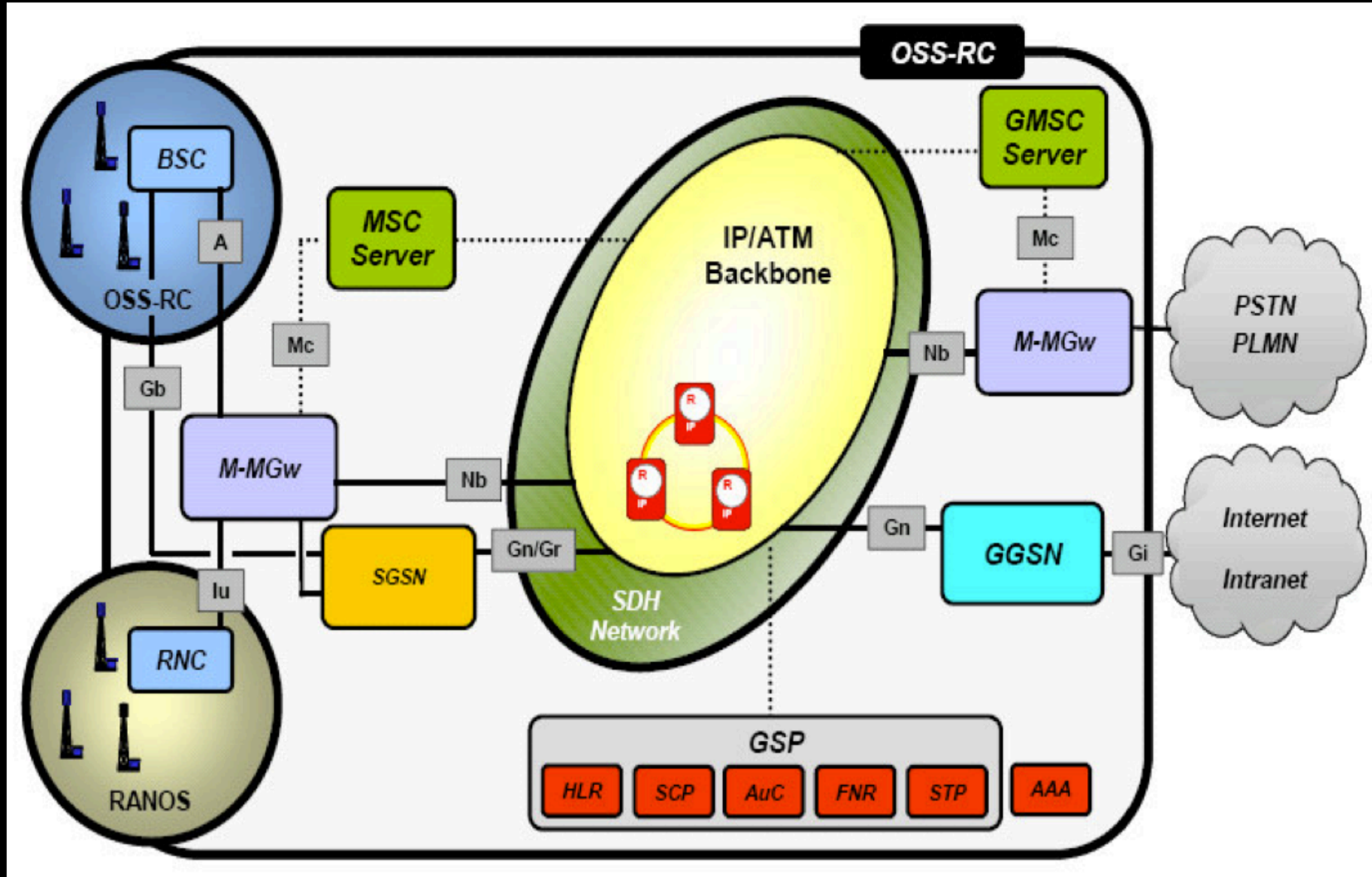


# Vendor Attempts at Security

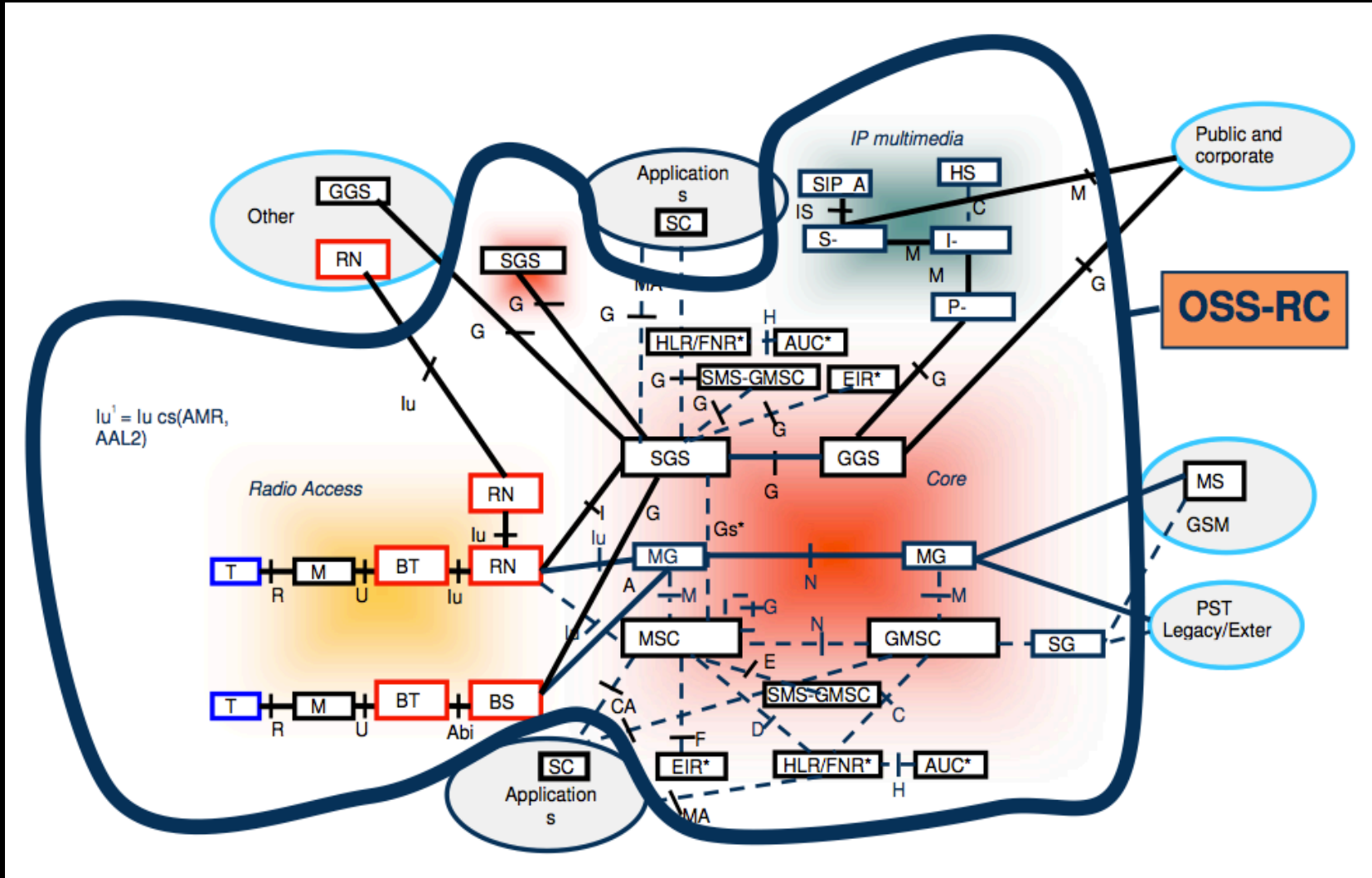
Security Functional Class	Security Functional Requirement	Component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
Security Audit (FAU)	FAU_GEN.1 Audit data generation	FAU_GEN.1	CC Part 2	No	No	Yes	Yes
	FAU_GEN.2 User identity association	FAU_GEN.2	CC Part 2	No	No	No	No
	FAU_SAR.1 Audit review	FAU_SAR.1	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, ...)

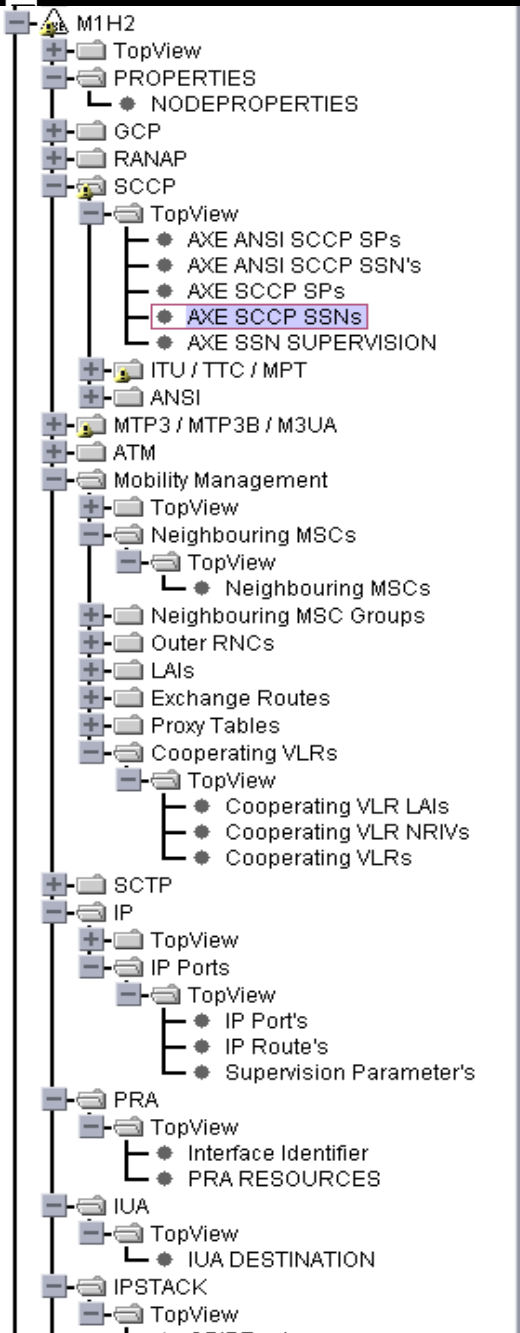
# Core Network gets complicated



# OSS



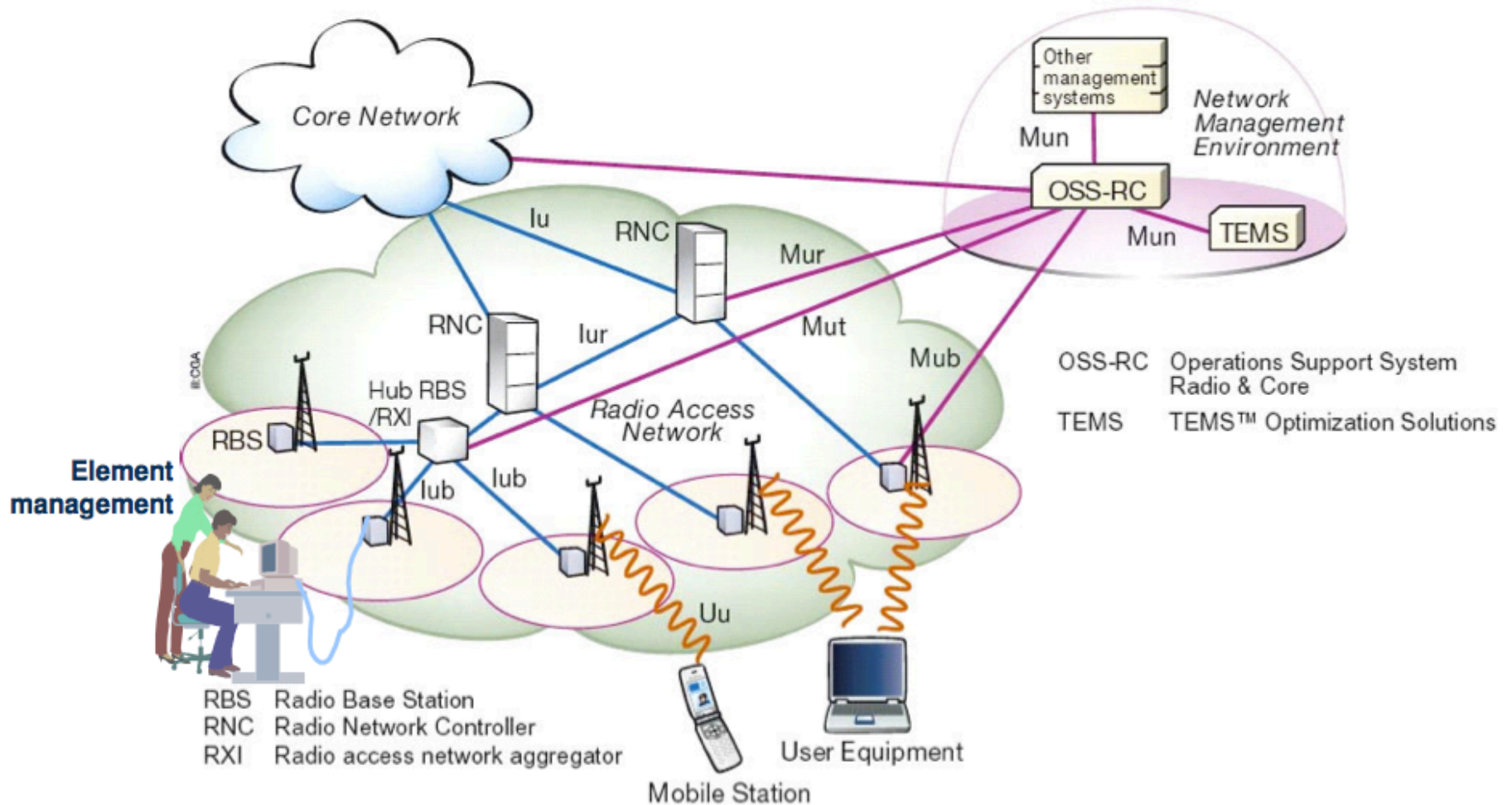




M1H2	2-1505	15	YES
M1H2	2-1506	15	YES
M1H2	2-1507	15	YES
M1H2	2-1510	15	YES
M1H2	2-1511	15	YES
M1H2	2-1512	15	YES
M1H2	2-1513	15	YES
M1H2	2-1528	15	YES
M1H2	2-1529	15	YES
M1H2	2-1556	146	YES
M1H2	2-1556	6	YES
M1H2	2-1556	8	YES
M1H2	2-302	146	YES
M1H2	2-302	6	YES
M1H2	2-302	8	YES
M1H2	2-303	146	YES
M1H2	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

## WCDMA Radio Access Network



- 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

GNIP	Information Item	GNIP GUI	Type
------	------------------	----------	------

**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

PerceivedSeverity	AlarmId	ObjectOfReference	Acknowledg
Critical	721166292	rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103	eabbkhn_at_NME
Critical	721166298	rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103	eabbkhn_at_NME
Critical	721166299	rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103	eabbkhn_at_NME
Critical	721166300	rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103	eabbkhn_at_NME
Critical	721166301	rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103	eabbkhn_at_NME
Major	721165876	rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103	eabbkhn_at_NME
Major	721165877	rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103	eabbkhn_at_NME
Major	721165905	rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103	eabbkhn_at_NME
Major	721166243	rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103	eabbkhn_at_NME
Major	721166245	rk=ONRM_RootMo,SubNetwork=AXE,ManagedElement=M103	eabbkhn_at_NME
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.

**Alarm Status Matrix**

File Edit View Tools Help

M103+ 5 88 2 2	M1G1+ 17 18 12 29	M1S2+ 8 20 1
M1C5+ 17 1	M2N3+ 4 17 1	M182+ 3 1
GMPC1+	SMPC1+	SMSC_jagw0+ 1
LBS2+ 2	EMM1+ 2 4 11 6	

# 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	ObjectOfReference
Critical	EMG CONTROL DOWN	NW=AXE,NE=BSC4,EQ=
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

Acknowledged [1/51] Changed at 12:41:16 PM 0 1 0 0 0 0

PerceivedSeverity	SpecificProblem	ObjectOfReference
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	Acknc
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	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.

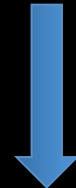
# Mobile Payments PIN attacks

```
- Component: invoke (1)
  - invoke
    invokeID: 0
    + opCode: localValue (0)
    + ussd-DataCodingScheme: 0F
      ussd-String: AA180D3602
      USSD String: *140#
    + msisdn: ██████████59020F7
```

0000 00 14 4f 9f c7 d6 00 12 da 01 94 00  
0010 00 e8 d7 c7 00 00 3f 84 3e 3a 0a 01  
0020 2f 84 0b 59 0b 5b 04 3b 62 63 56 97

```
- opCode: localValue (0)
  localValue: unstructuredSS-Request (60)
- ussd-DataCodingScheme: 0F
  0000 .... = Coding Group: Coding Group 0(Language
  .... 1111 = Language: Language unspecified (15)
  ussd-String: 31D98C56B301
  USSD String: 123456
```

00 14 4f 9f c7 d6 00 12 da 01 94 00 08 00 45 00 ..0....  
00 a4 08 7b 00 00 3f 84 0d cb 0a 01 21 0b 0a 01 ...{..?  
2f 84 0b 59 0b 59 ab 2f a4 d0 23 04 9c 34 00 03 /..Y.Y./  
00 84 38 72 3f 56 00 0a f5 44 00 00 00 03 01 00 ..8r?V..



```
- opCode: localValue (0)
  localValue: unstructuredSS-Request (60)
- ussd-DataCodingScheme: 01
  0000 .... = Coding Group: Coding Group 0(Language using the GSM 7
  .... 0001 = Language: English (1)
  ussd-String: 5076393C2F83CA6E7A590ECABFEB72900D444E9FD374501B...
  USSD String: Please enter your 6 digit mPIN
```

0 00 12 da 01 94 00 00 14 4f 9f c7 d6 08 00 45 00 ..... 0.....E.  
0 00 ec 53 ae 40 00 40 84 81 4f 0a 01 2f 84 0a 01 ..S.@.@. .0../...  
0 21 0b 0b 59 0b 59 11 51 f4 45 b0 84 48 98 03 00 !..Y.Y.Q .E..H...

```
- ussd-DataCodingScheme: 01
  0000 .... = Coding Group: Coding Group 0(Language u
  .... 0001 = Language: English (1)
  ussd-String: 31172819A42A642E50F32D4EB3CBA0E6DB5DCE2B6
  USSD String: 1. IAT
  2. Mobile Money
  0. Logout
```

00 12 da 01 94 00 00 14 4f 9f c7 d6 08 00 45 00 .....  
00 b4 ad 3a 40 00 40 84 23 ec 0a 01 2f 84 0a 10 ...:@.0  
25 0b 0b 5a 0b 59 67 78 c6 33 90 f2 f1 8f 03 00 %..Z.Y0



# 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
[REDACTED]516	8997[REDACTED]	02019390764	427[REDACTED]0015701
[REDACTED]519	8997[REDACTED]	02044606663	427[REDACTED]1941155
[REDACTED]520	8997[REDACTED]	02056922529	427[REDACTED]3172882
[REDACTED]521	8997[REDACTED]	02004899993	427[REDACTED]0128201
[REDACTED]524	8997[REDACTED]	02031545395	427[REDACTED]0635053

```
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]
4539[REDACTED]	002563	13	EBTI
4324[REDACTED]	044384	13	EBTI
5318[REDACTED]	670032	13	EBTI
4539[REDACTED]	139861	13	RKRI
4565[REDACTED]	015545	13	RKRI
4341[REDACTED]	125773	13	EBTI
4909[REDACTED]	219000	13	HSHA
4483[REDACTED]	176947	137	AALJ
4909[REDACTED]	134016	13	SAMI
4565[REDACTED]	101482	13	SNAZ

SIM_NO	IMSI_NO	PUK	KI	ENCRYPTED_KIVALUE
89[REDACTED]	02019239516	427[REDACTED]	424014 34[REDACTED]	32373832 73A[REDACTED]
89[REDACTED]	02019239524	427[REDACTED]	424015 35[REDACTED]	36323537 F6F[REDACTED]
89[REDACTED]	02019239557	427[REDACTED]	424018 33[REDACTED]	32373339 1EA[REDACTED]
89[REDACTED]	02019239565	427[REDACTED]	424019 35[REDACTED]	31323335 483[REDACTED]



# Insecure Clients Repositories

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

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

@usagold.com

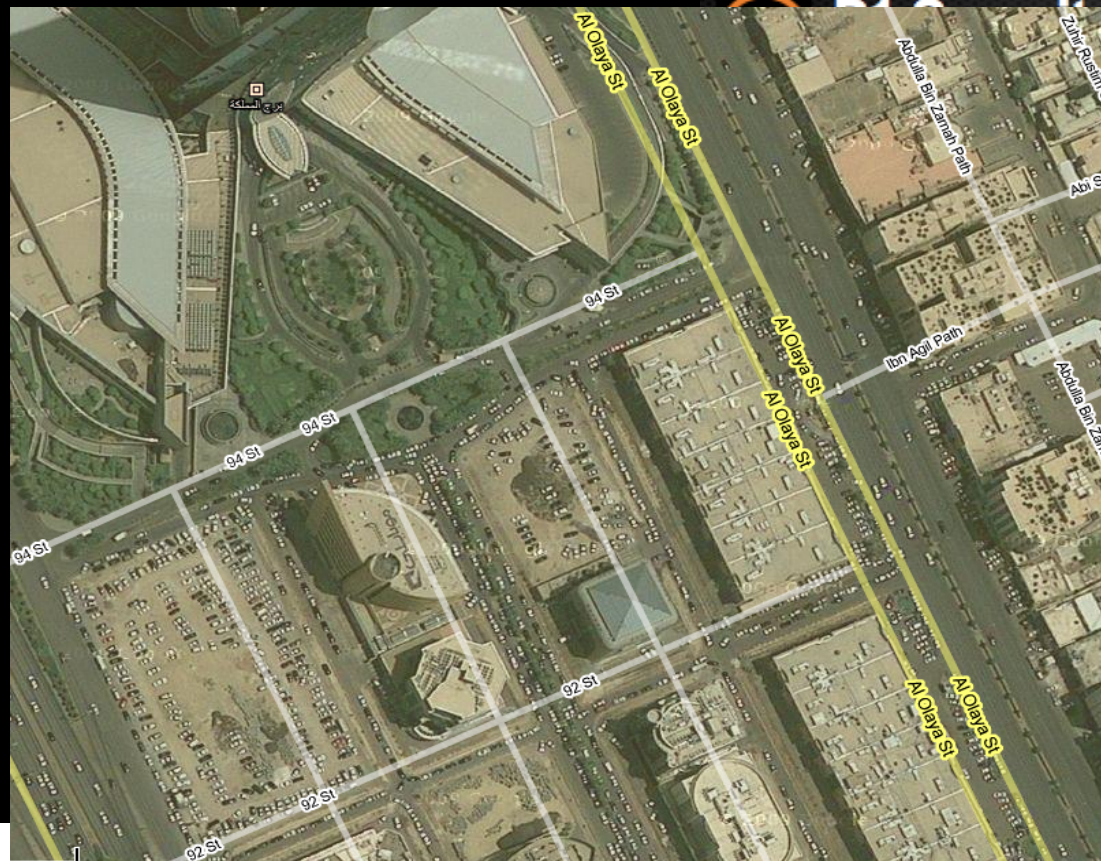




# TSTF

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]	14447257	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]	4444725	2525		Mon Oct 19 17:16:15 AST 2009	<input type="button" value="Resend"/>
				location 0544811486			



# Prepaid Vouchers Counterfeiting

MINSAT - Cust Care Config

Task Search View Reset Help

Cust Care Config

Title:	MINSAT for CS	Voucherless Refill Min:	0	Voucherless Refill Max:	1000000
Debit Min:	0	Debit Max:	1000000	Rebate Min:	0
Rebate Max:	1000000	Expiry Days:	10	Network Operator ID:	
Default SDP:	SDP01 (10.1.4.14)	Default Transaction Ty...:	General Adjustment	Default Transaction Co...:	General Adjustment
Default Home Region:		Primary Currency:	SAR	Bonus Amount:	10

Reset Sub Password:       Additional MML:

Secondary Currency:       Registration Bonus:

Bonus to Subordinates:

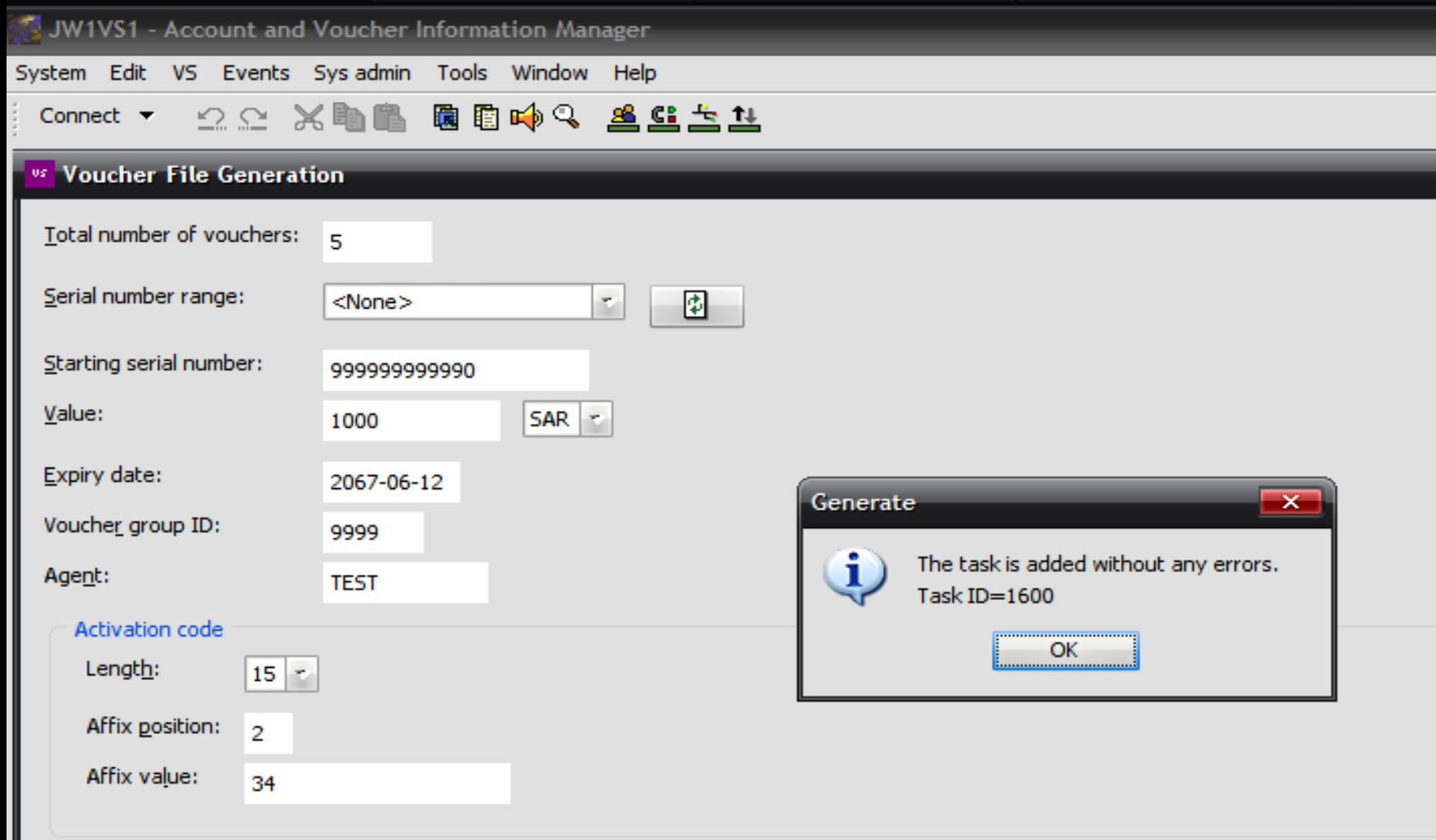
Submit

- Subscriber Admin
- Account Admin
- Subordinate Data
- Rebate
- Debit
- Language
- Notepad
- Service Class
- Name and Address
- Barring
- Advanced
- Voucher
- Promotion Plan
- Family and Friends
- Communities
- Service Offering
- Account Group
- USSD EOCN
- Account Home Region
- Voucher Based Refill
- Voucherless Refill

Customer Care Administration 1 Administration 2 O and M

Ready Super User: minsat [Operator: Host Organization]

# Print your own money



The screenshot shows the 'Voucher File Generation' window of the JW1VS1 software. The interface includes a menu bar (System, Edit, VS, Events, Sys admin, Tools, Window, Help) and a toolbar with various icons. The main area contains several input fields for configuring voucher generation:

- Total number of vouchers: 5
- Serial number range: <None>
- Starting serial number: 999999999990
- Value: 1000 SAR
- Expiry date: 2067-06-12
- Voucher group ID: 9999
- Agent: TEST
- Activation code section:
  - Length: 15
  - Affix position: 2
  - Affix value: 34

A 'Generate' dialog box is displayed in the foreground, indicating a successful operation:

**Generate**  
The task is added without any errors.  
Task ID=1600  
OK

# 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



# 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;
```

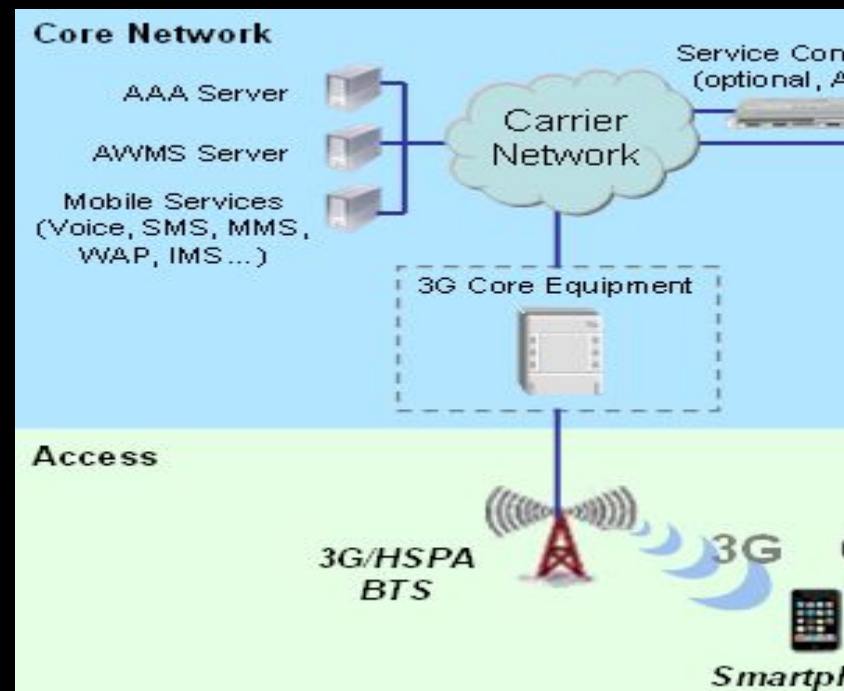
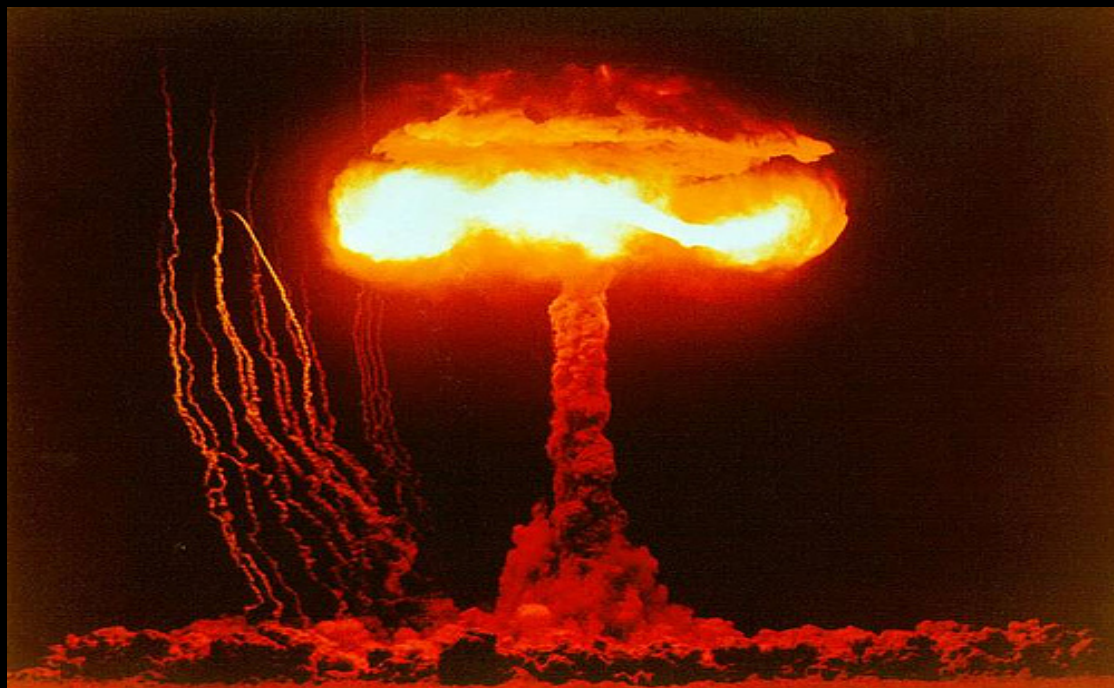
```
SP HARDWARE DATA
```

```
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	I0G20
WSU-1	MEMORY		WSU	****	1	32
SCSI-1	SCSI			****	3	5
VSA-1	EBA_VSA			****	1	1

# SIGTRAN injection from 3G mobile data

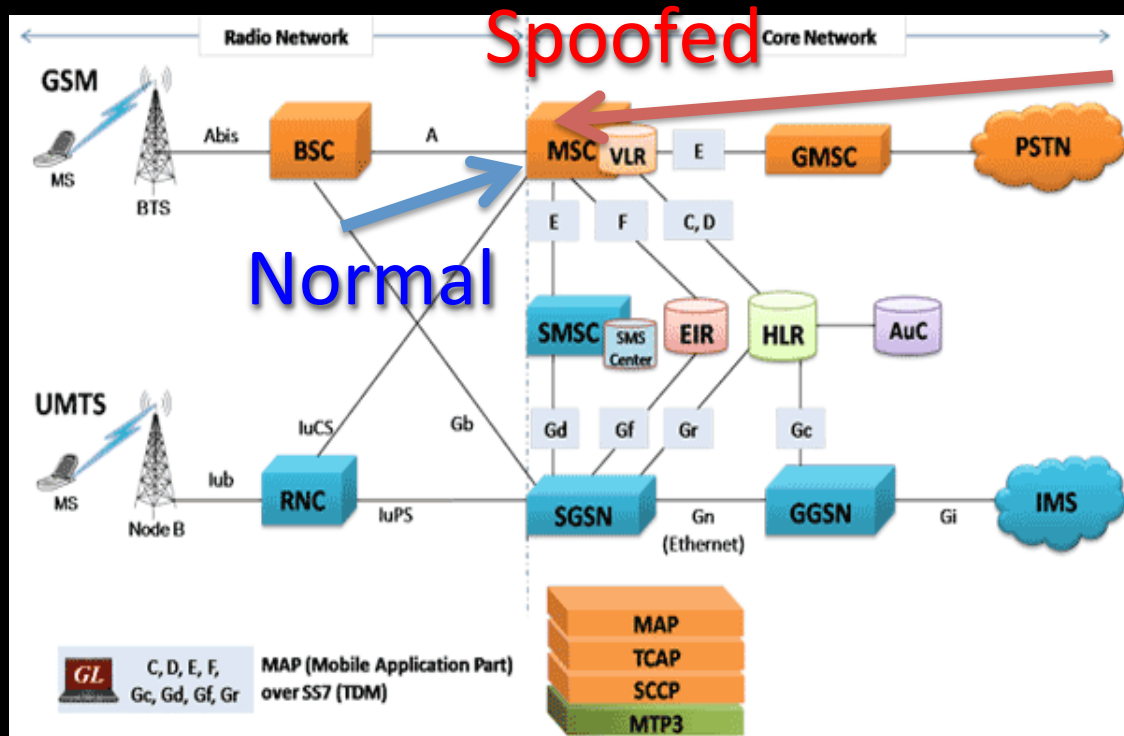
1. Establish 3G mobile data
2. Connect to SIGTRAN SS7 to 10.31.33.7 sctp/2905
3. Global DoS on the network possible





# 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

# Huawei MGW MML pseudo test signaling abuse capability

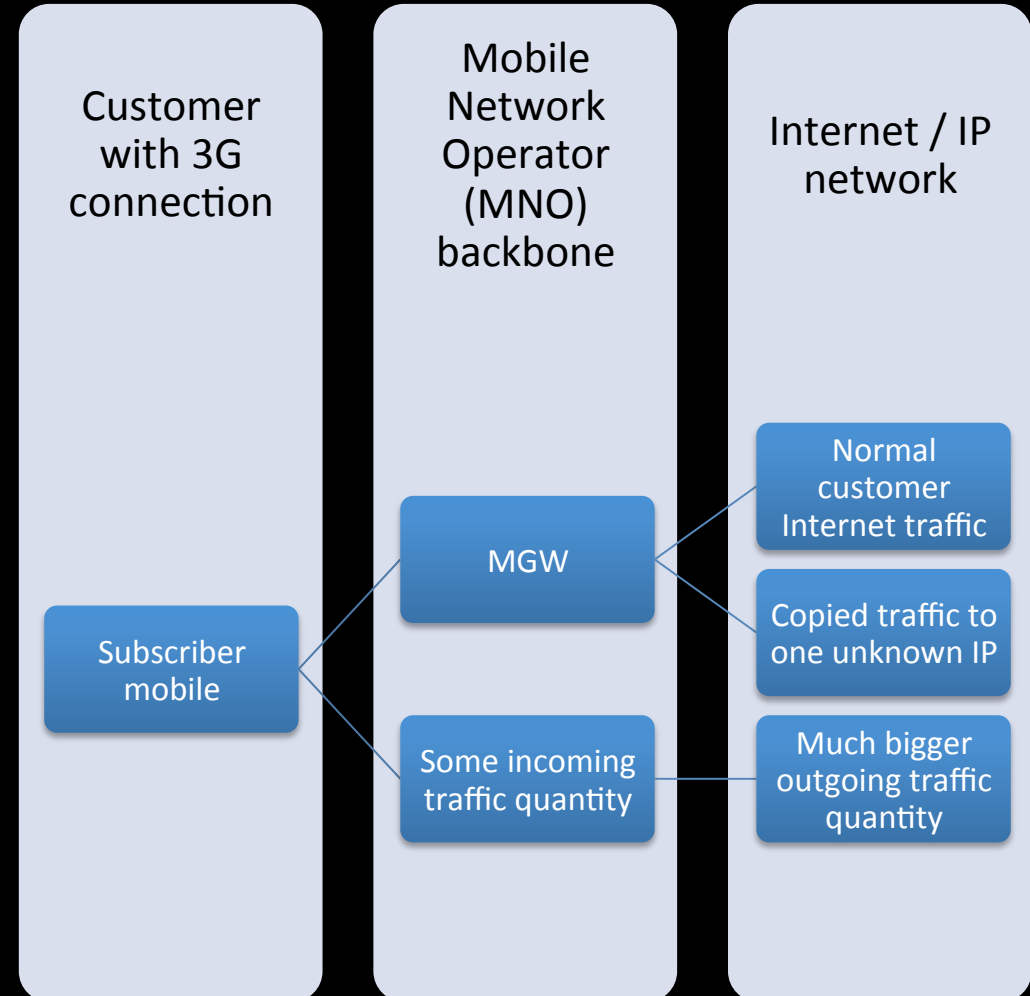
Severity	Critical
Description	Huawei MGW UMG 8900 has a MML command that enables total freedom in sending any kind of MSU content.
Impact	SS7 signaling injection capability

- 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!”**



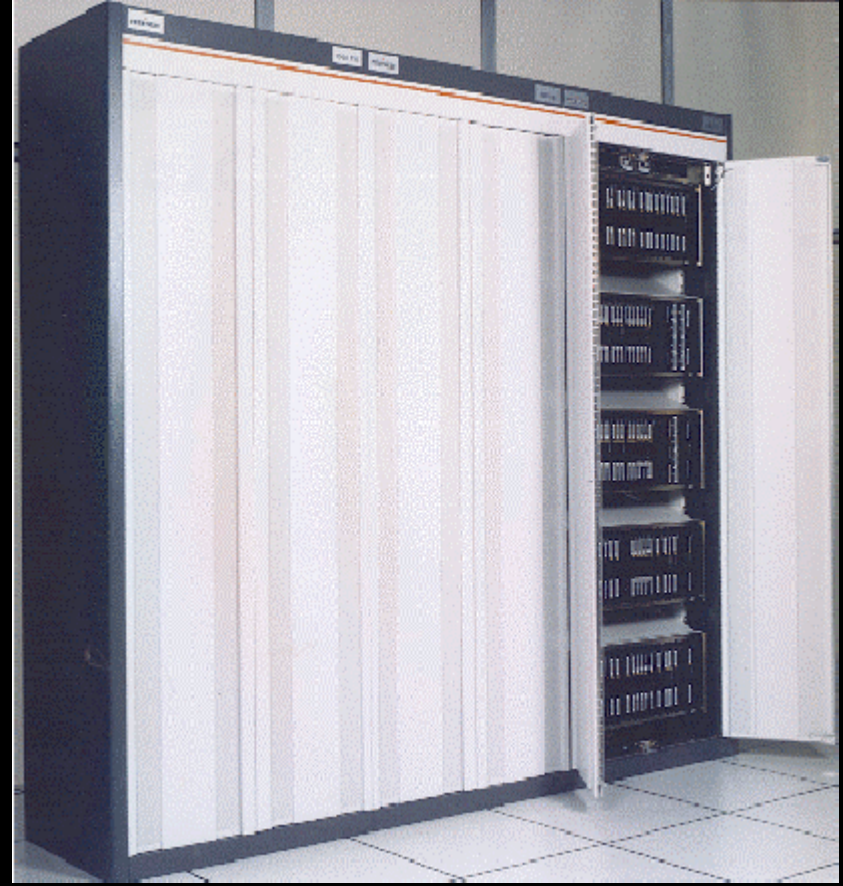
# Caribbean operator equipment backdoor

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

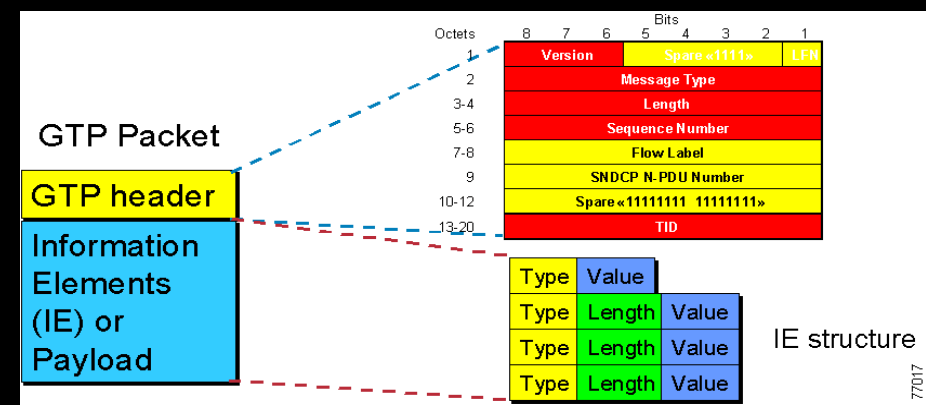
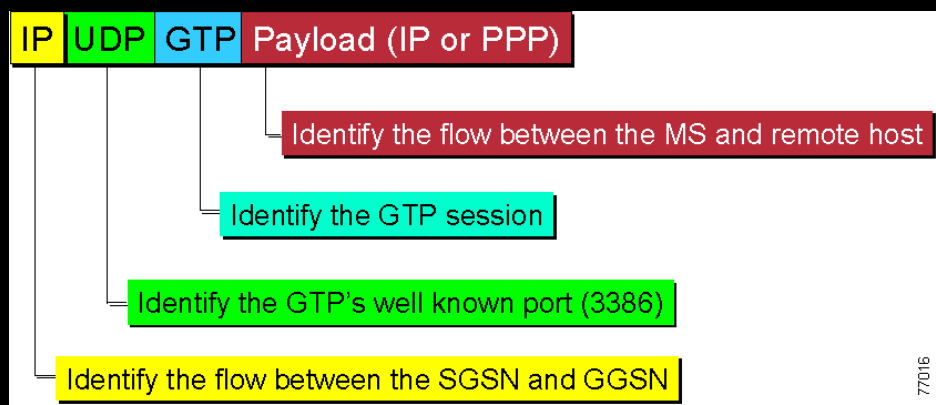
Severity	Critical
Description	NGHLR SS7 stack software is not robust and suffers from Remote Denial of Service.
Impact	Enables any person sending malicious SCCP traffic to the HLR to crash it. This includes the whole international SS7 network as HLRs need always to be globally reachable.

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

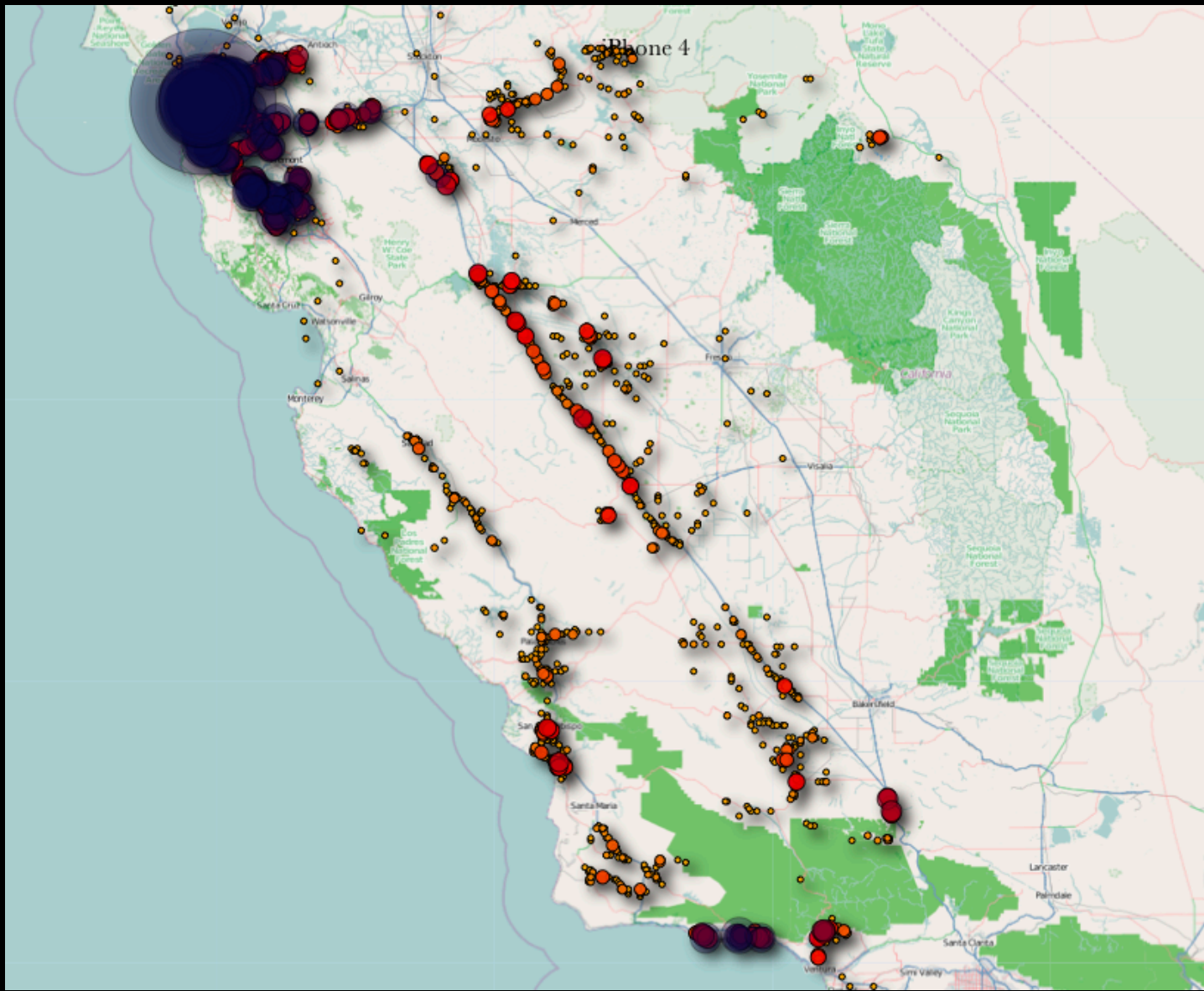


# GGSN accept GTP tunnel creation from any origin

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.



# GPRS M2M hell for Police geolocation



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

# Fake charging attacks

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

GRX	MNO
	

- 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

GRX	MNO
✓	✓

# 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.



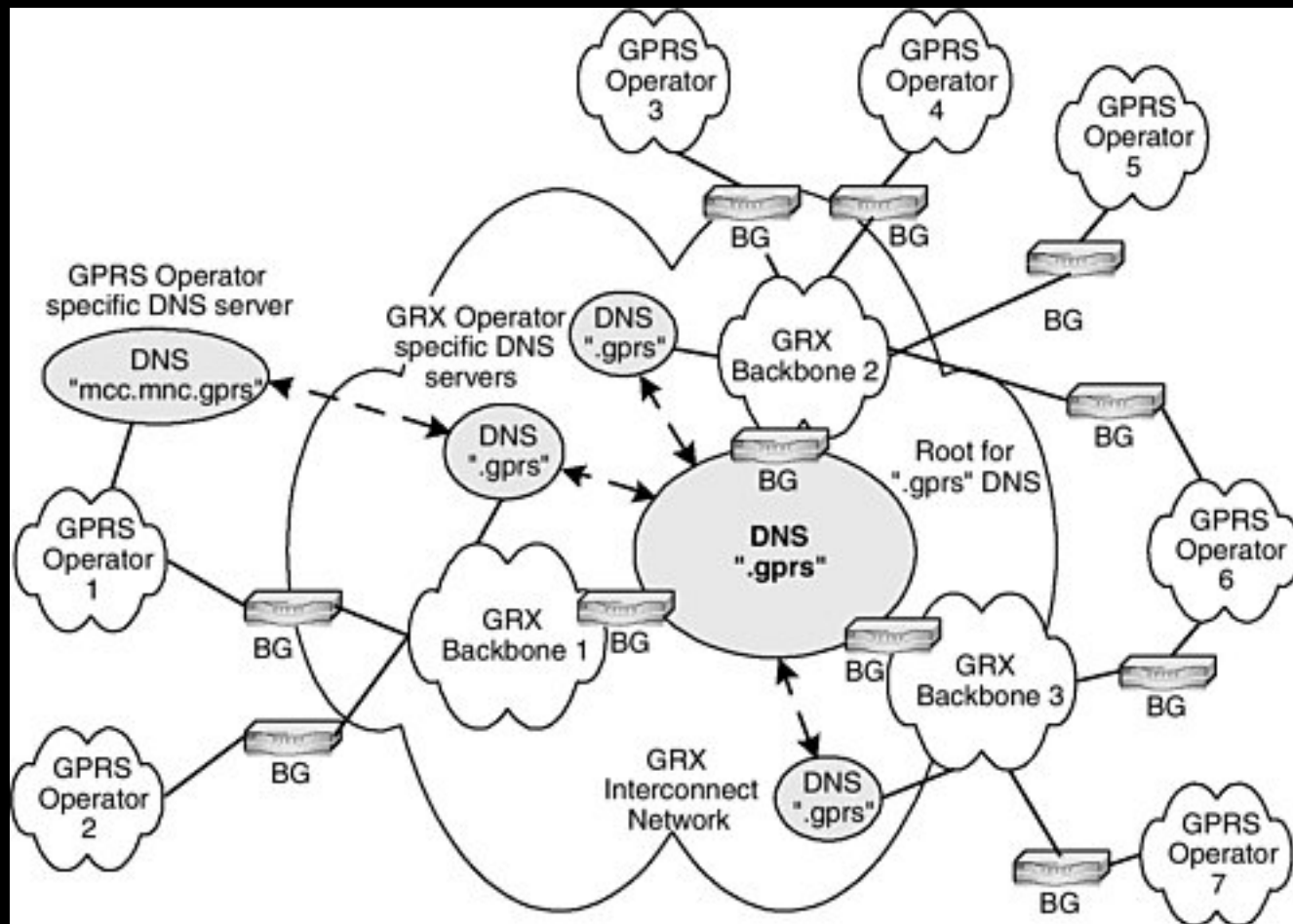
# LTE EPC leaks of DNS resolving for internal/interwork zones

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 boxes are still Solaris 2.6 in 2012... unfiltered)



# 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

# 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

# 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