Telecom Signaling attacks on 3G and LTE networks

from SS7 to all-IP, all open

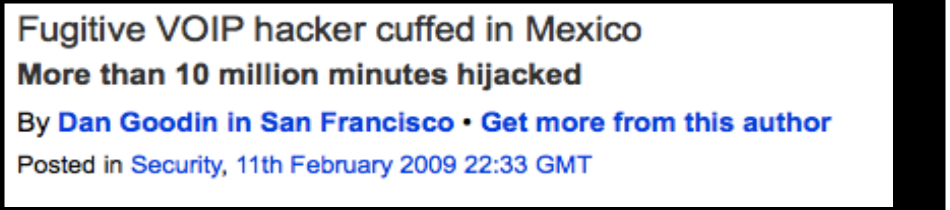
Philippe.Langlois@p1sec.com

P1 Security Inc.

v1.1

Telecom security intro

- SIP, PBX, ...
- Periphery, customer side.
- Long gone world of Blue Box.
- Sometime hear about “Roaming frauds”.
- Rarely hear the Core Network horror stories.

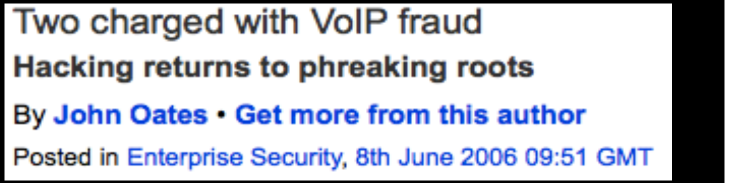


Fugitive VOIP hacker cuffed in Mexico

More than 10 million minutes hijacked

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Security, 11th February 2009 22:33 GMT

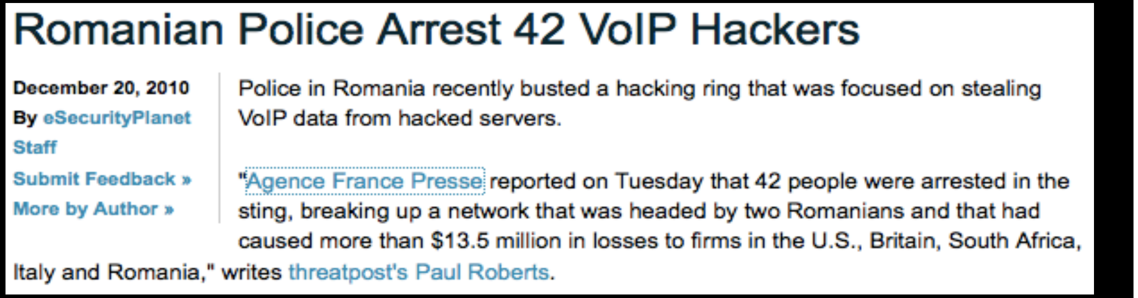


Two charged with VoIP fraud

Hacking returns to phreaking roots

By **John Oates** • **Get more from this author**

Posted in Enterprise Security, 8th June 2006 09:51 GMT



Romanian Police Arrest 42 VoIP Hackers

December 20, 2010
By eSecurityPlanet Staff

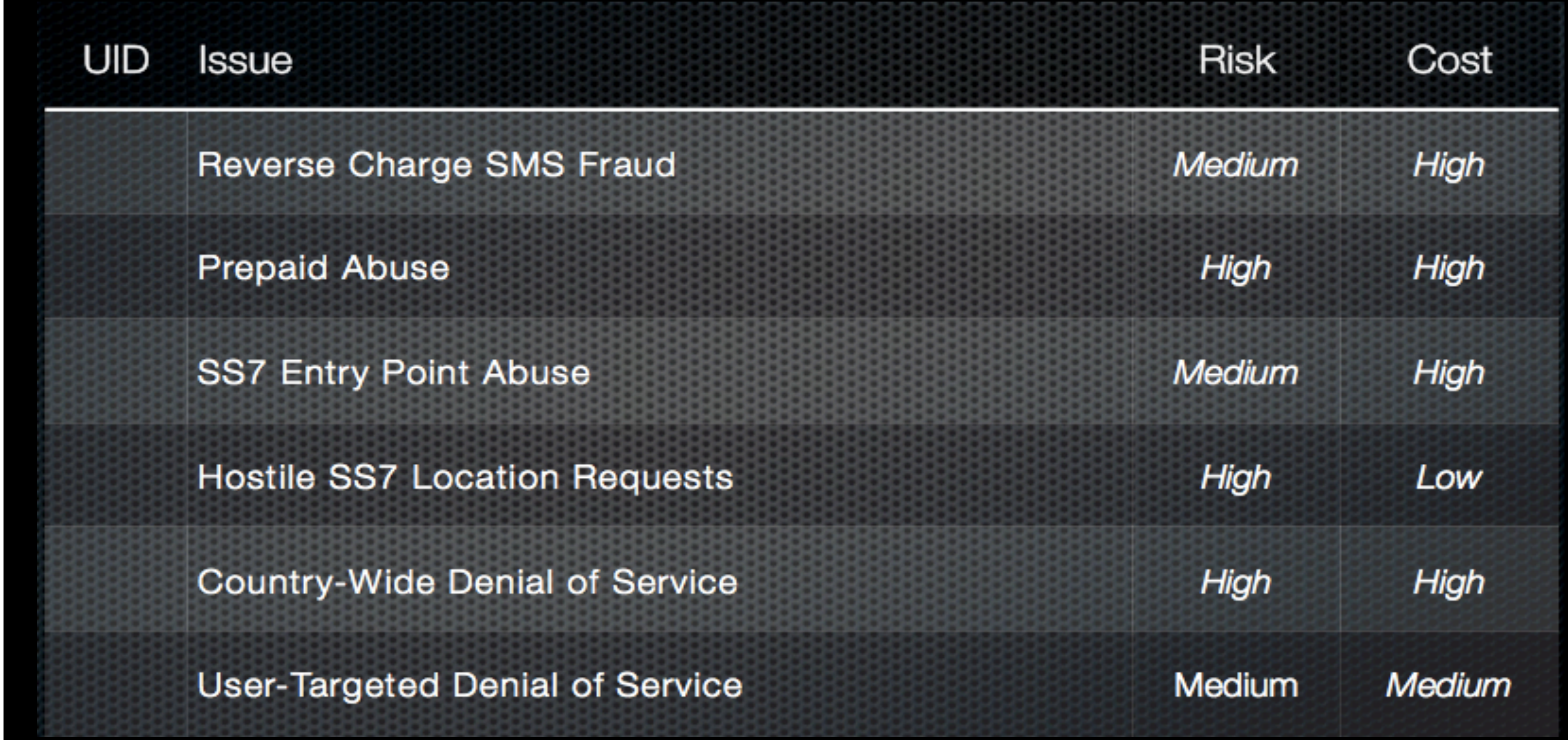
Submit Feedback »
More by Author »

Police in Romania recently busted a hacking ring that was focused on stealing VoIP data from hacked servers.

"Agence France Presse reported on Tuesday that 42 people were arrested in the sting, breaking up a network that was headed by two Romanians and that had caused more than $13.5 million in losses to firms in the U.S., Britain, South Africa, Italy and Romania," writes threatpost's Paul Roberts.

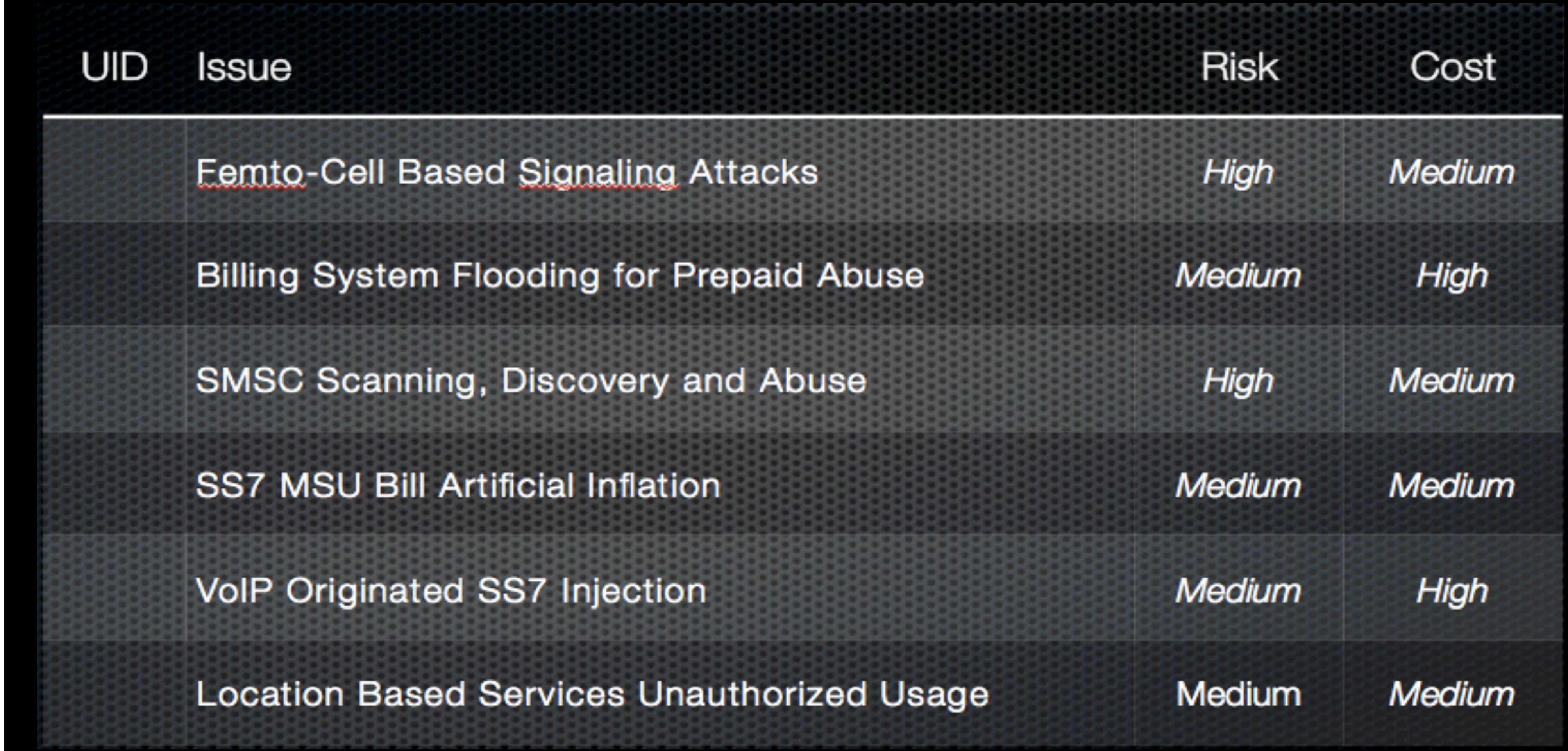
Steve Jobs and Steve Wozniak in 1975 with a bluebox

Telecom frauds and attacks



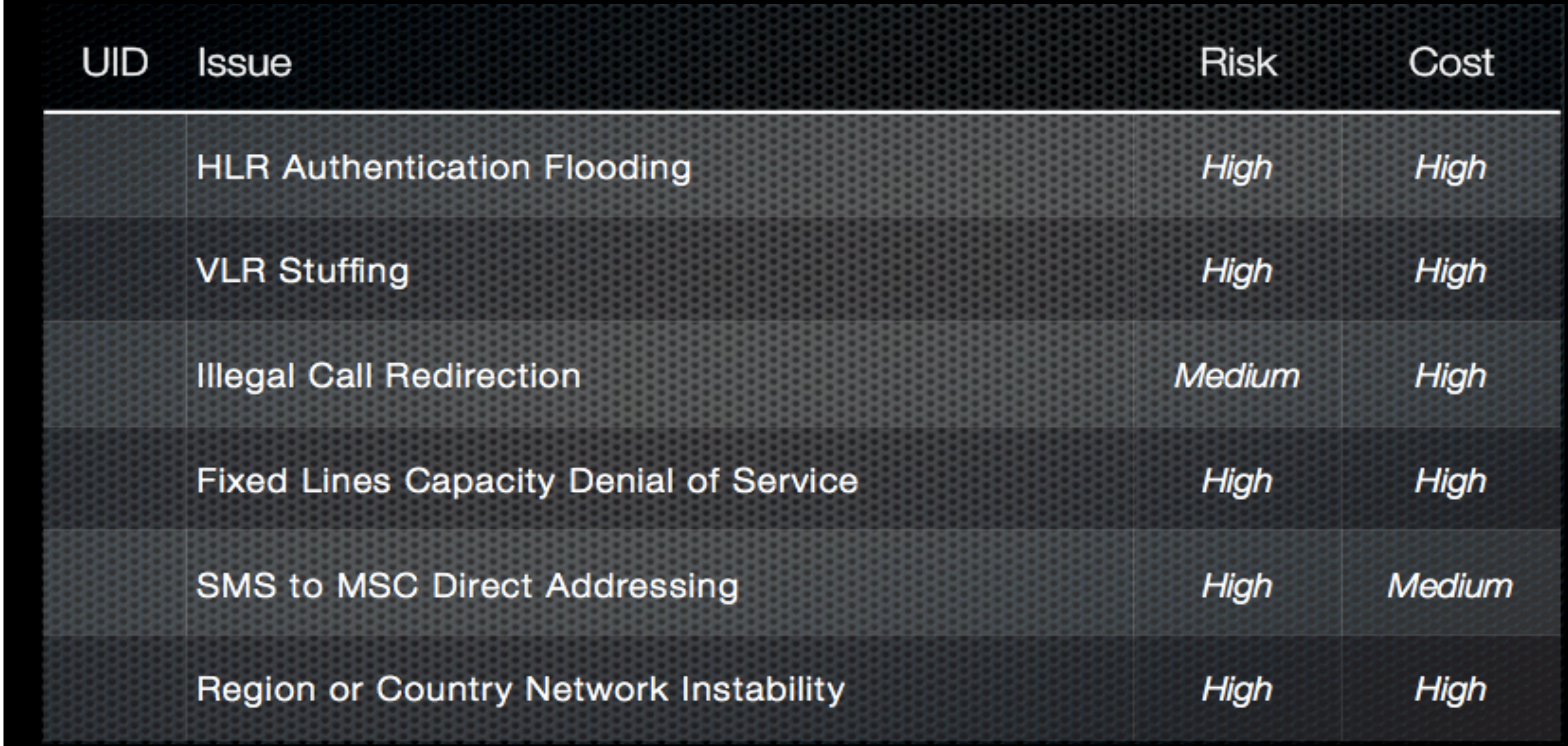
UID	Issue	Risk	Cost
	Reverse Charge SMS Fraud	*Medium*	*High*
	Prepaid Abuse	*High*	*High*
	SS7 Entry Point Abuse	*Medium*	*High*
	Hostile SS7 Location Requests	*High*	*Low*
	Country-Wide Denial of Service	*High*	*High*
	User-Targeted Denial of Service	Medium	*Medium*

Telecom frauds and attacks



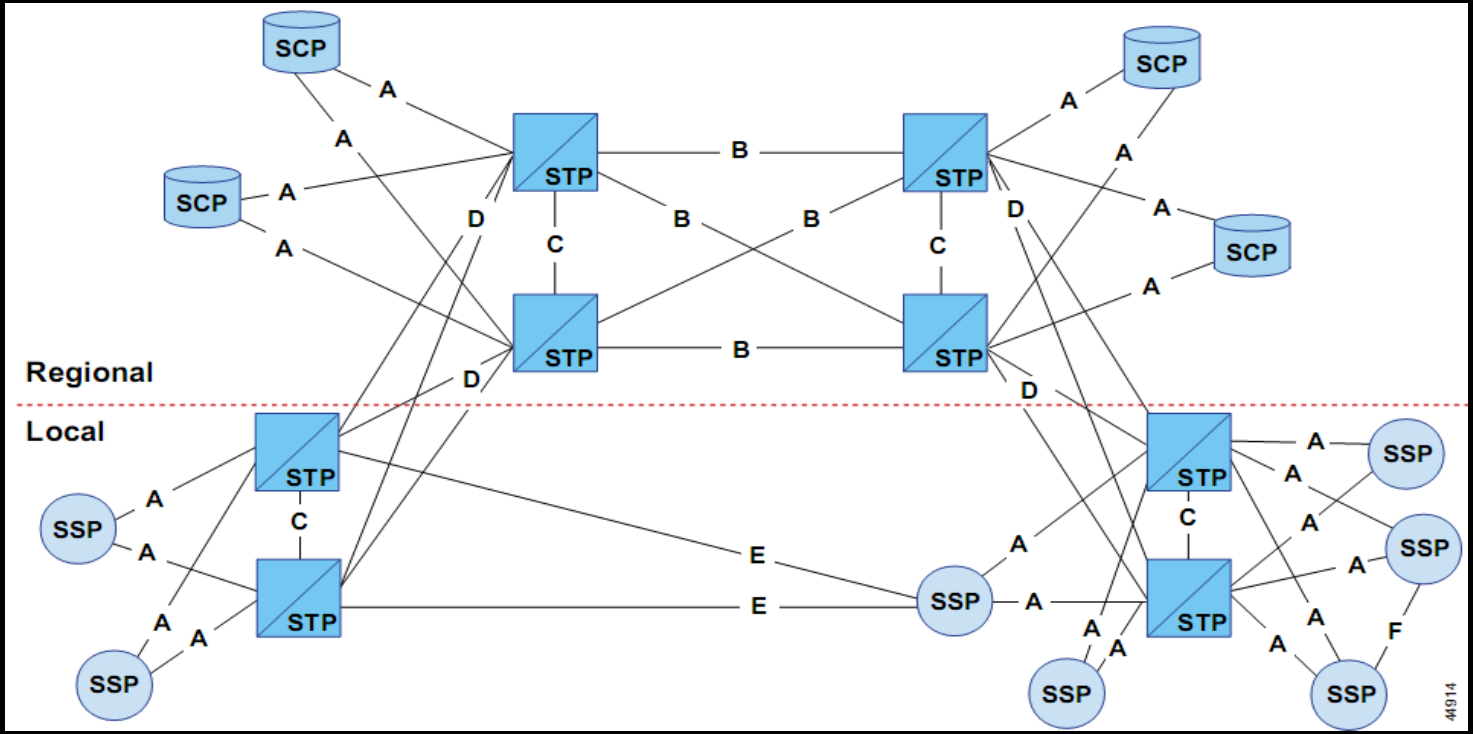
UID	Issue	Risk	Cost
	Femto-Cell Based Signaling Attacks	*High*	*Medium*
	Billing System Flooding for Prepaid Abuse	*Medium*	*High*
	SMSC Scanning, Discovery and Abuse	*High*	*Medium*
	SS7 MSU Bill Artificial Inflation	*Medium*	*Medium*
	VoIP Originated SS7 Injection	*Medium*	*High*
	Location Based Services Unauthorized Usage	Medium	*Medium*

Telecom frauds and attacks



UID	Issue	Risk	Cost
	HLR Authentication Flooding	*High*	*High*
	VLR Stuffing	*High*	*High*
	Illegal Call Redirection	*Medium*	*High*
	Fixed Lines Capacity Denial of Service	*High*	*High*
	SMS to MSC Direct Addressing	*High*	*Medium*
	Region or Country Network Instability	*High*	*High*

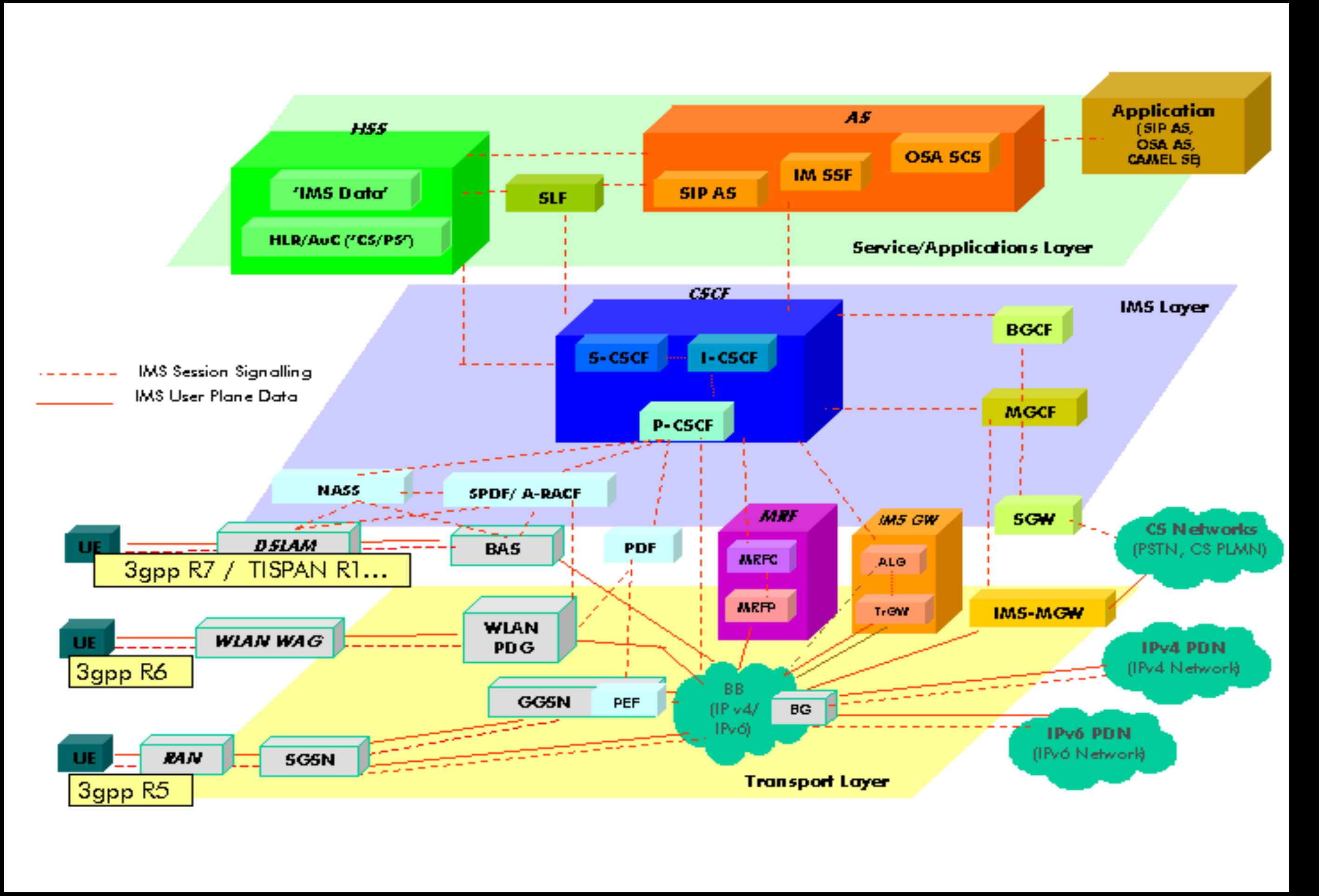
Structure of operators: SS7



- SS7 basis for international interconnection & transit
- Called “Legacy”: Why it is not going away?
- “Walled garden” approach to security.

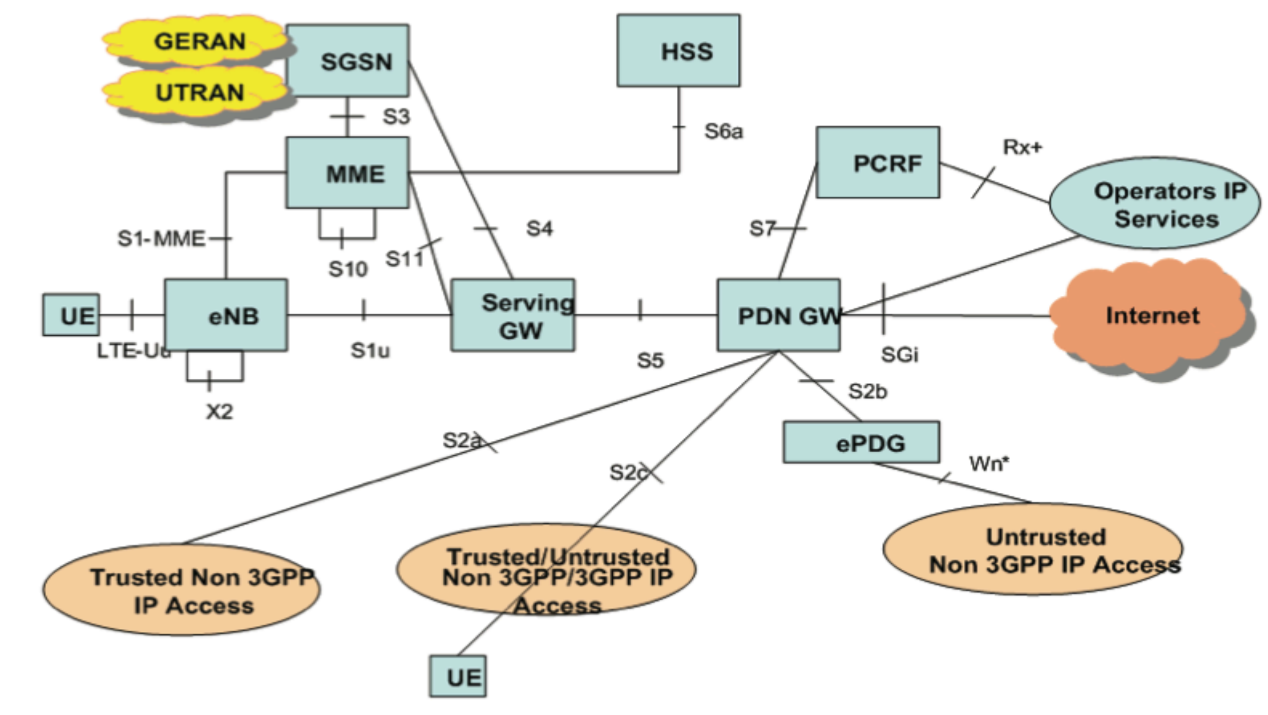
NGN, IMS, 3G

- IP friendly.
- More “IETF”
- Diameter
- Partly SIP-based
- SCTP appears
- Encapsulates SS7 over IP
- SIGTRAN



LTE, LTE Advanced

- More “P2P”
- Even more IP
- SIGTRAN is simplified
- Simpler protocols (S1)
- eNB handover & communications



- Deeper integration, less layering & segmentation
- Addresses performances issues & bottlenecks

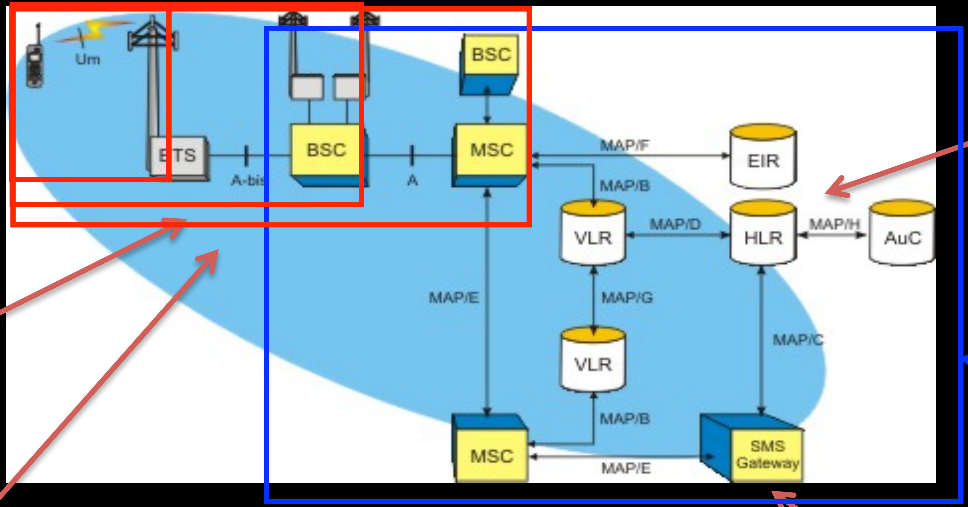
Current state of security research

ME vulnerability research (SMS o Death, OsmocomBB)

OpenBTS + crypto cracking (Karsten Nohl, …), Baseband vulns (R.P. Weinman)

OpenBSC

FemtoCell hacking (THC, P1 Security, SEC-T, …)



External APIs to HLR: location, IMSI. (Tobias Engel, …)

Scanning and Attacking SS7 CN, SIGTRAN, IMS vulnerabilities, LTE scanning, …
(Philippe Langlois,
P1 Security, Enno Rey)

SMS injection (TSTF, …)

Nothing really new in IP domain?
WRONG:
Many things come from Telecom and IP merger & legacy obscurity.

Attacking Telecom Networks

- Newbie question “How do you get access?”
- Steps
  1. Footprint
  2. Scan
  3. Exploit
  4. Detect & Protect
- No “recipe” as in IP world, each telecom environment is quite different (legacy sandwich)

1. Footprint (demo)

Demo

2. Scan: PS entry points

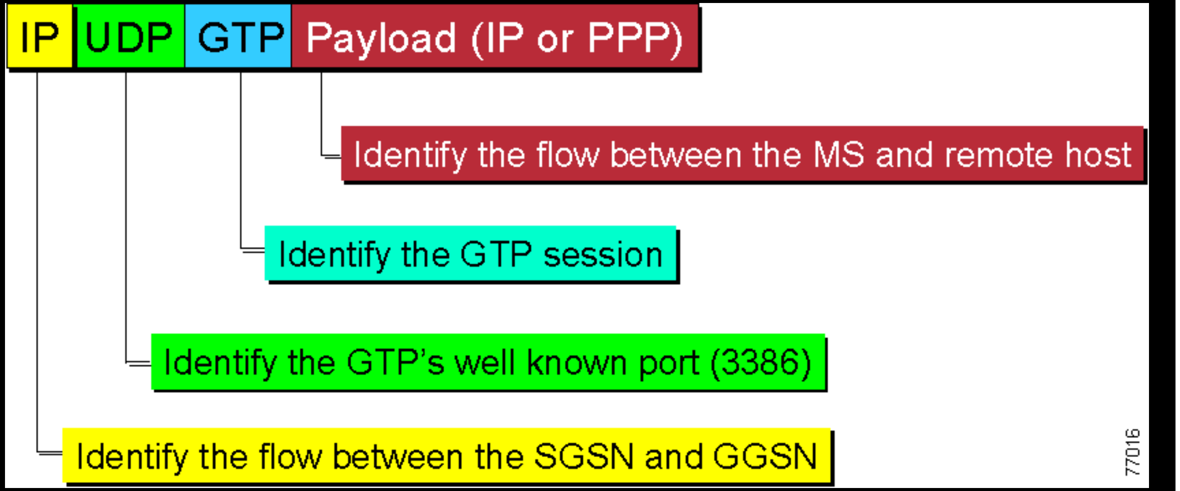
- PS Domain is huge now
- Many common mistakes:
  - IP overlaps,
  - APN misconfiguration,
  - firewall issues,
  - IPv6 control
  - M2M specifics.

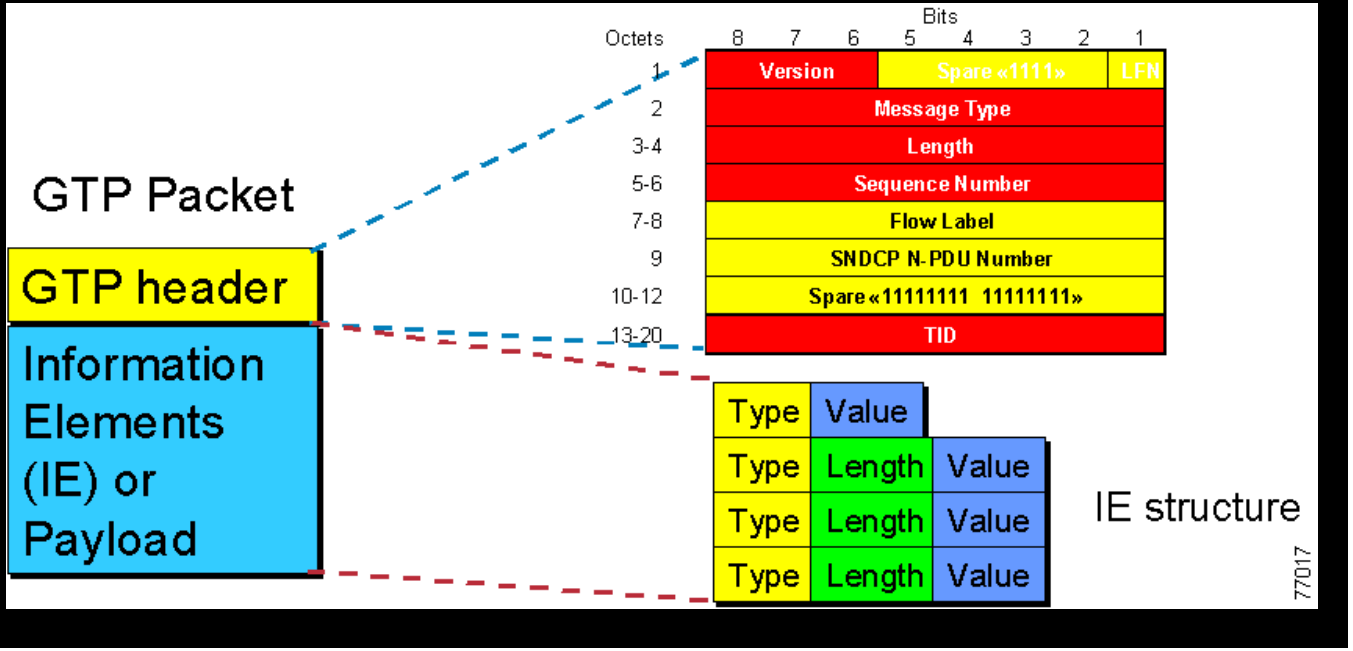
GTP entry points

- GTP’, GTP-C, GTP-U, v1 or v2
- UDP or SCTP based
- Many APNs (from 100-200 to 5000), many configurations, many networks with their corresponding GGSN.
- packet “slips” in M2M or public APNs
- GTP tunnel manipulation means traffic insertion at various point of the network (Core or Internet)

First, GTP basics

- From SGSN (client)
- To GGSN (server)
- Many “commands” possible in Message Type
- Extended a lot
  - GTP v0
  - GTP v1
  - GTP v2


IP
UDP
GTP
Payload (IP or PPP)
Identify the flow between the MS and remote host
Identify the GTP session
Identify the GTP’s well known port (3386)
Identify the flow between the SGSN and GGSN
77016



Octets	Bits 8	7	6	5	4	3	2	1
1	Version				Spare «1111»			LFN
2	Message Type							
3-4	Length							
5-6	Sequence Number							
7-8	Flow Label							
9	SNDCP N-PDU Number							
10-12	Spare «11111111 11111111»							
13-20	TID							

Type	Value	
Type	Length	Value
Type	Length	Value
Type	Length	Value

GTP scanning in 3G/LTE

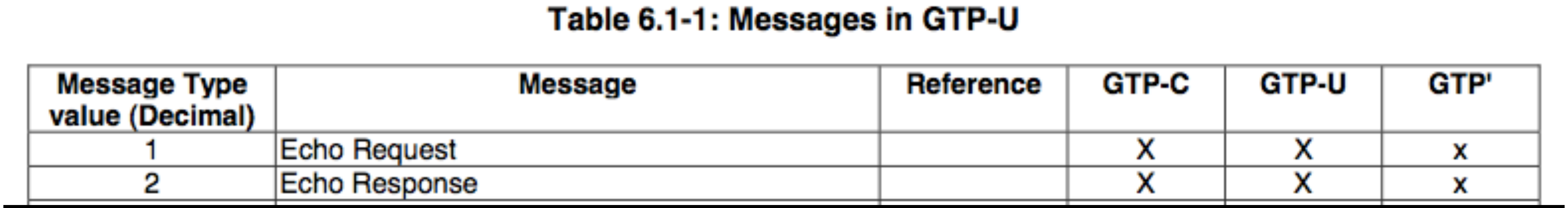


Table 6.1-1: Messages in GTP-U

Message Type value (Decimal)	Message	Reference	GTP-C	GTP-U	GTP'
1	Echo Request		X	X	x
2	Echo Response		X	X	x

- Way too many open GTP service on the Internet
- Higher ratio on LTE/GRX of course
- Easily scanned with GTP Echo Request
- UDP ports 2123, 2152, 3386, Super fast positive scanning
- LTE new protocols (from eNodeB S1/X2 to MME/PGW/…)

GRX	LTE
✓	✓

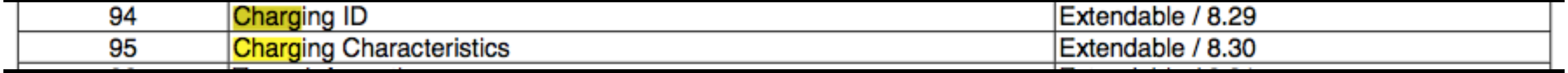
GTP Tunnel disconnection DoS attack

GRX	MNO
✓	✓

- TEID bruteforce
- Disconnect Message Type (Delete Session Request. Delete PDP, …) + spoof SGSN (really?)
- 2^32 would be a problem… if TEID were not sequential :-)

```
[...]
00 00 17 04    Delete PDP Context: Request Accepted
00 00 17 44    Delete PDP Context: Request Accepted
00 00 17 A1    Delete PDP Context: Request Accepted
00 00 17 BF    Delete PDP Context: Request Accepted
00 00 17 D8    Delete PDP Context: Request Accepted
00 00 17 E8    Delete PDP Context: Request Accepted
[...]
```

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 :-)

GRX	MNO
✓	✓

GRX Subscriber Information Leak

GRX	LTE
✓	✓

- GRX is GPRS/3G/LTE paradise (soon IPX)
- SGSN and GGSN need to communicate with many Network Elements in 3G and 4G networks
- GTP v2 enables many requests to these equipment directly over GTP.
- Think “HLR Request” over UDP
  - No authentication
  - Much more available than an SS7 interconnection :-)
- And you’re GLOBAL ! Thanks GRX. That is, any operator in the world that is connected to any GRX.

Relocation Cancel attack

- Basically tell one SGSN that the user it is serving should come back to you
- User is effectively disconnected (or hangs), no more pac

GRX	LTE
✓	✓

- Targer user by IMSI
  - But you already got that by the Info leak of previous attack

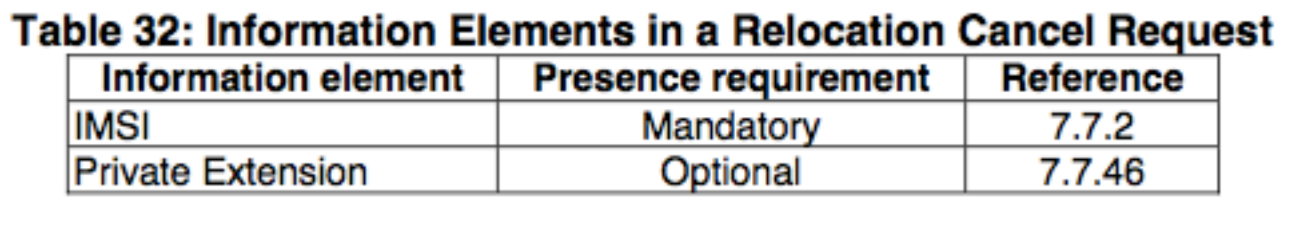


Table 32: Information Elements in a Relocation Cancel Request

Information element	Presence requirement	Reference
IMSI	Mandatory	7.7.2
Private Extension	Optional	7.7.46

  - Shoule be Intra-operator, but does work over GRX!

GGSN DoS attack

GRX	LTE
✓	✓

- 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

GRX	LTE
✓	✓

- 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.

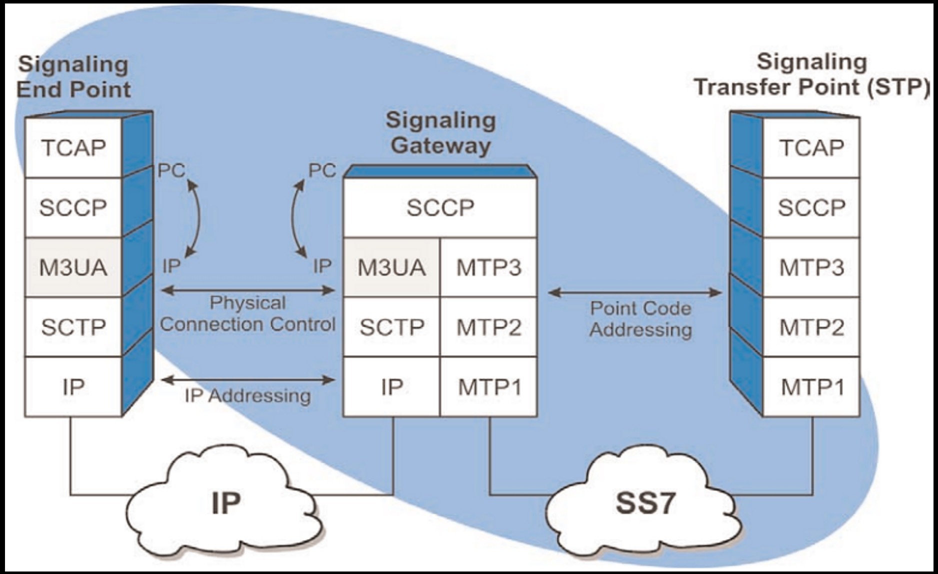
Scan Femto Cells entry points

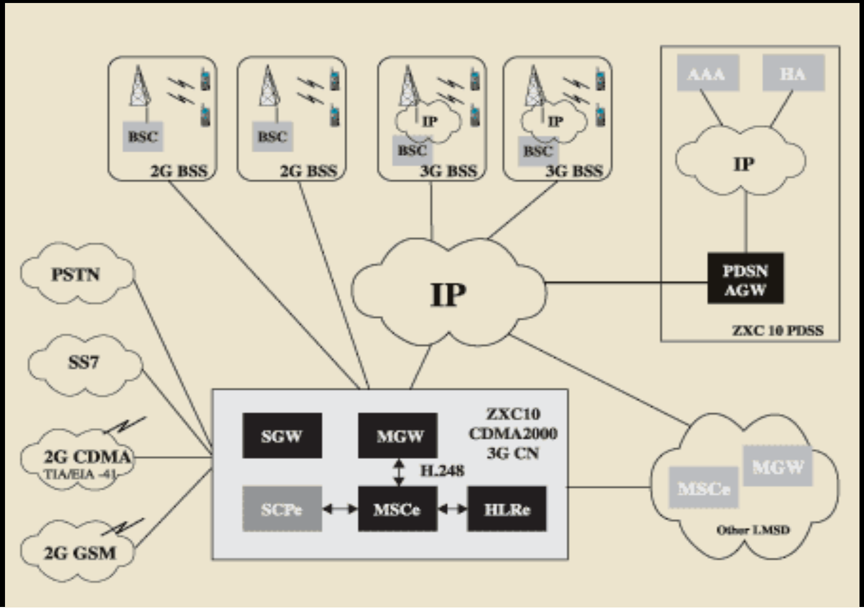
- Femto Cell security is improving
  - Better boot harden
  - IPsec tunnels
  - EAP-SIM protected

- But many compromise vectors still.
- Exposes directly signaling network (HNBAP), HLR/HSS (Diameter, ...), infrastructure network (routing, NTP, ...) to the user.

Core Network (CN) scan

- Some Core Network start of migration since 2008 to IPv6
- SCTP based (RFC4960, Stream Control Transmission Protocol)
- Still SS7 encapsulated
- Implementations make scanning easy...



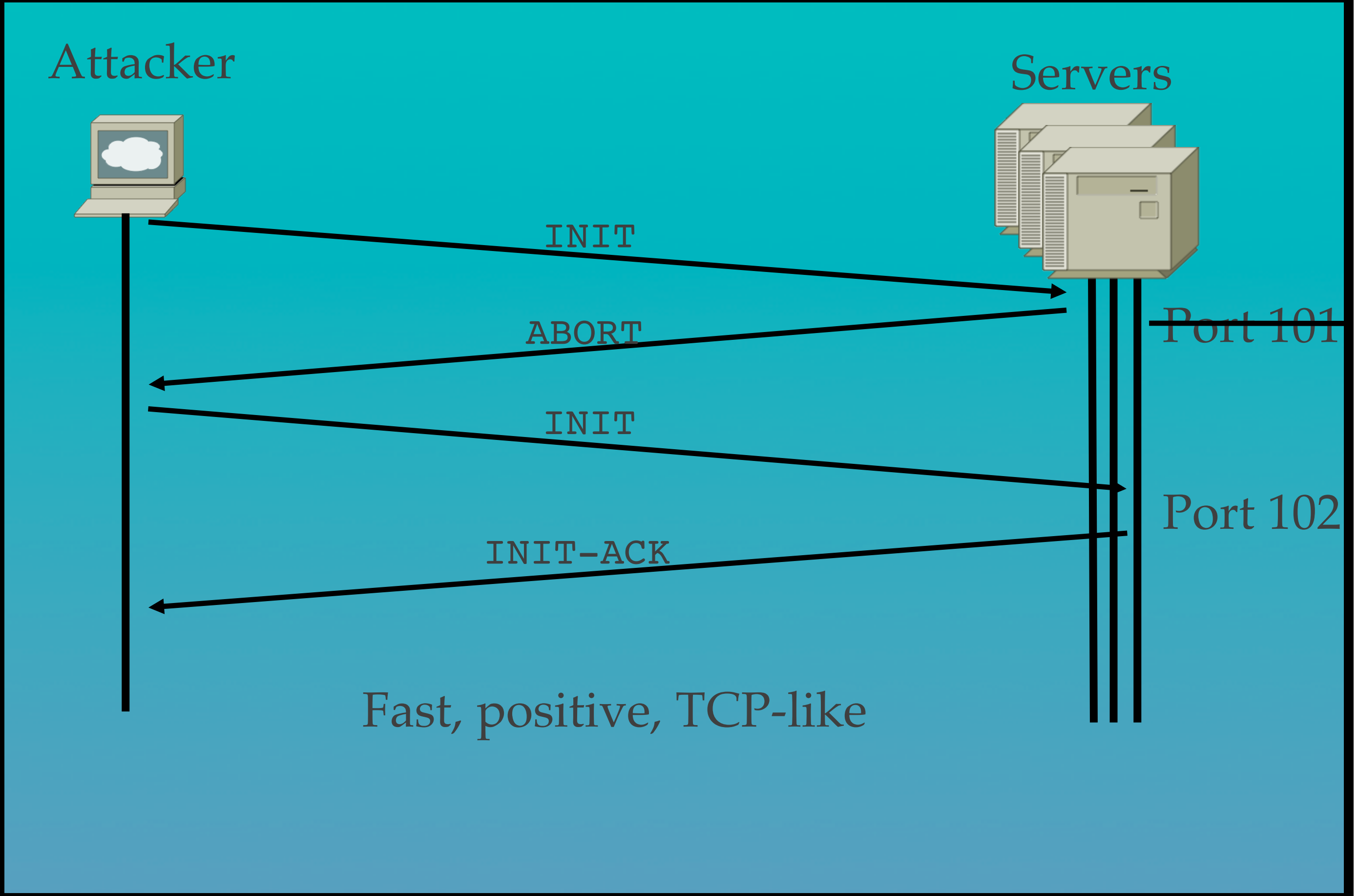


SCTP scan

- Pioneered in SCTPscan, ported into nmap.

- Both don’t work anymore (SCTP protocol evolved).

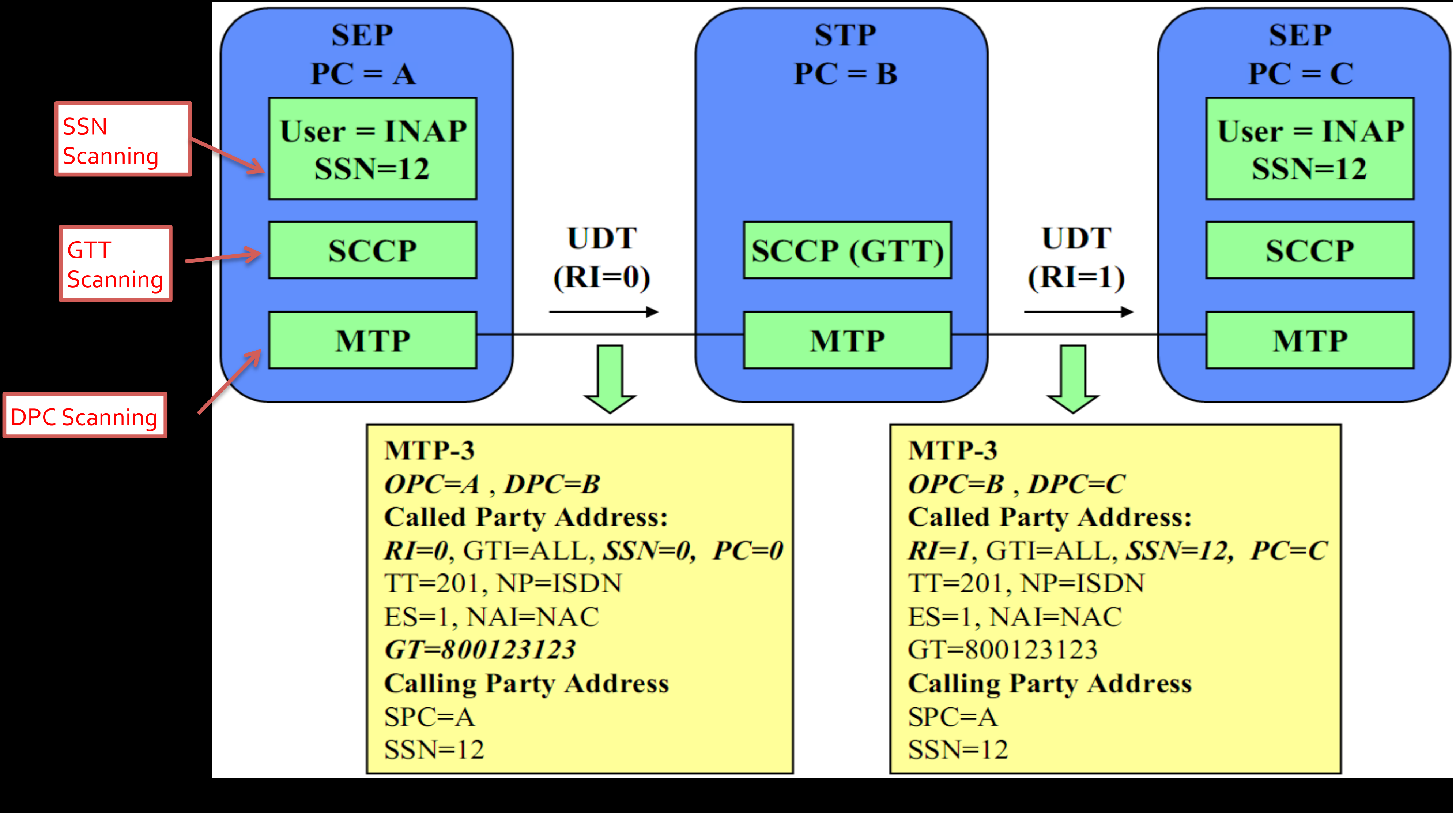
- Now in SCTPscan NG



CN Scan specificities

- SCTP changed a lot, public tools don’t work anymore. (Difficulty)
- IPv6 starts to be deployed, scan is completely possible but “regular consultants” don’t know how to. (Size)
- CN Protocols are very complex (ASN.1 madness, Difficulty) cannot be tested by hand
- Signaling protocols address ranges makes then hard to assess by hand (Size)
- Size + Difficulty increase requires automation

Scan & Address spaces



SSN Scanning

GTT Scanning

DPC Scanning

SEP
PC = A

User = INAP
SSN=12

SCCP

MTP

UDT
(RI=0)

STP
PC = B

SCCP (GTT)

MTP

UDT
(RI=1)

SEP
PC = C

User = INAP
SSN=12

SCCP

MTP

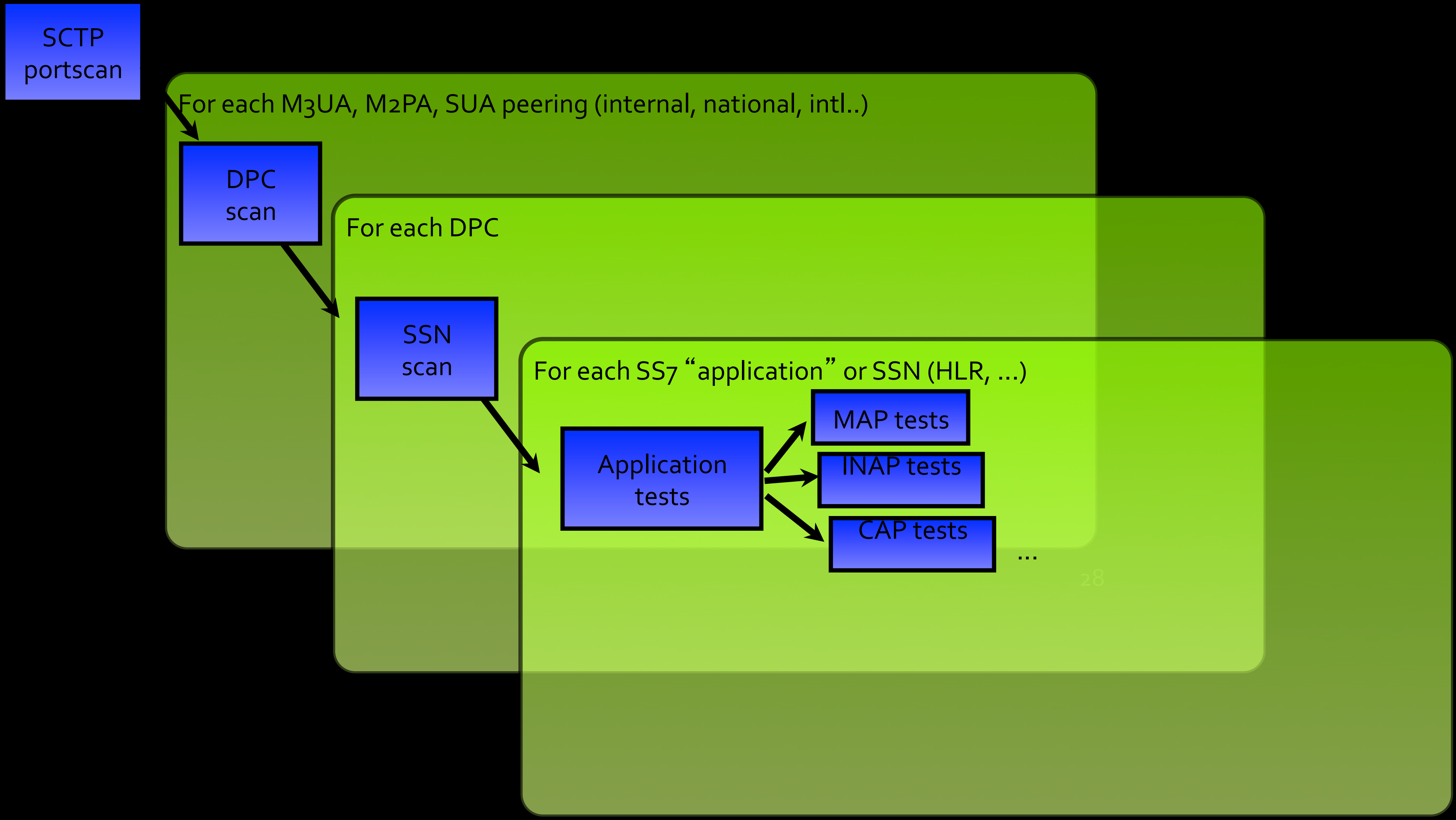
MTP-3
OPC=A* , *DPC=B
Called Party Address:
RI=0, GTI=ALL, ***SSN=0***, ***PC=0***
TT=201, NP=ISDN
ES=1, NAI=NAC
GT=800123123
Calling Party Address
SPC=A
SSN=12

MTP-3
OPC=B* , *DPC=C
Called Party Address:
RI=1, GTI=ALL, ***SSN=12***, ***PC=C***
TT=201, NP=ISDN
ES=1, NAI=NAC
GT=800123123
Calling Party Address
SPC=A
SSN=12

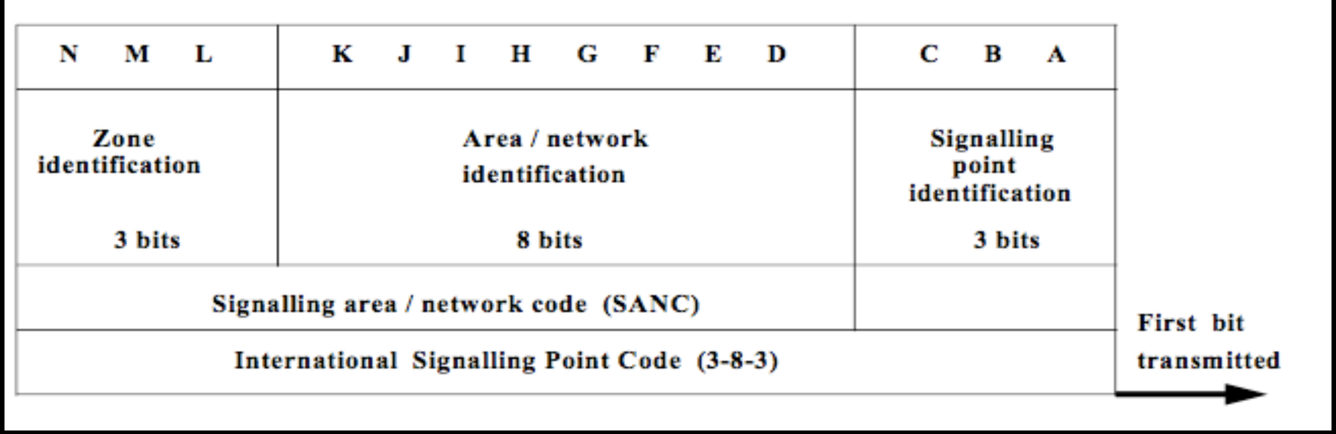
Scan IP vs. Telecom Signaling

TCP/IP	SS7
IPsec endpoint scan, MPLS label scan, VLAN tag scan	SCTP endpoint scan
Arp or Ping scan	MTP3 or M3UA scanning
Ping scan using TCP SYN	SCCP DPC scanning
TCP SYN or UDP port/service scanning	SCCP SSN (SubSystem Number) scanning
Service-specific attacks and abuses (e.g. attacks over HTTP, SMB, RPC, ...)	Application (*AP) traffic injection (e.g. MAP, INAP, CAP, OMAP...)

SIGTRAN Audit Strategies

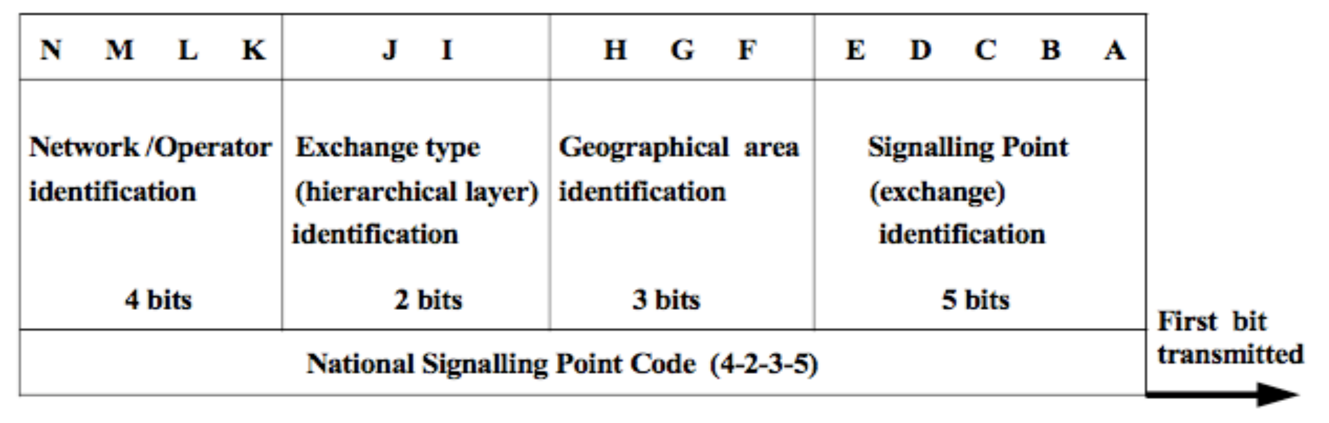

SCTP portscan
For each M3UA, M2PA, SUA peering (internal, national, intl..)
DPC scan
For each DPC
SSN scan
For each SS7 “application” or SSN (HLR, ...)
Application tests
MAP tests
INAP tests
CAP tests
...

National and International SPCs



N M L	K J I H G F E D	C B A
Zone identification 3 bits	Area / network identification 8 bits	Signalling point identification 3 bits
Signalling area / network code (SANC)		
International Signalling Point Code (3-8-3)		

First bit transmitted



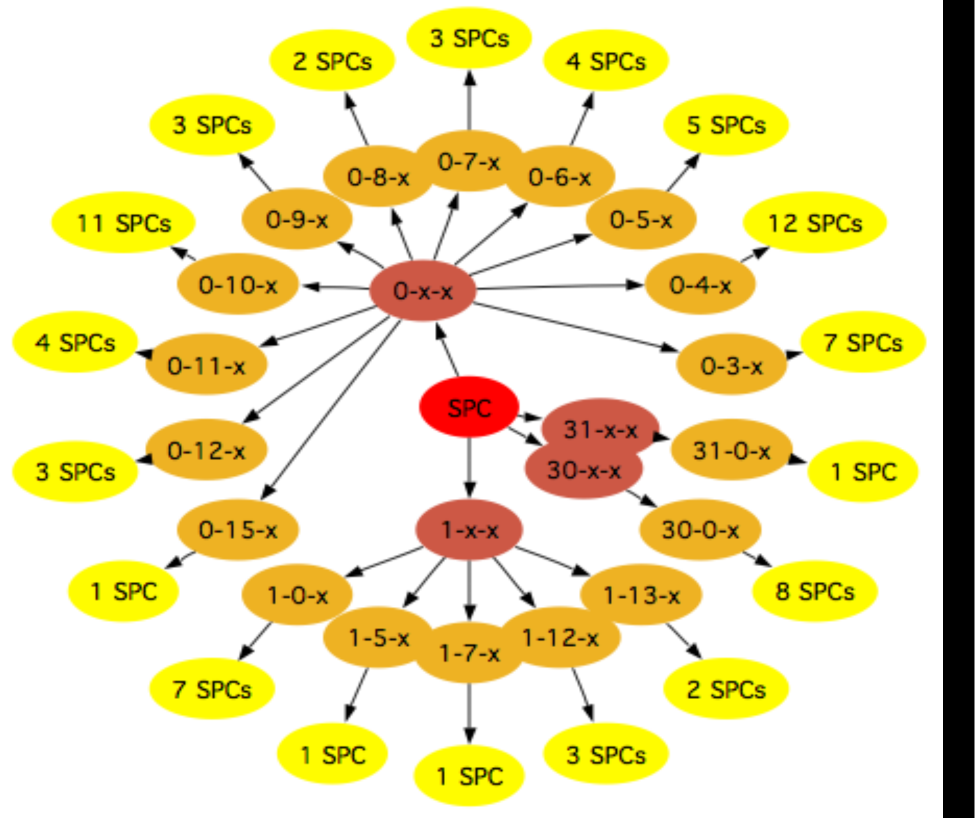
N M L K	J I	H G F	E D C B A
Network /Operator identification 4 bits	Exchange type (hierarchical layer) identification 2 bits	Geographical area identification 3 bits	Signalling Point (exchange) identification 5 bits
National Signalling Point Code (4-2-3-5)			

First bit transmitted

- SANC and ISPCs
- SANC assigned by ITU
- 4-2-3-5 SPCs

Scan to network maps

- Multiple formats for Point Code representation (3-8-3, NIPC, 5-4-5, Hex, Decimal)
- One Point Code “1-2-1” can represent many different addresses.
- Helps target “good” part of the network (SMSC, Testbed, HLR cluster or BSCs?)



SS7 Signaling Point Code map

Address type: 5-4-5

http://www.p1security.com

LTE scanning strategies

- Mix between SIGTRAN scan and IP scan
- Target protocols: S1, X2
- Inter- eNodeB communications (X2)
- Communication between eNodeBs and Core Network
- Tools: SCTP connect scan, SCTPscan NG or PTA

3. Exploit

- Standard vulnerabilities:
  - Known vulnerabilities are present, but scarce: proprietary tools, network elements, ...
  - Misconfiguration is present often: once working, people don’t touch (fix) the network.
  - Simple architecture problems: HLR without SSL on OAM, logs exposed, vulnerable VLAN setup
- And unstandard / Telecom specific vulnerabilities:

HLR heap overflow

- One single SS7 MAP packet
  - HLR crash! … consequences for operator.
  - DoS at first, then exploitable
  - Solaris (sometime old, sometime exotic architecture)
- Reverse engineering after
  - Hardcoded crypto keys!!
  - Many vulnerabilities
- Works on HSS too

ASN.1 paradise or hell

- ITU is ASN.1 addicted
- Plenty of TLV, tons of complex protocols
- Encodings:
  - Old protocols: BER, DER
  - Newer: PER, Aligned, Unaligned
- Encoding bombs, Decompression bombs
- e.g. LTE S1 protocol between eHNB and SGW, MME

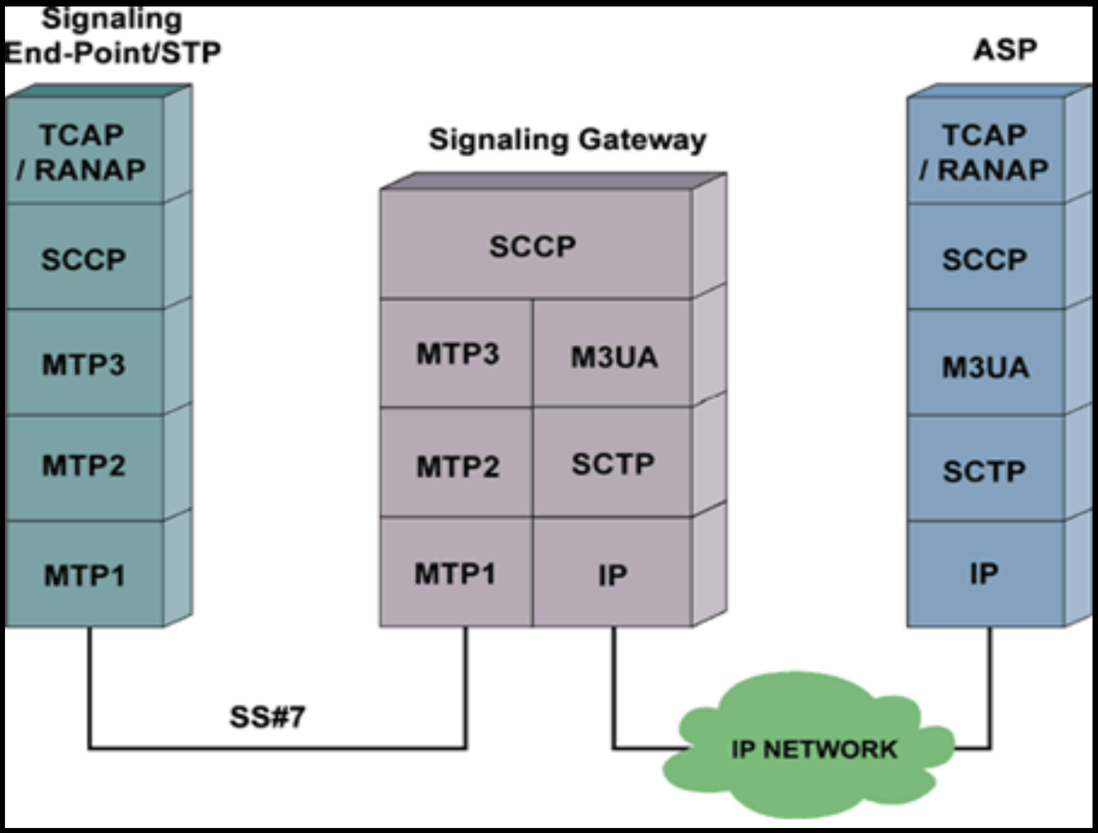
SCTP Fuzz Target

- Protocol Specification is huge
  - RFC 5062, RFC 5061, RFC 5043, RFC 4960, RFC 4895, RFC 4820, RFC 4460, RFC 3873, RFC 3758, RFC 3554, RFC 3436, RFC 3309, RFC 3286, RFC 3257, RFC 2960
- Good target for vulnerabilities
  - CVE-2010-1173 CVSS Severity: 7.1 (HIGH), CVE-2010-0008 CVSS Severity: 7.8 (HIGH), CVSS Severity: 7.8 (HIGH), CVE-2009-0065 CVSS Severity: 10.0 (HIGH), CVE-2008-4618 CVSS Severity: 7.8 (HIGH), CVE-2008-3831, CVE-2008-4576, CVE-2008-4445, CVE-2008-4113, CVE-2008-3792, CVE-2008-3526, CVE-2008-2826, CVE-2008-2089, CVE-2008-2090, CVE-2008-1070, CVE-2007-6631, CVE-2007-5726, CVE-2007-2876, CVE-2006-4535 ... CVE-2004-2013 (33 vulnerabilities)

Scapy and SCTP

- send(IP(dst="10.0.0.1")/SCTP(sport=2600,dport=2500)/SCTPChunkInit(type=1))
- send(IP(dst="10.37.129.140")/SCTP(sport=2600,dport=2500)/SCTPChunkInit(type=1)/SCTPChunkParamCookiePreservative()/SCTPChunkParamFwdTSN()/SCTPChunkParamIPv4Addr())
- send(IP(dst="10.37.129.140")/SCTP(sport=2600,dport=2500)/SCTPChunkInit(type=1)/SCTPChunkParamAdaptationLayer()/SCTPChunkParamCookiePreservative()/SCTPChunkParamFwdTSN()/SCTPChunkParamIPv4Addr()/SCTPChunkParamUnrocognizedParam()/SCTPChunkParamECNCapable()/SCTPChunkParamHearbeatInfo()/SCTPChunkParamHostname()/SCTPChunkParamStateCookie())
- It can get ugly... and i’m not even fuzzing here. Use better solution.

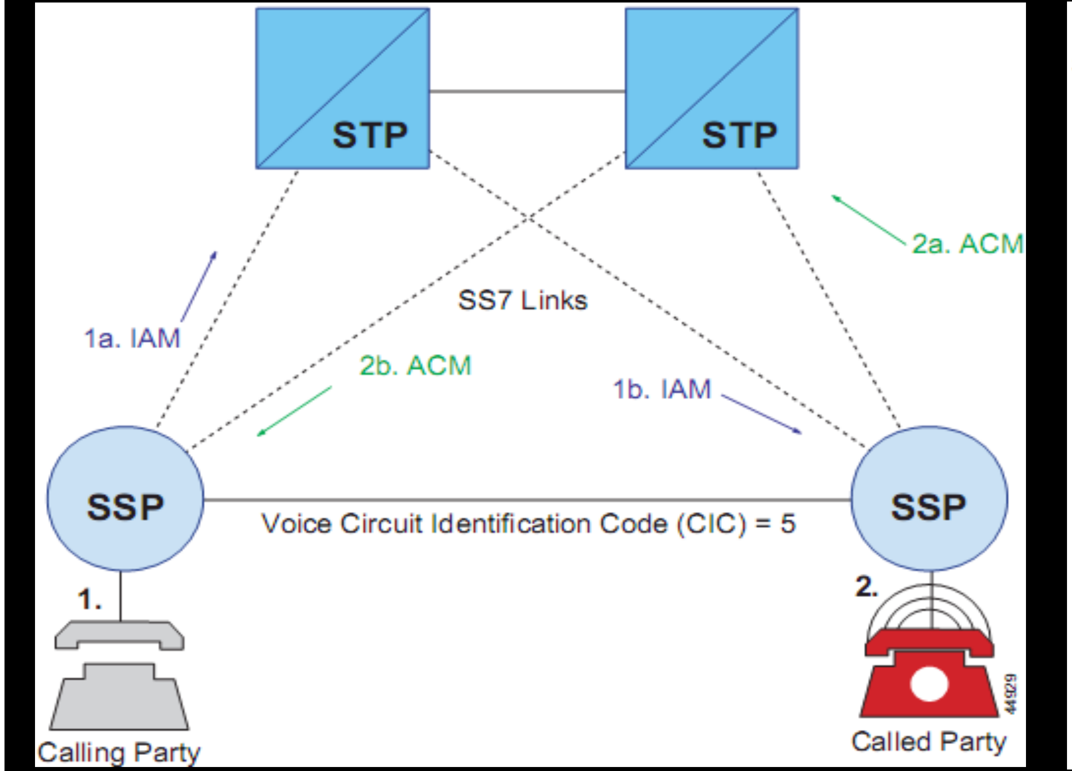
SIGTRAN Stack de-synchronization: more exposure & attacks

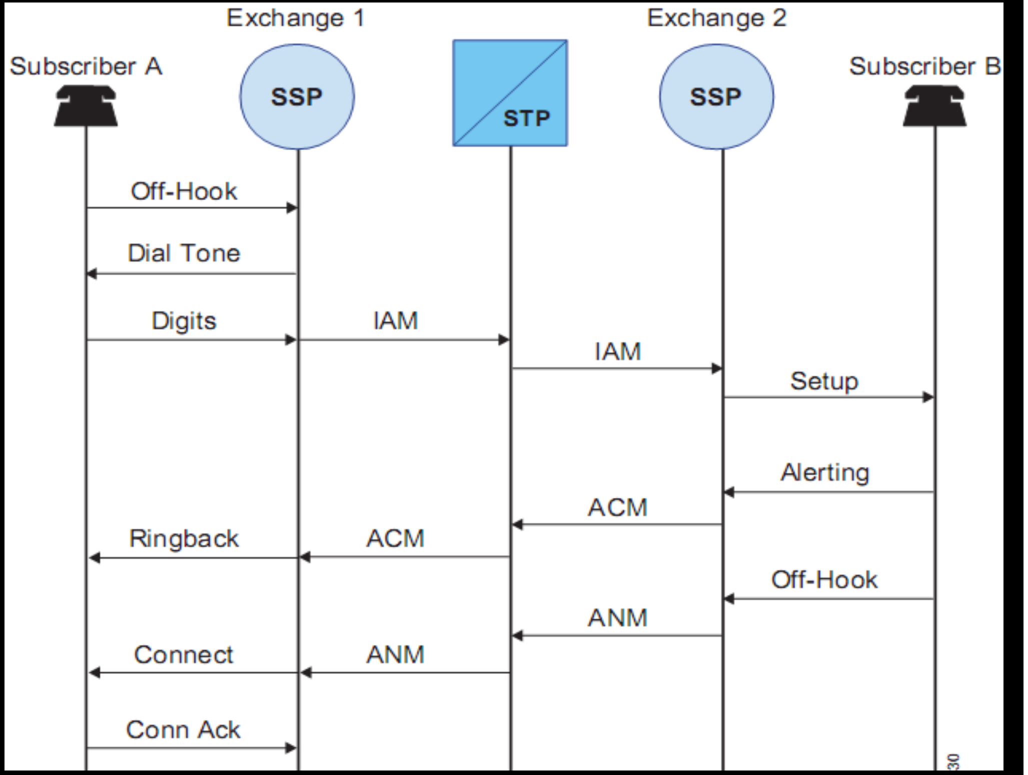


- IP/SCTP/M3UA std by IETF
- MTP3/SCCP/TCAP std by ITU
- Finite State Machine in M3UA can be tricked into believing you’re a peer.
- Once you’re signaling peer you can...

SS7 ISUP Call Initiation Flow

IAM attack: Capacity DoS

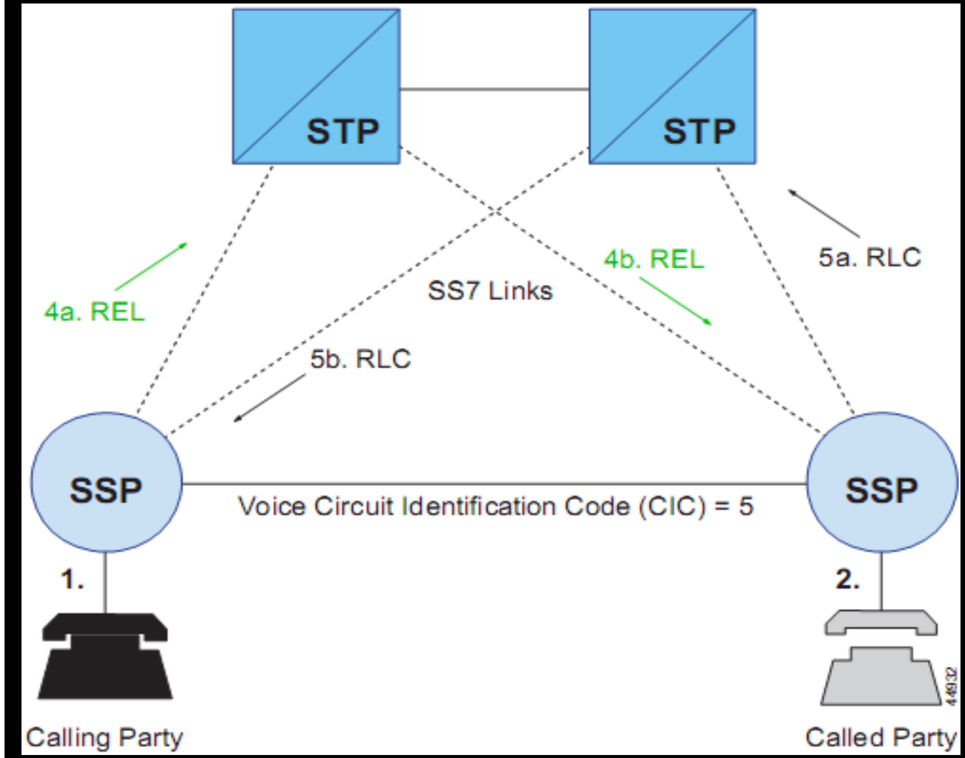




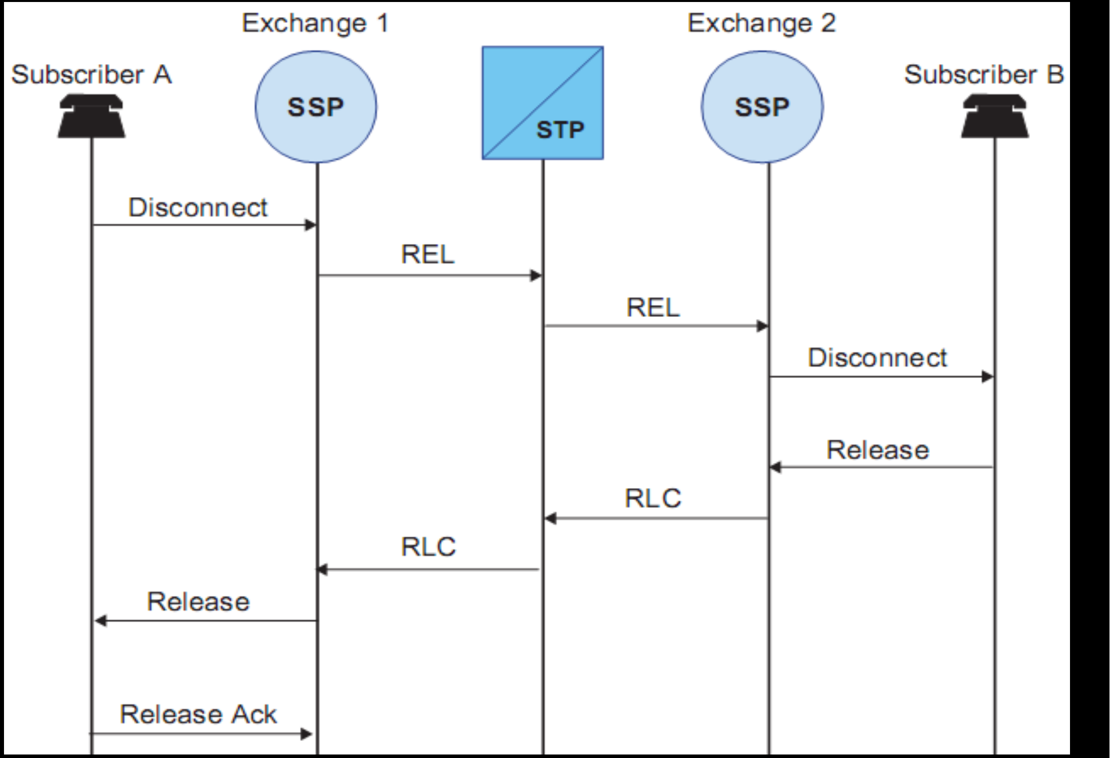
Attack Quiz!

SS7 ISUP Call Release Flow

REL attack: Selective DoS



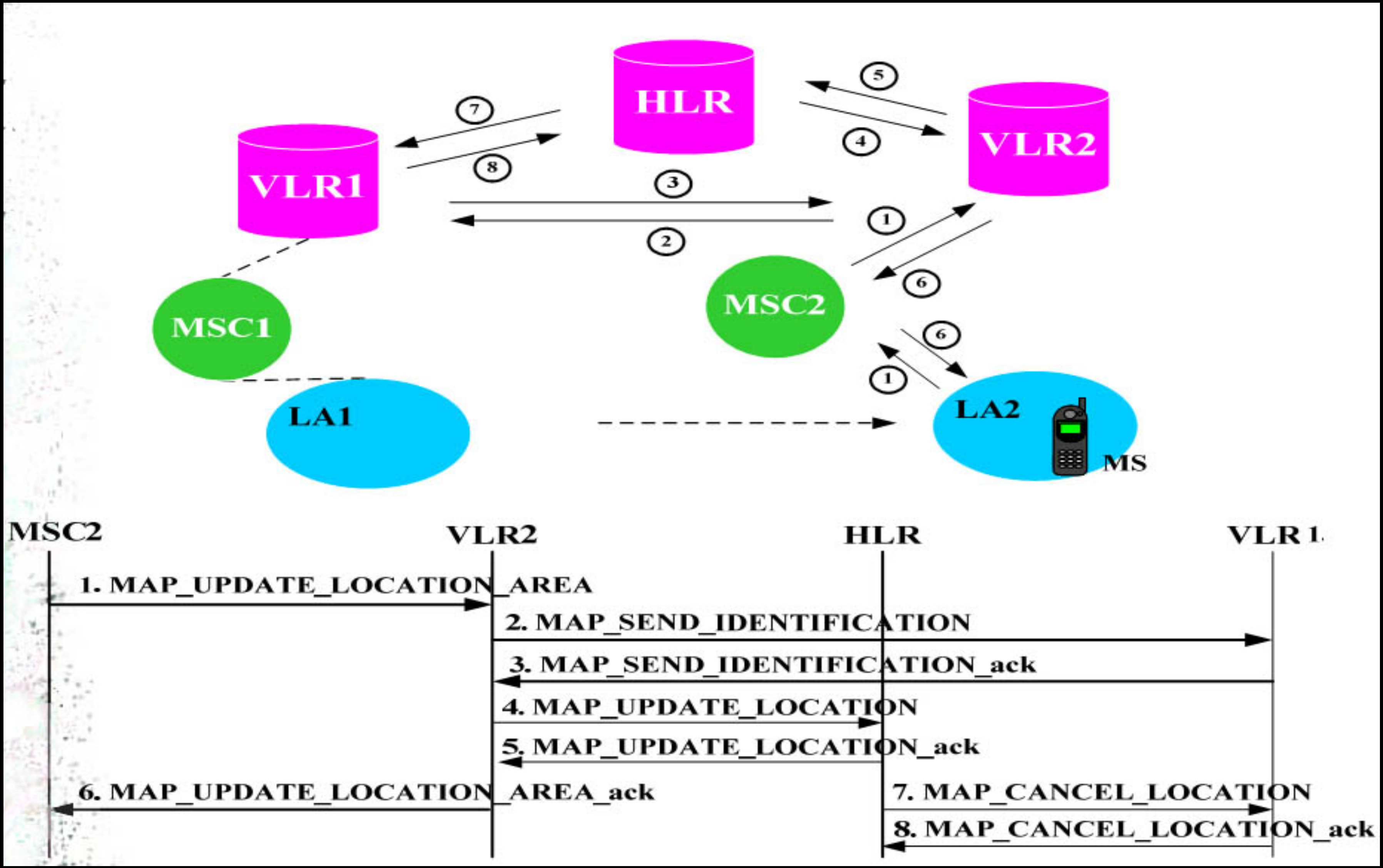
STP
STP
4a. REL
SS7 Links
4b. REL
5a. RLC
5b. RLC
SSP
SSP
Voice Circuit Identification Code (CIC) = 5
1.
2.
44932
Calling Party
Called Party



Exchange 1
Exchange 2
Subscriber A
SSP
STP
SSP
Subscriber B
Disconnect
REL
REL
Disconnect
Release
RLC
RLC
Release
Release Ack

Attack Quiz!

User targeted DoS


HLR
VLR1
VLR2
MSC1
MSC2
LA1
LA2
MS
1
2
3
4
5
6
7
8
MSC2
VLR2
HLR
VLR 1.
1. MAP_UPDATE_LOCATION_AREA
2. MAP_SEND_IDENTIFICATION
3. MAP_SEND_IDENTIFICATION_ack
4. MAP_UPDATE_LOCATION
5. MAP_UPDATE_LOCATION_ack
6. MAP_UPDATE_LOCATION_AREA_ack
7. MAP_CANCEL_LOCATION
8. MAP_CANCEL_LOCATION_ack

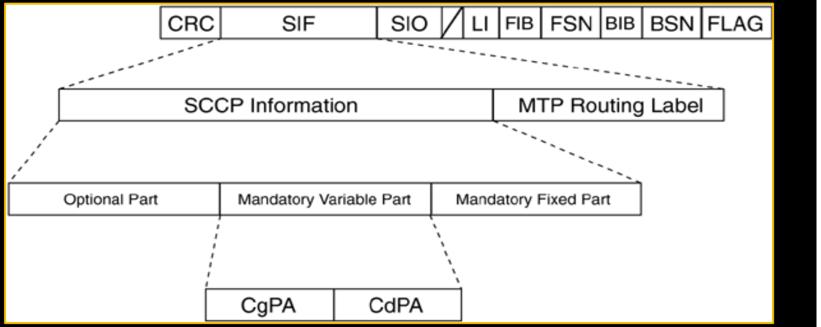
Sending hostile MSU (MAP)

- Sent from any network (in the world)

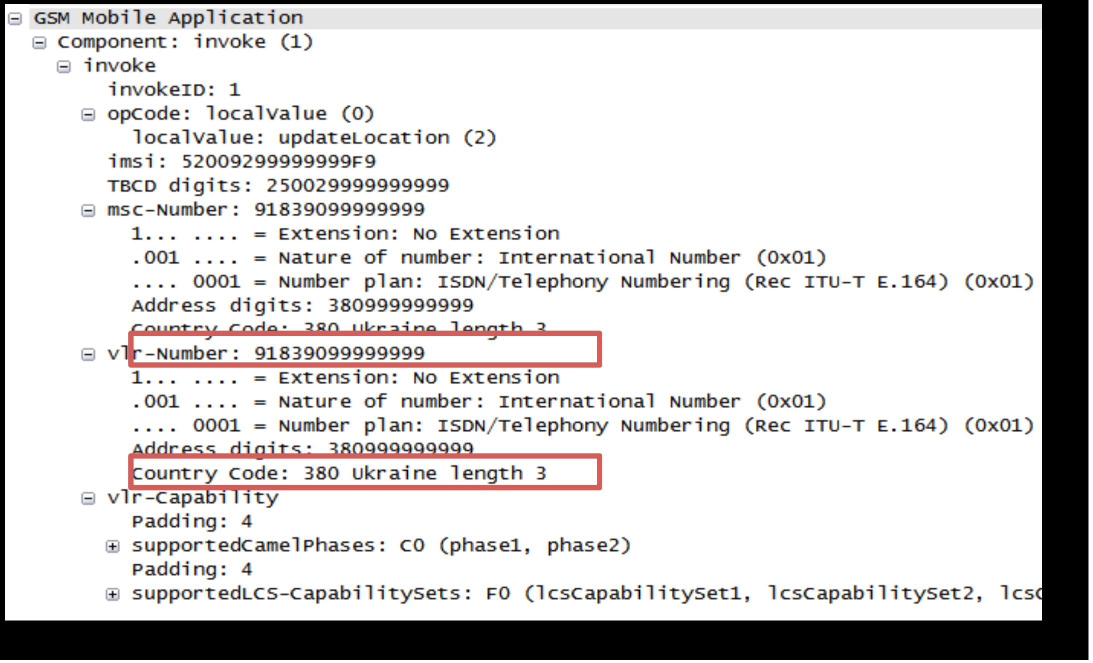
- to any target mobile phone

- HLR Lookup may be used to prepare attack (IMSI gathered through SRI_for_SM)

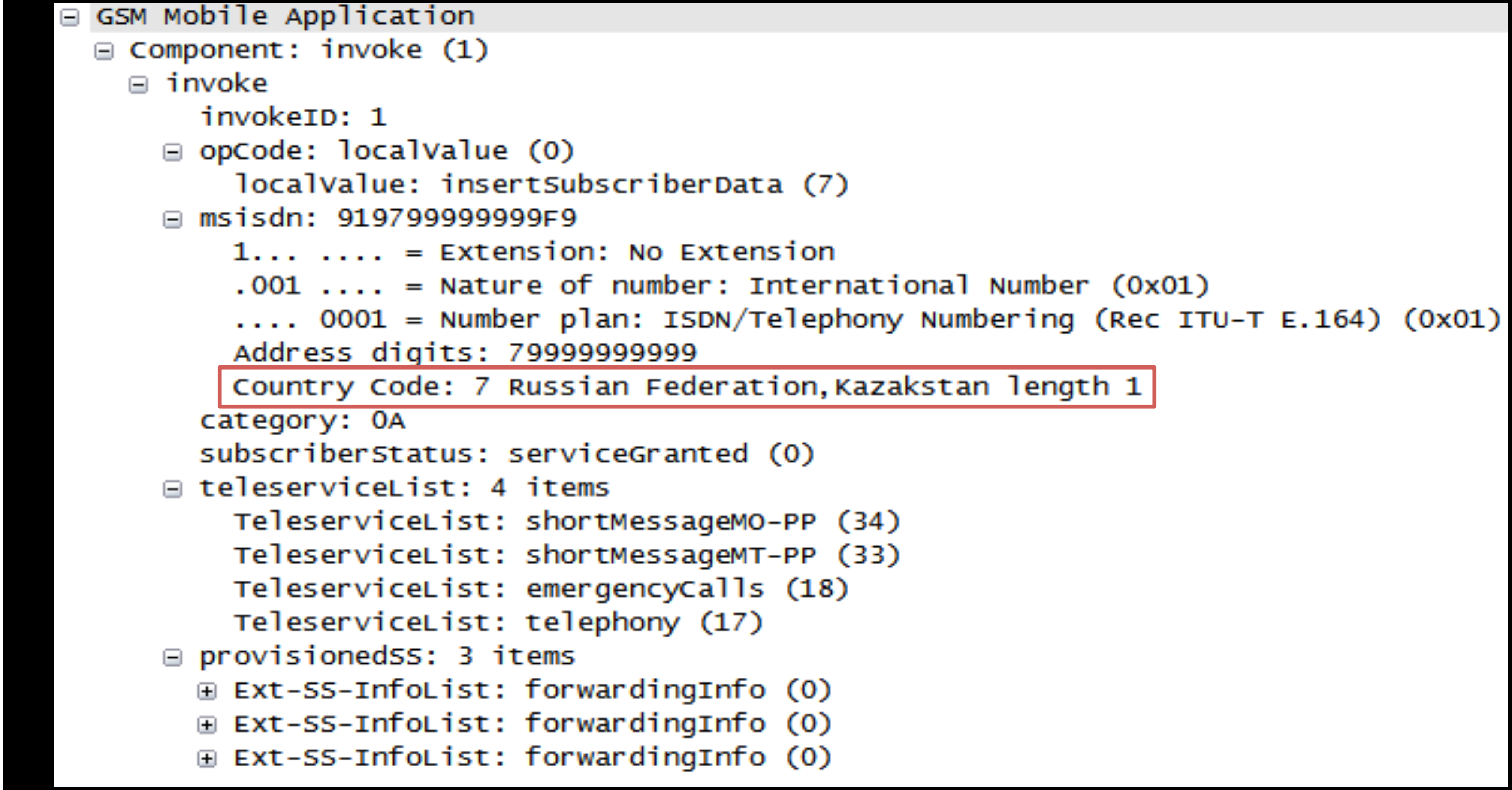
- Phone is registered on network, can make call, cannot receive calls or SMS.



IMSI scanning / querying needed !


```
⊟ GSM Mobile Application
  ⊟ Component: invoke (1)
    ⊟ invoke
        invokeID: 1
      ⊟ opCode: localValue (0)
          localValue: updateLocation (2)
        imsi: 52009299999999F9
        TBCD digits: 250029999999999
      ⊟ msc-Number: 91839099999999
          1... .... = Extension: No Extension
          .001 .... = Nature of number: International Number (0x01)
          .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
          Address digits: 380999999999
          Country Code: 380 Ukraine length 3
      ⊟ vlr-Number: 91839099999999
          1... .... = Extension: No Extension
          .001 .... = Nature of number: International Number (0x01)
          .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
          Address digits: 380999999999
          Country Code: 380 Ukraine length 3
      ⊟ vlr-Capability
          Padding: 4
        ⊞ supportedCamelPhases: C0 (phase1, phase2)
          Padding: 4
        ⊞ supportedLCS-CapabilitySets: F0 (lcsCapabilitySet1, lcsCapabilitySet2, lcsC
```

Attack success

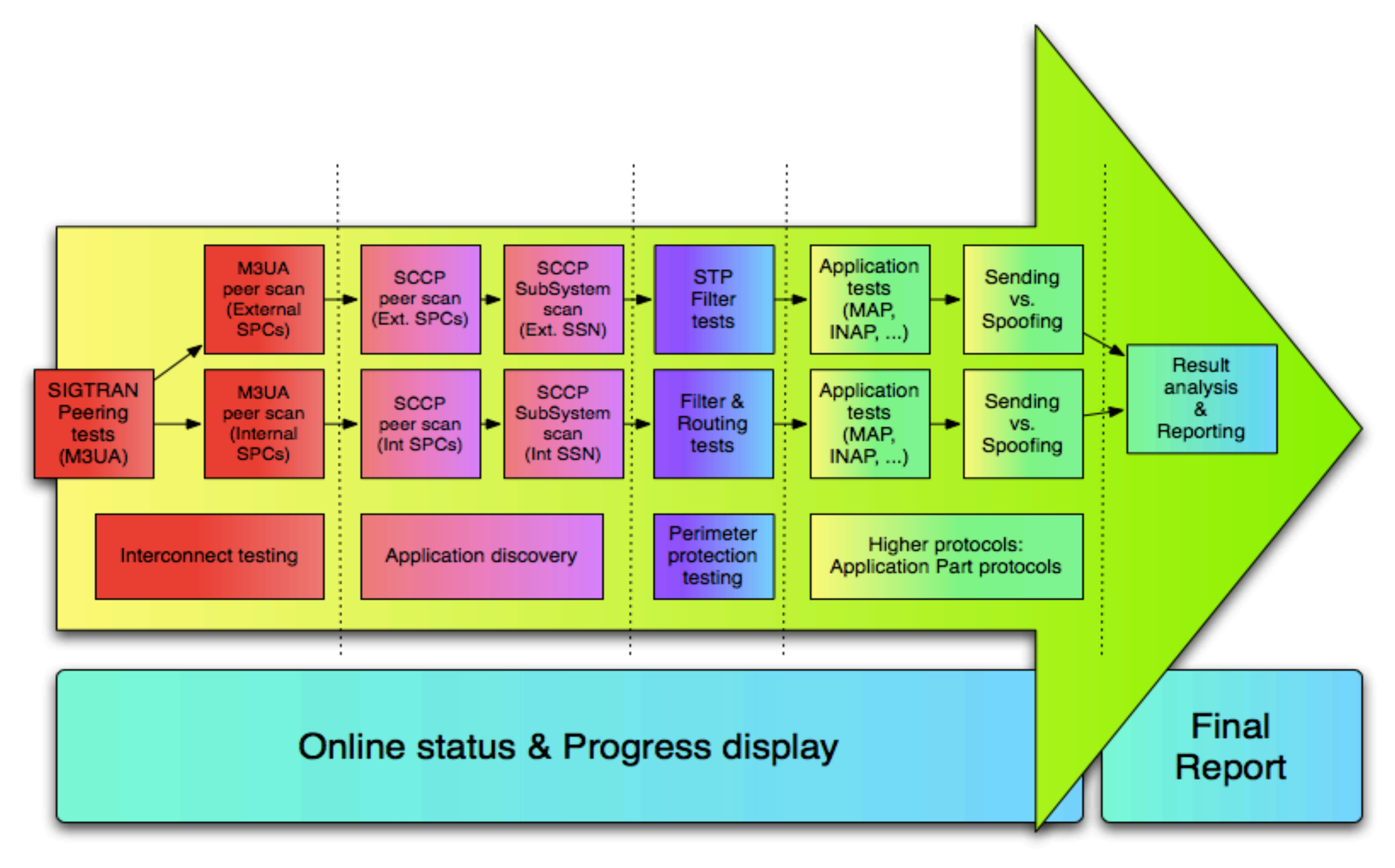


```
⊟ GSM Mobile Application
  ⊟ Component: invoke (1)
    ⊟ invoke
        invokeID: 1
      ⊟ opCode: localValue (0)
          localValue: insertSubscriberData (7)
      ⊟ msisdn: 9197999999999F9
          1... .... = Extension: No Extension
          .001 .... = Nature of number: International Number (0x01)
          .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
          Address digits: 79999999999
          Country Code: 7 Russian Federation,Kazakstan length 1
        category: 0A
        subscriberStatus: serviceGranted (0)
      ⊟ teleserviceList: 4 items
          TeleserviceList: shortMessageMO-PP (34)
          TeleserviceList: shortMessageMT-PP (33)
          TeleserviceList: emergencyCalls (18)
          TeleserviceList: telephony (17)
      ⊟ provisionedSS: 3 items
        ⊞ Ext-SS-InfoList: forwardingInfo (0)
        ⊞ Ext-SS-InfoList: forwardingInfo (0)
        ⊞ Ext-SS-InfoList: forwardingInfo (0)
```

Fuzzing, research and DoS

- Fuzzing only in testbed environment
- Because it’s easy to DoS equipments
- Telecom developer obviously don’t think like hackers
  - MGW: hardcoded Backdoor found in OAM terminal
  - eNodeB: protocol flaw leads to DoS
  - HLR/HSS: DB/Directory protocol leads to DoS + Diameter flaw
- Equipments are rarely tested before integration/production

Complete audit process


SIGTRAN Peering tests (M3UA)

M3UA peer scan (External SPCs)

M3UA peer scan (Internal SPCs)

SCCP peer scan (Ext. SPCs)

SCCP SubSystem scan (Ext. SSN)

SCCP peer scan (Int SPCs)

SCCP SubSystem scan (Int SSN)

STP Filter tests

Filter & Routing tests

Application tests (MAP, INAP, ...)

Sending vs. Spoofing

Application tests (MAP, INAP, ...)

Sending vs. Spoofing

Result analysis & Reporting

Interconnect testing

Application discovery

Perimeter protection testing

Higher protocols: Application Part protocols

Online status & Progress display

Final Report

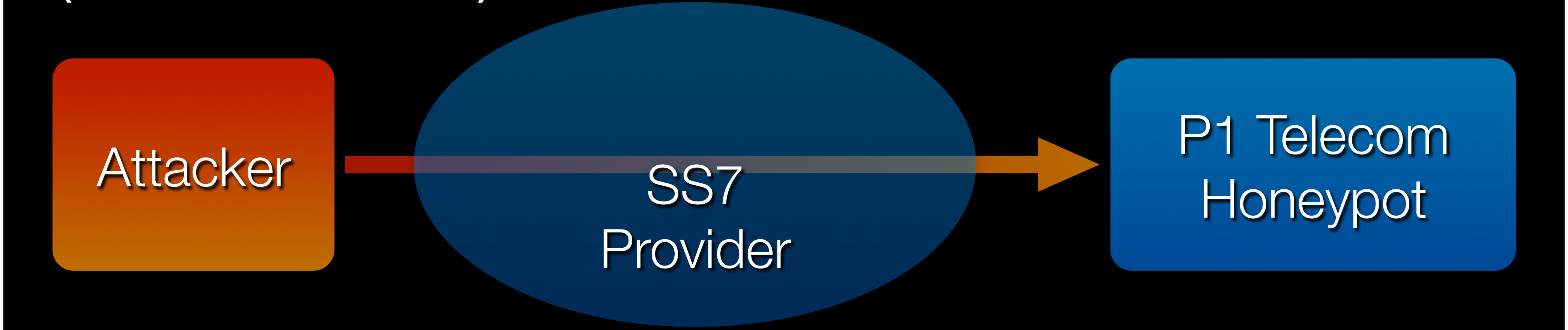
4. Detect & Protect

- IP IDS don't detect these problems
- Previous Lack of IDS for telecom networks
- Fraud Management Systems target only CDR: bills, statistical analysis
- DShield.org don’t log SCTP attempts
- “netstat -anp” doesn’t list SCTP associations
- hard to track! We’re building tools to help.

Tales of Telecom Honeypots

- Fraud and attacks in telecom is mostly stealth
  - But the impact is massive (100k to 3 million Euro per incident is typical)
- Telecom engineers mindset is not as open for proactive security as in IP crowds
  - Prefer not to do anything and suffer from attacks
  - “If nothing is there to detect attacks, there are no attacks”
- Lack of threat intelligence in the telecom domain

SS7 Honeypot Deployment (standalone)

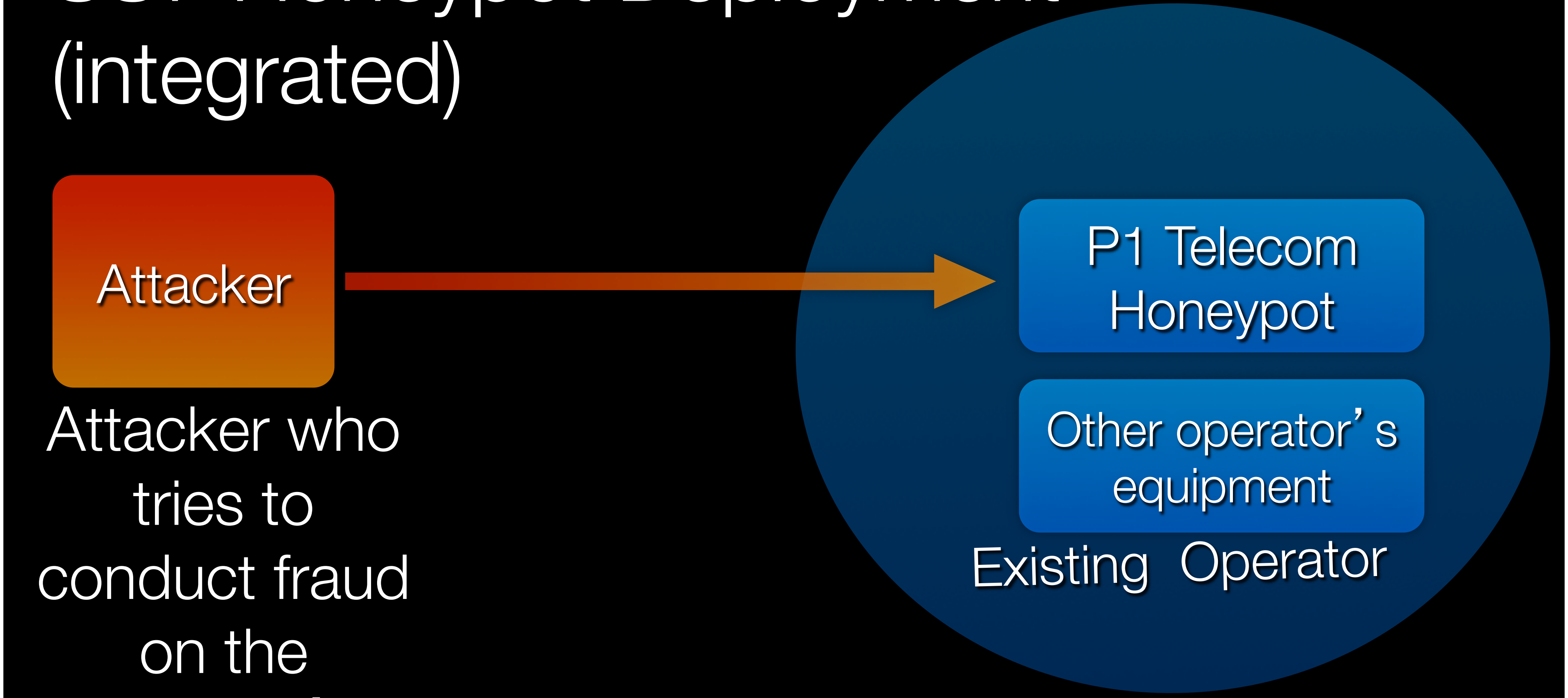


Attacker who tries to conduct fraud on the target system

SS7 Provider who manages SS7 links (like ISP)

SS7 Honeypot with SS7 link and address (pointcode or SPC)

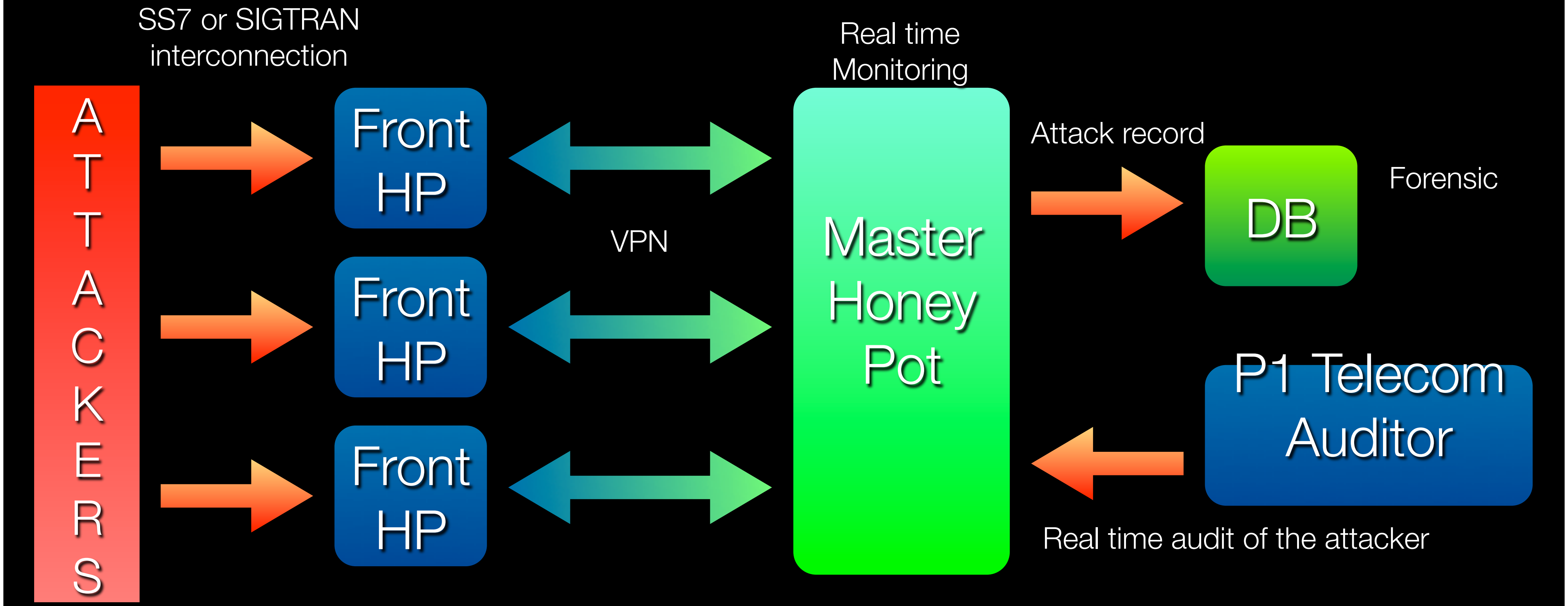
SS7 Honeypot Deployment (integrated)



Attacker who tries to conduct fraud on the operator’s system

SS7 Honeypot within operator SS7 network

Architecture



- Interconnection is like a VPN, always two-way
- If attackers does requests (interco), we can request too
- We conduct scan with P1 Telecom Auditor through interco.

Detection results

- Realtime detection of scans (IDS)
  - SIGTRAN scans
  - SS7 scans
- Detection of telecom specifics
  - SIM Boxes (subscription fraud),
  - traffic steering and anti-steering packets/techniques
  - Illegal traffic routing (mostly SMS, never seen before by operator, “lost in traffic”)

Honeypot results

- Threat intelligence!
- Nice attacker fingerprints:
  - Single node attackers (stack on one system)
  - Whole carrier infrastructure attacking (insider? relay? approved?)
- Helps the blacklisting of IDs, Phone numbers, ...
- And identification of the fraudsters

Conclusions

- End of walled garden era, more exposed:
- High Exposure in term of IP-reachability (starting in 3G/IMS) and reachability of the IP-equipment (specifically in LTE networks)
- Network complexity (planes/layers) and protocol diversity make it very hard to get right from the beginning.
- Few “dare” to audit / test their telecom environment.
- Tools and services are now mature and efficient.
- First need to visualize the problem: discovery, awareness.

Credits

- Everybody from Telecom Security Task Force
- Fyodor Yarochkin
- Emmanuel Gadaix
- Raoul Chiesa
- Daniel Mende, Rene Graf, Enno Rey
- Everyone at P1 Security and P1 Labs

Thank you!

Questions?

Ask: Philippe.Langlois@p1sec.com

Hackito Ergo Sum, Paris, France

12-14 April 2012

Russia is the country of honor for Hackito 2012!

Submit a talk!

[redacted]

Backup slides

P1 Security
http://www.p1sec.com

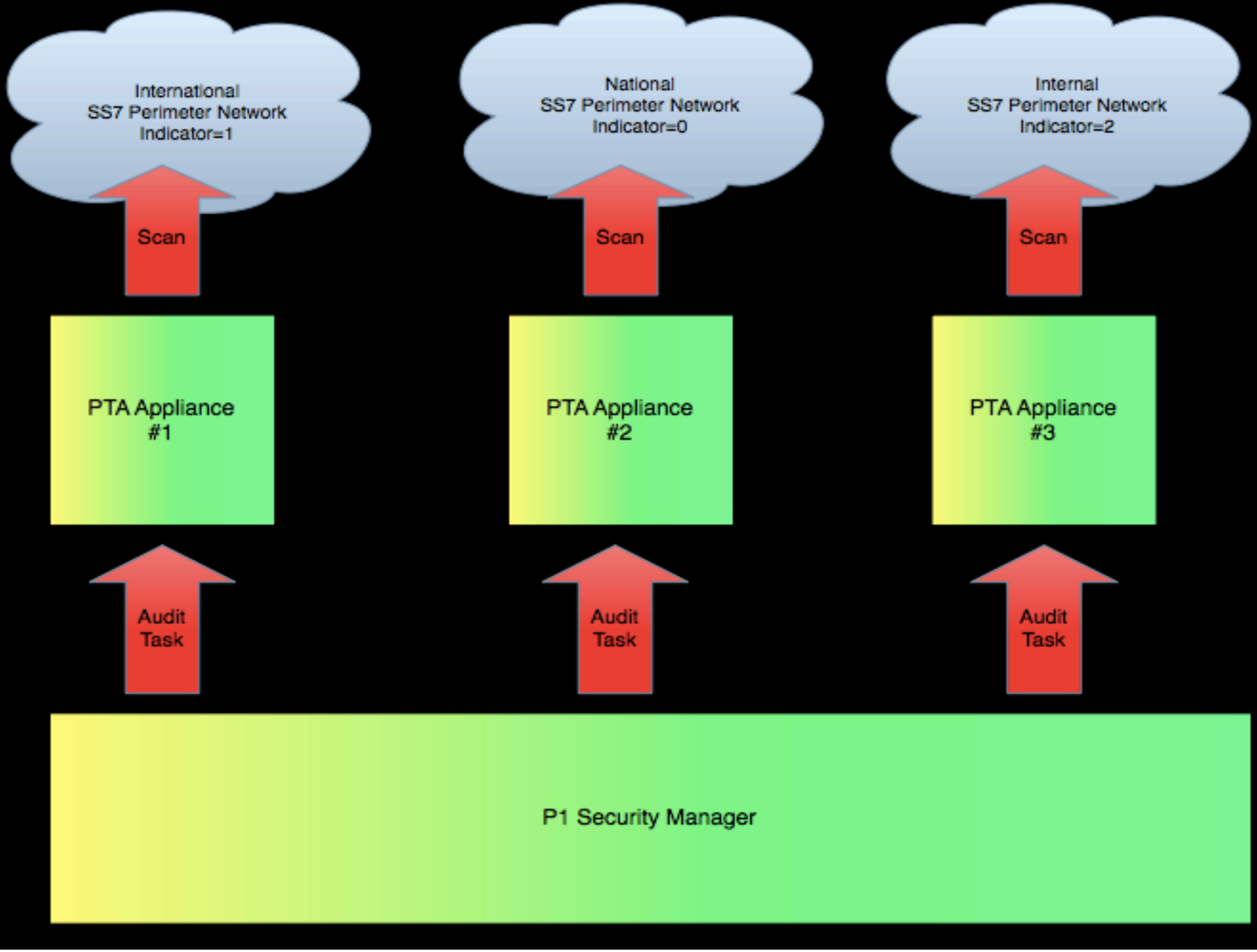
Problem

- Mobile Network Operators and other Telecom Operators
  - use Fraud Management System that are reactive only, only see fraud when it has stolen money from the operator,
  - have no way to tell if their network weaknesses are,
  - must wait for fraud, network downtime, crashes, spam, intrusions to happen in order to see how it happened.
- Governments, safety agencies and telecom regulators
  - have no way to assess the security, resiliency and vulnerability of their Telecom Critical Infrastructure

P1 Security Solution

- PTA gives vision on Telecom signaling networks (SS7, SIGTRAN, LTE sig), a security perimeter previously without technical audit.
- Telecom and Mobile Operator can scan and monitor their signaling perimeter as they do for their Internet and IP perimeter, detecting vulnerabilities before hackers, fraudsters and intruders do.
- Delivers metric for management, reports and fixes for experts.
- Right now, all the following problems go undetected (next pages) and could be detected with PTA:

PTA Deployment



International
SS7 Perimeter Network
Indicator=1

National
SS7 Perimeter Network
Indicator=0

Internal
SS7 Perimeter Network
Indicator=2

Scan

Scan

Scan

PTA Appliance
#1

PTA Appliance
#2

PTA Appliance
#3

Audit
Task

Audit
Task

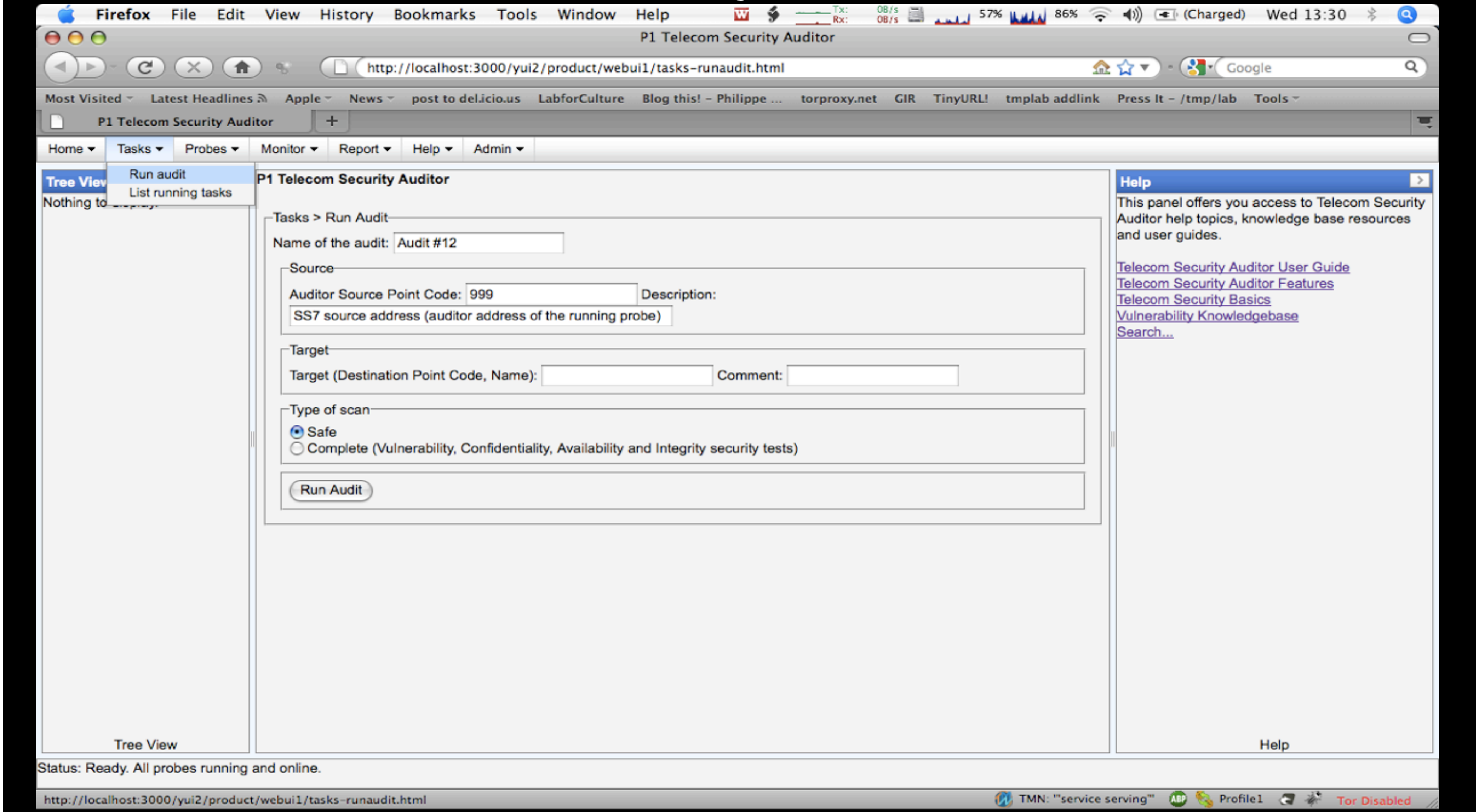
Audit
Task

P1 Security Manager

PTA Audits

- PTA Audits simulate human analysis of a SS7 signaling network.
  - It is composed of a set of signaling tests each representing one category of attack scenario or one specific attack or fraud attempt.
  - The Test Knowledge Base is constantly updated with new attack scenarios.
- The behavior, strategy and analysis of the Audit results is driven by a Machine Learning engine using SVM methods to mimic the intelligence of a human expert.

Web Access: Easy & Standardized



Firefox File Edit View History Bookmarks Tools Window Help
57% 86% (Charged) Wed 13:30
Most Visited Latest Headlines Apple News post to del.icio.us LabforCulture Blog this! - Philippe ... torproxy.net GIR TinyURL! tmplab addlink Press It - /tmp/lab Tools
Home Tasks Probes Monitor Report Help Admin
Run audit
List running tasks
Tree View
Run Audit
Tree View
Help

P1 Telecom Security Auditor

http://localhost:3000/yui2/product/webui1/tasks-runaudit.html

Nothing to display.

Tasks > Run Audit

Name of the audit: Audit #12

Source

Auditor Source Point Code: 999 Description: SS7 source address (auditor address of the running probe)

Target

Target (Destination Point Code, Name): Comment:

Type of scan

● Safe

○ Complete (Vulnerability, Confidentiality, Availability and Integrity security tests)

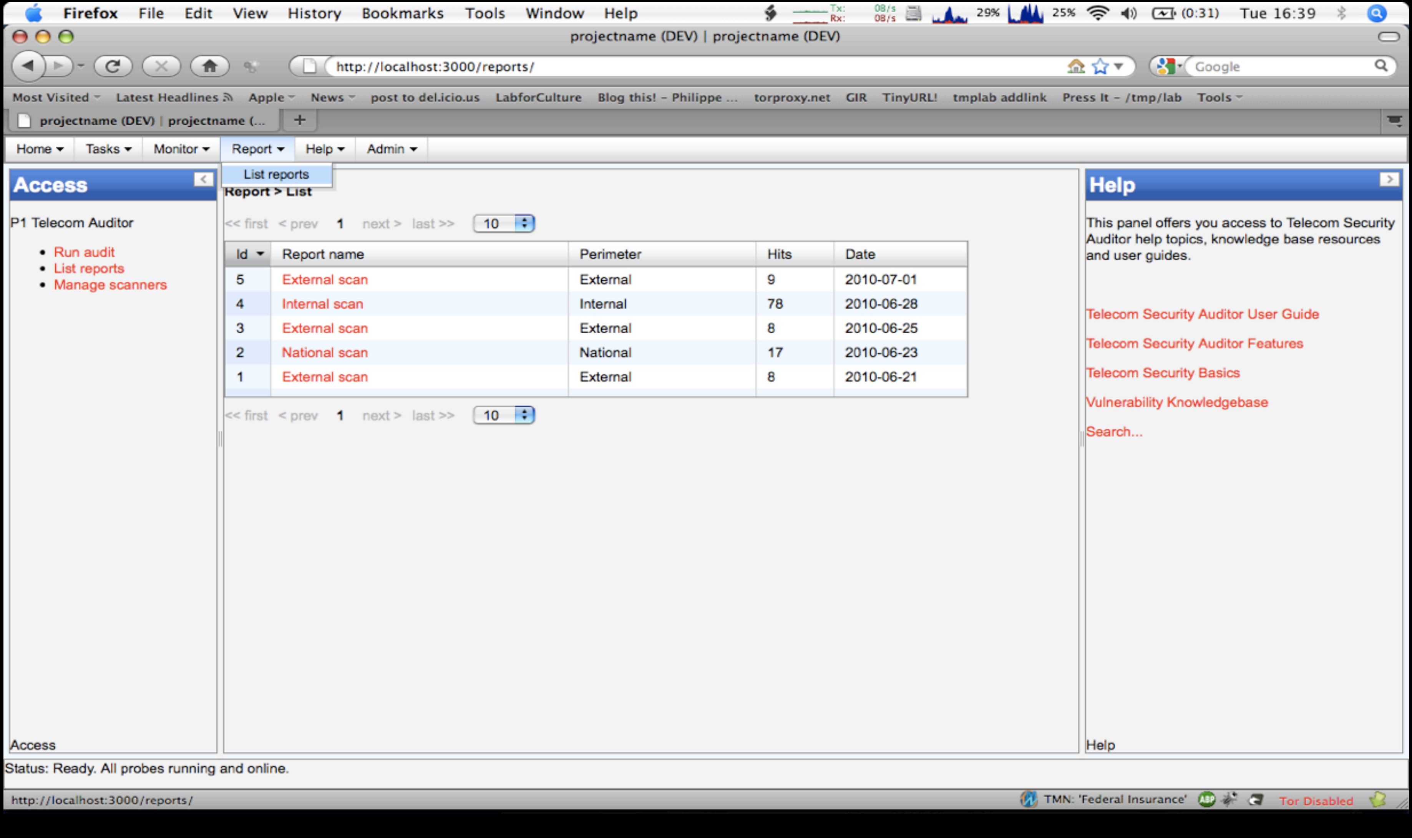
This panel offers you access to Telecom Security Auditor help topics, knowledge base resources and user guides.

- Telecom Security Auditor User Guide
- Telecom Security Auditor Features
- Telecom Security Basics
- Vulnerability Knowledgebase
- Search...

Status: Ready. All probes running and online.

http://localhost:3000/yui2/product/webui1/tasks-runaudit.html TMN: "service serving" Profile1 Tor Disabled

Report Management


Firefox File Edit View History Bookmarks Tools Window Help
Tue 16:39
projectname (DEV) | projectname (DEV)
Google
Most Visited Latest Headlines Apple News post to del.icio.us LabforCulture Blog this! – Philippe ... torproxy.net GIR TinyURL! tmplab addlink Press It – /tmp/lab Tools
Home Tasks Monitor Report Help Admin
List reports
Access
P1 Telecom Auditor
Run audit
List reports
Manage scanners
Report > List
<< first < prev 1 next > last >> 10
Help
Telecom Security Auditor User Guide
Telecom Security Auditor Features
Telecom Security Basics
Vulnerability Knowledgebase
Search...
TMN: 'Federal Insurance'
Tor Disabled

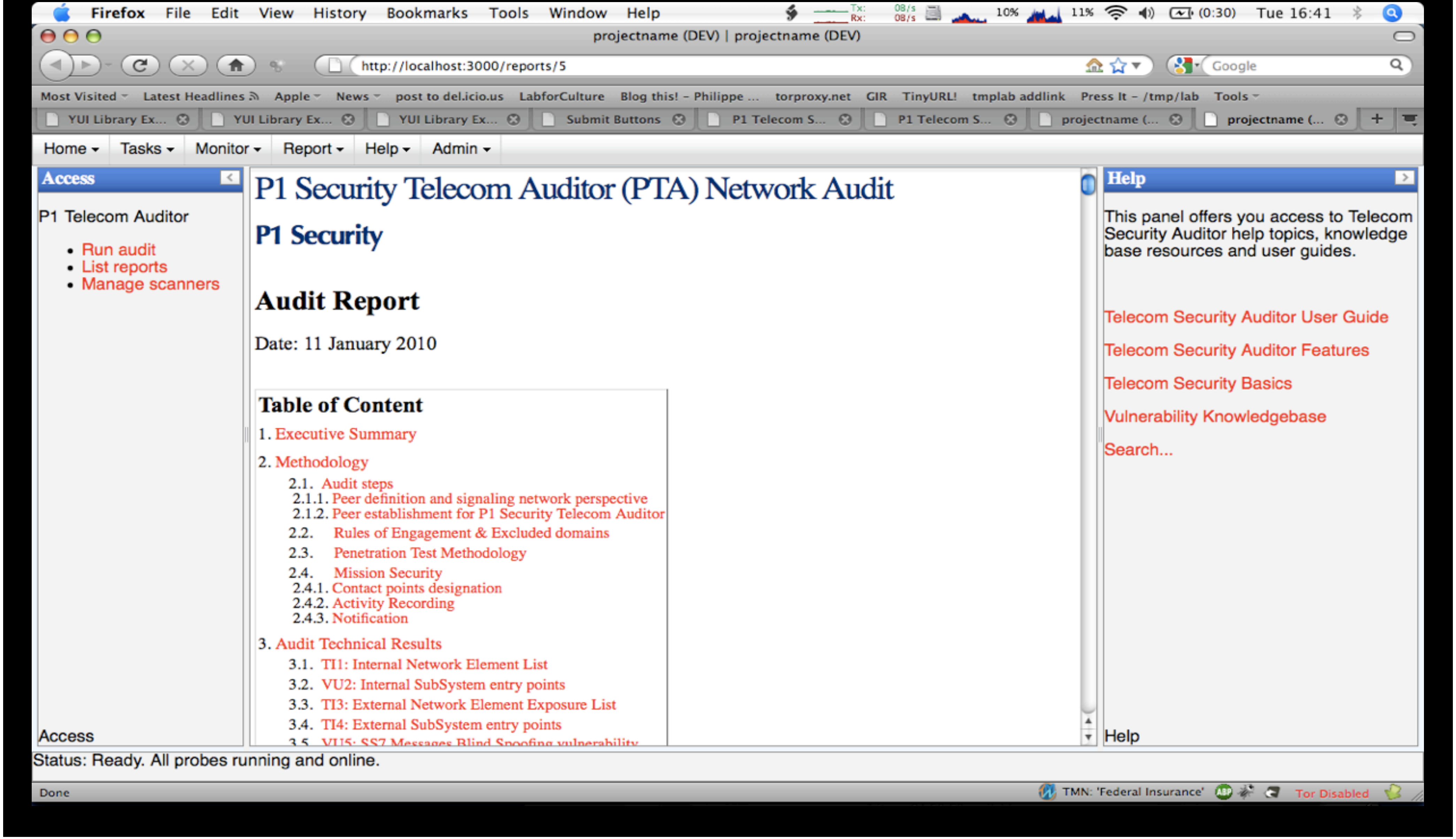
http://localhost:3000/reports/

Id	Report name	Perimeter	Hits	Date
5	External scan	External	9	2010-07-01
4	Internal scan	Internal	78	2010-06-28
3	External scan	External	8	2010-06-25
2	National scan	National	17	2010-06-23
1	External scan	External	8	2010-06-21

This panel offers you access to Telecom Security Auditor help topics, knowledge base resources and user guides.

Status: Ready. All probes running and online.

PTA Report



Access

P1 Telecom Auditor

- Run audit
- List reports
- Manage scanners

Access

P1 Security Telecom Auditor (PTA) Network Audit

P1 Security

Audit Report

Date: 11 January 2010

Table of Content

Help

This panel offers you access to Telecom Security Auditor help topics, knowledge base resources and user guides.

Telecom Security Auditor User Guide

Telecom Security Auditor Features

Telecom Security Basics

Vulnerability Knowledgebase

Search...

Help

Status: Ready. All probes running and online.

Who?

- Established management team
  - Avg of 15 year of industry background, both Security and Telecom.
  - Successful Entrepreneurs (Qualys, INTRINsec, TSTF)
- Start-up launched in January 2009
  - Already established references in Europe and Asia
  - Financial backing from private investors