P1 Security
Priority One Security

Remotely crashing HLR... MSC... STP... MME...

Why it took telecom industry 20 years to recognize the problems with SS7

Philippe Langlois, P1 Security

TROOPERS
MAKE THE WORLD A SAFER PLACE

Intro

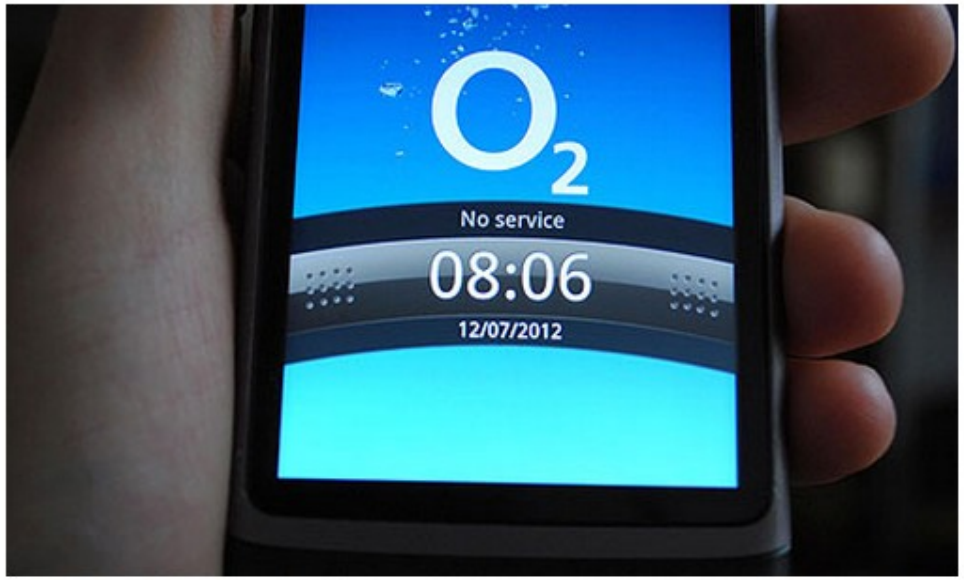
- Philippe Langlois
  - Founder of Qualys, Worldnet, TSTF, WaveSecurity, Non-Linear Group, Immunap, P1 Security
- Entrepreneur, Security, Networking
  - Since 1987 in security
  - Since 1993 starting companies
- Niche products, Blue ocean strategy

O2 network 'fully restored' after 24-hour blackout

Mobile network apologises, telling its users to turn phone on and off again if they are still having problems

Josh Halliday and **David Batty**
guardian.co.uk, Thursday 12 July 2012 14.19 BST

Article history



Hundreds of thousands of O2 customers were unable to use their mobile phones after the operator's network crashed. Photograph: Andy Hepburn/PA

O2 has said its mobile network is now fully restored after a 24-hour blackout left hundreds of thousands of its customers unable to receive calls or text

Technology
Telecoms · Mobile phones

Business
Telecommunications industry

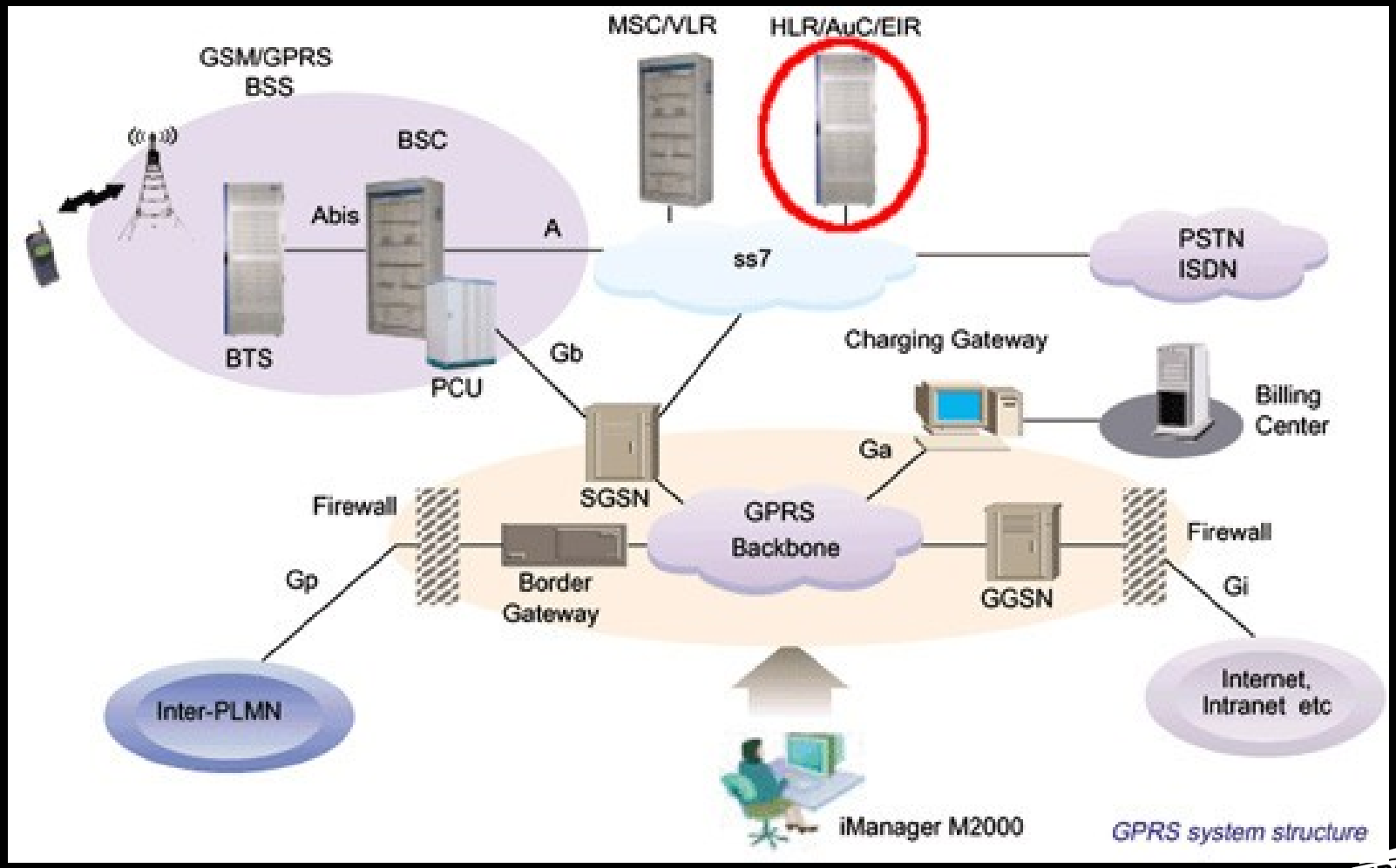
UK news

More news

More on this story

O2 apologises over 'embarrassing' network problems
Mobile operator likely to have to pay compensation to the

HLR Crash?

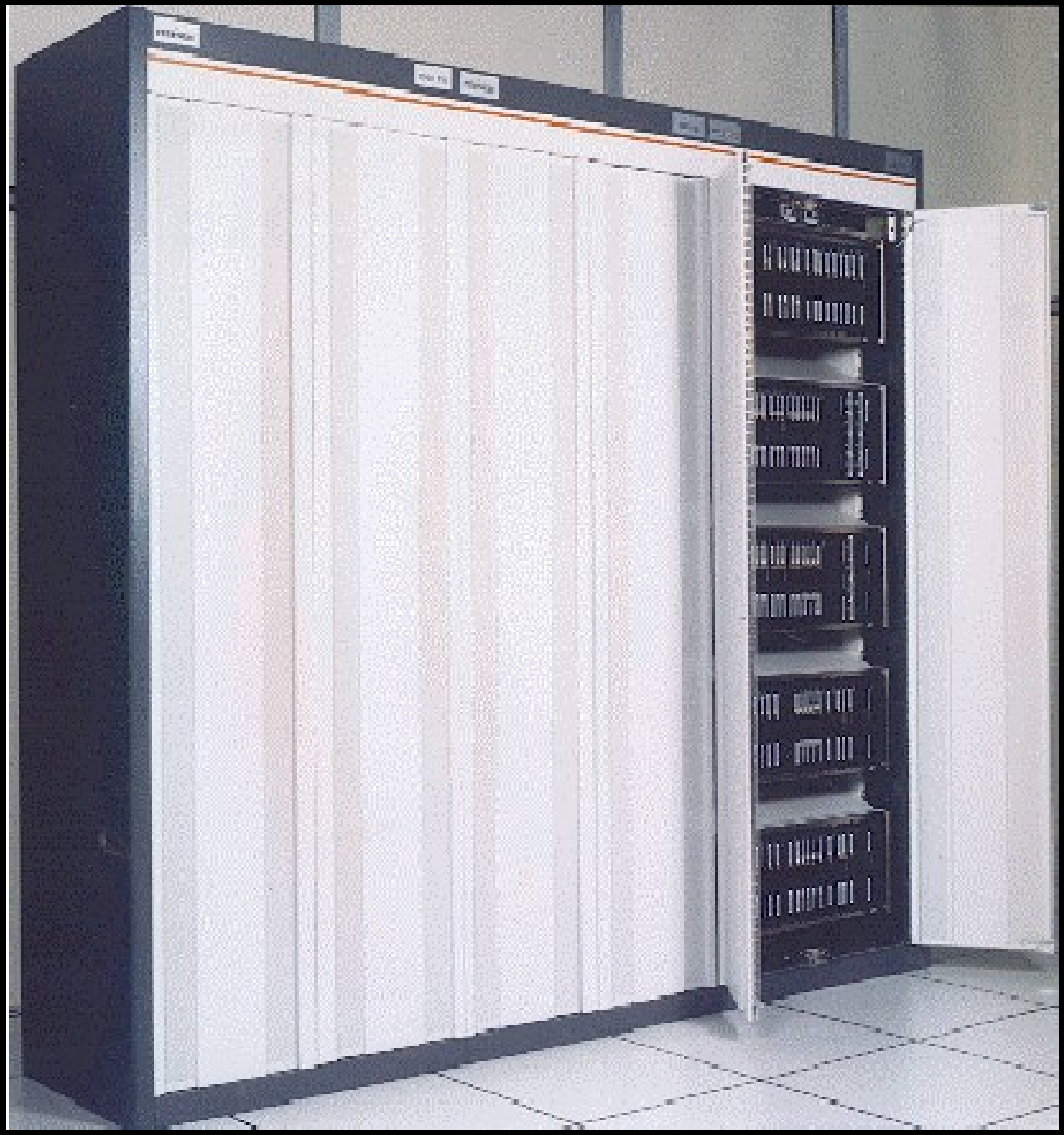

MSC/VLR
HLR/AuC/EIR
GSM/GPRS
BSS
BSC
Abis
A
ss7
PSTN
ISDN
BTS
PCU
Gb
Charging Gateway
Billing
Center
Ga
SGSN
Firewall
GPRS
Backbone
Firewall
Gp
Border
Gateway
GGSN
Gi
Inter-PLMN
Internet,
Intranet etc
iManager M2000
GPRS system structure

HLR Crashes impact

- O2 (UK)
  - Network Downtime for 1 day, instability for 2 days
- Orange (FR)
  - Network Downtime for nearly 1 day this summer (2012)
- And these were not even due to attacks
- Most often
  - New equipment or feature deployed in network
  - Protocol incompatibilities causes software instability

HLR Crash Symptoms

- “When receiving traffic, all cluster nodes started to become unresponsive, one after another, eventually knocking off all 12 cluster nodes”
- Solaris Cluster nodes
  - 128 Gb RAM
  - High end SUN server
  - SAN connected
- Running full load balanced, distributed HLR software



P1 Security
Priority One Security

TROOPERS
MAKE THE WORLD A SAFER PLACE

Explicit Lyrics^W Logs

P1 Security
Priority One Security

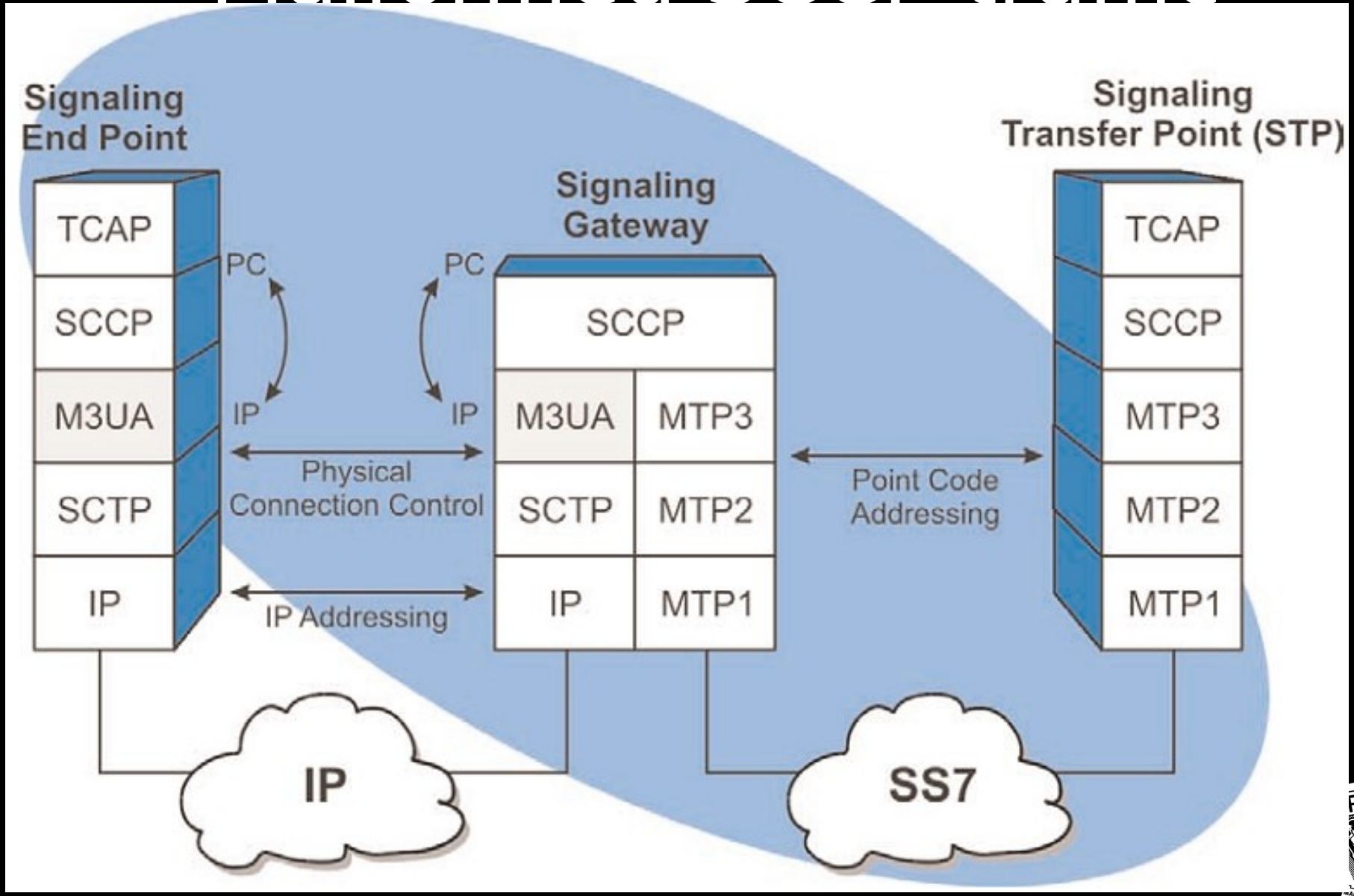
hlr-trace.txt

```
28/09/2012 17:55:48 [10120]: main.cxx.255: Problem sending a message, TYPE=SINGLE DUMP: 11: No
destination: INAP:CM2. Unknown GroupID:2
Message: DESTADDR :
01001c6b00->  de e8 ea 26 00 00 49 89  00 30 09                 .....$.P.0.
,ORIADDR :
01001c6c80->  de e8 ea 26 00 00 49 89  00 80 67                 .....$.P..g
QOS = 0x80000001
,APPLNAME :
01001c6ae0->  4c 89 ff 31 f6 32 b2                             .....2.
APPLINFO :
COMPO : TRUE
CLASS = 0
IVK = 1
CORR ID = -1
OPERATION :
01001c6bc0->  00                                               .
PARAM :
01006fff50->  cd 69 08 3e 8c 48 92 24  b2 6d d7 30 be cf d8 e4 0.......$.q.`..
01006fff60->  c8 a7 97 81 d0 1e 23 dc  38 99 5f 61 fe 85 02 03 ...$..U.e.......
01006fff70->  01 00 01 a3 81 b4 30 81  b1 30 0e 06 03 55 1d 0f $.P.p...........
01006fff80->  01 01 ff 04 04 03 02 01  86 30 16 06 03 55 1d 25 u....2.2..X.....
01006fff90->  01 01 ff 04 0c 30 0a 06  08 2b 06 01 05 05 07 03 3....4.......$`
01006fffa0->  03 30 0f 06 03 55 1d 13  01 01 ff 04 05 30 03 01  ......2. .%"..5
01006fffb0->  01 ff 30 1d 06 03 55 1d  0e 04 16 04 14 8e 69 a6 .....6.L/.[..7..
01006fffc0->  c4 77 42 4e 04 a5 56 42  9c 51 1f 86 da d2 20 8f $.P.p..9....pA0C
01006fffd0->  23                                               #
TIMEOUT = 0
LASTCP :0
, SEND NOK: 13: No more free buffer
```

HLR crash

- Investigated a few HLR crashes for Operators
  - When there was dispute with vendor
  - Vendor always try to keep it private with Operators
- Some Vendors billed Operators when HLR was not under maintenance contract anymore
  - Over 500,000 USD
  - “Typical in Telecom industry”
- We decided to investigate further into existing HLR software and crashes

Malformed SCCP traffic



Simple SCCP “append fuzz”

P1 Security
Priority One Security

sccp-1-fuzzed.pcap [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2	1	SCCP (Int.	198	UDT [Malformed Packet]

```
▷ Frame 1: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits)
▷ Ethernet II, Src: Vmware_b0:9e:df (00:0c:29:b0:9e:df), Dst: Vmware_f5:c3:4e (00:0c:29:f5:c3:4e)
▷ Internet Protocol Version 4, Src: 192.168.2.103 (192.168.2.103), Dst: 192.168.2.102 (192.168.2.102)
▷ Stream Control Transmission Protocol, Src Port: m3ua (2905), Dst Port: m3ua (2905)
▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
▽ [Malformed Packet: SCCP]
  ▽ [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
      [Message: Malformed Packet (Exception occurred)]
      [Severity level: Error]
      [Group: Malformed]
```

```
0000  00 0c 29 f5 c3 4e 00 0c  29 b0 9e df 08 00 45 02   ..)..N.. )......E.
0010  00 b8 00 56 40 00 40 84  b3 4c c0 a8 02 67 c0 a8   ...V@.@. .L...g..
0020  02 66 0b 59 0b 59 ba 29  5b 58 a8 3b cf aa 00 03   .f.Y.Y.) [X.;....
0030  00 98 e3 a8 e1 b8 00 01  00 00 00 00 00 03 01 00   ........ ........
0040  01 01 00 00 00 88 00 06  00 08 00 00 00 01 02 10   ........ ........
0050  00 75 00 00 00 02 00 00  00 01 03 02 00 00 09 01   .u...... ........
0060  03 05 09 02 42 08 04 43  02 00 81 5a 02 24 63 db   ....B..C ...Z.$c.
0070  43 c1 ff 92 48 57 ab 15  a0 6c ac 33 ea 6d 39 69   C...HW.. .l.3.m9i
0080  b4 c2 f2 29 c2 08 75 ba  73 e9 20 77 9a 97 c0 b7   ...)..u. s. w....
0090  b4 14 fc 65 01 29 57 6f  59 f8 f3 55 2a 81 7e 80   ...e.)Wo Y..U*.~.
00a0  dd ee e7 95 32 45 7a 96  dc c0 c1 83 99 59 1f 4a   ....2Ez. .....Y.J
00b0  a0 cc 09 d8 e4 1d b7 b1  d0 93 a3 23 ea c3 43 dd   ........ ...#..C.
00c0  2d d5 e2 5f db 53                                  -.. .S
```

Wireshark expert group (e... | Packets: 1 Displayed: ... | Profile: Default

Vendor claims “Bug has been fixed”

- Right...
- Simple SS7 equivalent (over SCCP) of
  - “cat /dev/random | nc target.signaling.operator.com 80”
  - Result: 2 crashes
- Evolved fuzzer
  - Supports SS7 TCAP protocol: 7 more crashes
  - S upports SS7 MAP protocol: 19 more crashes
- Vendor discussion

One particular vendor discussion

P1 Security
Priority One Security

- Feels like talking to a big OS vendor in the 1990s
  1. “Who are you?”
  2. “Do you have a license for our product?”
  3. “What is fuzzing?”
  4. “Who authorized you to perform such fuzz testing?”
  5. “Send me the content of your harddrive, sources and emails”
  6. “We have already fuzzed our product using XYZ commercial fuzzer, you must be mistaken in your result”
  7. “We cannot reproduce”
- Silently fixes, push upgrades only to the reporting customer
- All this cost them nothing

TROOPERS
MAKE THE WORLD A SAFER PLACE

“Production ^ Debug” HLR Crash

- Mutually exclusive
  - Run production
  - Be able to debug problems and crashes
- Origin of the crash
  - Debug possible, Core dump enabled
  - HLR process crashes
  - Nearly 100 Gb of process to dump to disk
  - Average time = 2mn
- Attack rate = cluster size * 60 / crash time

  = 12*60/2 = 360 packets/hour = 6 packets/minutes

exposure

HLR Attack surface

- Legacy protocols (SCCP, TCAP, MAP)
- Diameter
- Billing interfaces
- Provisioning
- OAM
- Reporting interfaces
- Business, Datawarehousing, Marketing, Analytics
- Legal, Regulatory and Law Enforcement

Impact of the legacy sandwich

P1 Security
Priority One Security

Legacy TDM	IP-centric / SIGTRAN 80% of networks	LTE 15% of networks
MTP1	Gigabit Ethernet	Gigabit Ethernet
MTP2	ARP	ARP
MTP3	IP	IP
SCCP	MPLS	MPLS
TCAP	BGP	BGP
MAP	IP	IP
	SCTP	SCTP
	M3UA	Diameter
	SCCP	MAP
	TCAP	
	MAP	

Reachability

- IP reachability
  - Extremely limited
  - Local to VLAN only
  - Segmented Signaling plane
- SCCP reachability
  - Worldwide
  - LDC operators are routinely compromised
  - Average time to intrusion in pentest: 2 weeks

P1 Security
Priority One Security

One image is stronger than 10,000 pwns

IP Reachability? No way!

TROOPERS
MAKE THE WORLD A SAFER PLACE

221. . .
China Unicom Chongqing Province Network
Added on 23.01.2013
Chongqing

NetBIOS Response
Servername: HLR-ZTE
MAC: 00:0a:eb:2b:3e:02

Names:
HLR-ZTE <0x0>
WORKGROUP <0x0>
HLR-ZTE <0x20>
WORKGROUP <0x1e>
WORKGROUP <0x1d>
__MSBROWSE__ <0x1>

67. . .
Comporium Communications
Added on 18.09.2012
Fort Mill

.cm.comporium.net

NetBIOS Response
Servername: R9HLR2X
MAC: f0:de:f1:a2:7c:ba

Names:
R9HLR2X <0x20>
R9HLR2X <0x0>
MOROCH <0x0>
MOROCH <0x1e>
MOROCH <0x1d>
__MSBROWSE__ <0x1>

P1 Security
Priority One Security

202. . .
PTCL
Added on 07.01.2013
.pie.net.pk

Tekelec IP7 SG EAGLE5 43.0.2-63.65.1 (IPGWI) Tekelec SNMP 1.0

202. . .
PTCL
Added on 15.09.2012
Rawalpindi
.pie.net.pk

Tekelec IP7 SG EAGLE5 43.0.2-63.65.1 (IPGWI) Tekelec SNMP 1.0

202. . .
Added on 13.05.2012

Tekelec IP7 SG EAGLE5 40.0.0-61.48.1 (IPGWI) Tekelec SNMP 1.0

TROOPERS
MAKE THE WORLD A SAFER PLACE

Other systems

Ericsson STP

- Ericsson STP / SGW equipment
- Denial of Service (DoS) when it receives M3UA traffic with out of bound Signaling Point Code
- Simple integer overflow
- MTP3 -> 14 bits
- M3UA -> 32 bits
- Same code: block C7DR2 (20 year old) and TPLAT
- Downtime :(

Fun with forensics

- ALOGFIND
- Crash?

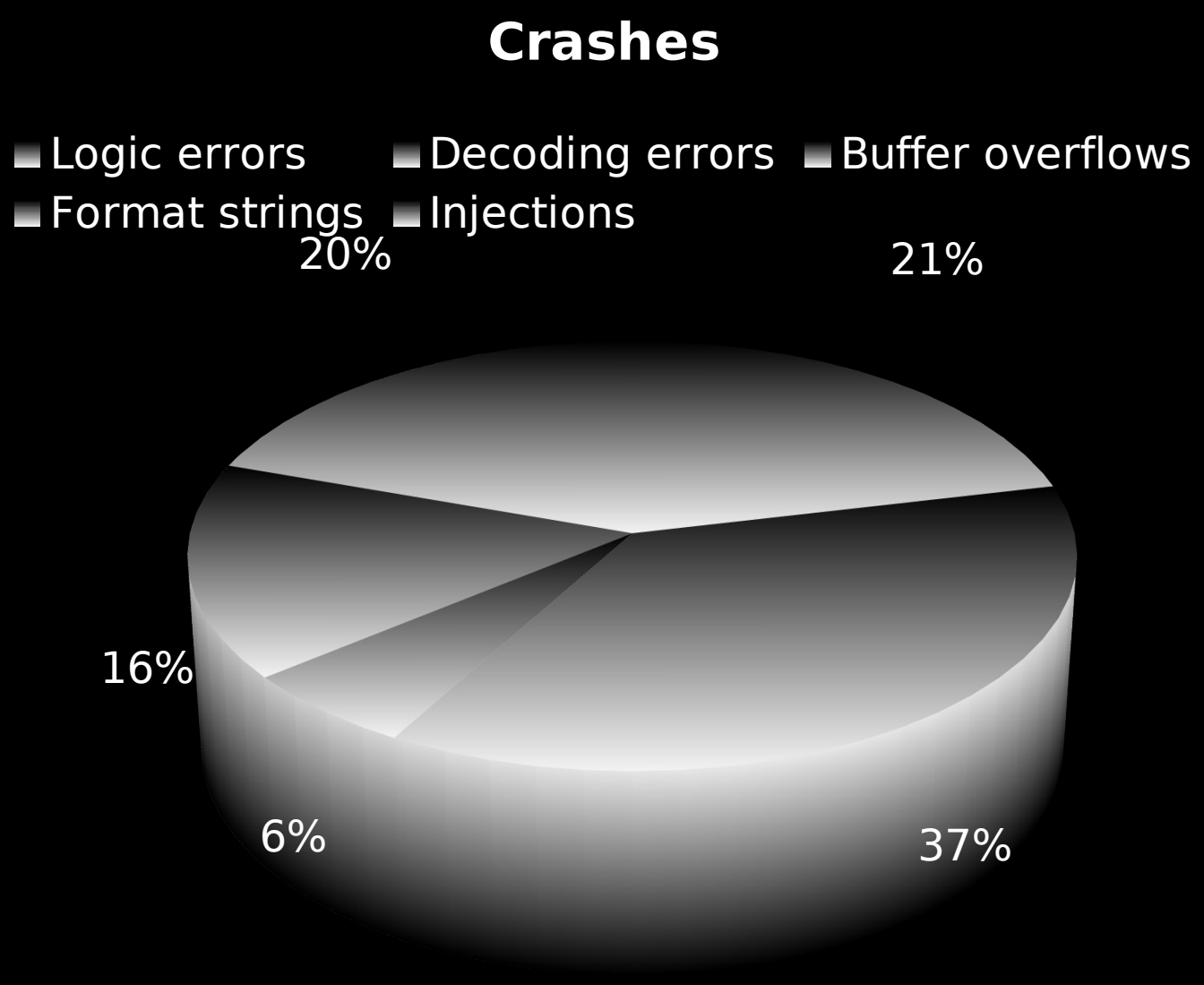
```
C:\>alogfind -a 0002 -b 0400 -e 20121020 -g 20121022 -t alp

PrcUnhandledExceptionFilter :  UNHANDLED EXCEPTION!!! (In alogfind)
```

Ericsson MSC R14

- Old interface and new interface

Industry status

Root causes of technical crashes



Occurrence in the wild

- We see many NMS traces of crashes
- During pentest
  - Always a core on Unix-based Network Elements
  - Always log traces of crashes
  - Even specific directories filled with crashes traces, core files, HD dumps of crashed machines etc…
- Some information leaks sometime about network element crashes
- It hit the news only when it’s network wide crash

Occurrence in the news

- Rarely explained
  - Only if it is witnessed by all the subscribers
- Very cautious about admitting it in public
- Consequences
  - Loss of image
  - Governmental enquiries

O2 UK suffers network glitch; France Telecom outage down to software error

12 Jul 2012

O2 UK suffered from a network outage that affected a number of its customers for almost a day, while France Telecom said a similar issue on its network last week was caused by a software problem.

The O2 network issue, in which customers had difficulty making or receiving calls, sending texts or using data, was first identified early on Wednesday (yesterday) afternoon. The operator's Live Status Checker stated at 16:45 yesterday that its engineers were dealing with the problem as a priority.

Jul 13, 2012 - 2:15PM PT

Why are mobile networks dropping like flies?

Permanent Link to Why are mobile networks dropping like flies?

BY Kevin Fitchard

7 Comments

Last week, Orange France's mobile network tanked, knocking out the mobile phones of millions of subscribers. This week the same thing happened to O2 in the U.K. U.S. carriers like Verizon and T-Mobile aren't immune either. Global networks have developed a big signaling problem.

Updated. Last week, Orange France's mobile network tanked, knocking out the mobile phones of millions of subscribers. This week the same thing happened to O2 in the U.K. The U.S. isn't immune either. Just last week T-Mobile suffered from a smaller glitch, but the granddaddy of all network failures hit Verizon Wireless in December when its LTE network went down on three separate occasions in a single month.

Why are networks suddenly conking out all over the world? It looks like global networks are developing a signaling problem – more specifically a signaling overload problem.

Instant search

RELATED

Cisco scales its mobile core to meet the smartphone boom

As mobile app usage explodes, wireless equipment vendors have been forced to not only keep pace to...

No telecommuting, please! We're signaling

The case for telecommuting is solid and gets more so with each new study. But despite this...

Why the world has suddenly come around to 4G

A new survey from Informa finds that 60 percent of all global carriers plan to deploy LTE...

SEE MORE RELATED STORIES FOR:
3g networks / outages / overload / signaling

1264 READERS RIGHT NOW

Just commented on:
Rackspace breaks out block storage with disk and SSD options

It's good to have the choice between high I/O SSDs for the likes...

Just commented on:
Hands-on with the brand new, thin and stunning iMac

Denial

- “The crash that you’ve shown is not a vulnerability because the network-wide crashes we suffered in our GSM and 3G network were caused by malformed traffic from a misconfigured equipment, not from an attacker”
- Spot the logic mistake here?
  - If the crash was not caused by attackers, then it’s not a vulnerability
  - Ouch!
- That implies that vulnerabilities exist only if exploited?
  - Vulnerability ≠ Risk ≠ Threat

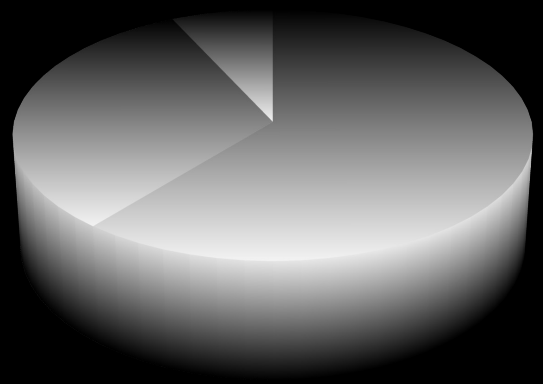
Fake security feeling

- Crashes only
- No tracing of origin
- No proof of hacking
- When proof, cover up
- When exposed, say it’s an internal problem only

Bias in analysis of equipment vulnerability

- Accessibility of crashes based on OS
- High availability mated pairs and clusters “Shield” identification of crashes
- Silent crash and restart
  - No reporting in NMS
  - No accessible crash files
- Vendor-only notifications

Equipment types

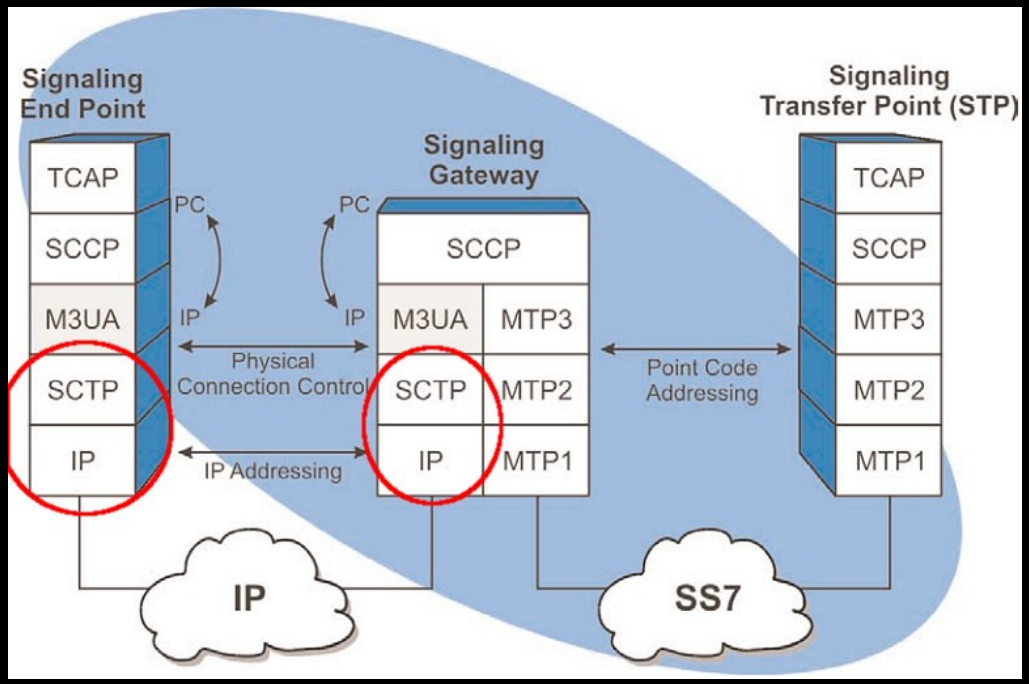


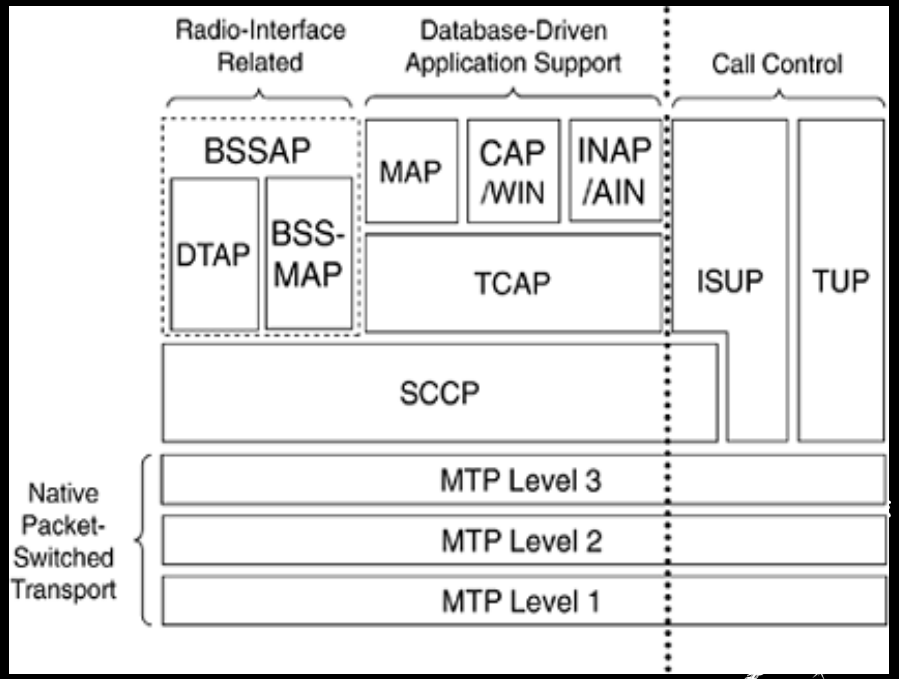
- Monolithic
- Commercial OS
- Open source OS

Fuzzing coverage and illusions

P1 Security
Priority One Security

- "We have already fuzzed our product using XYZ commercial fuzzer, you must be mistaken in your result"
- Fuzzer coverage
  - Need to reach higher protocols for more complex code path
- Commercial and generic fuzzers don't go that far





About telecom software & equipment vulnerabilities

- Good
  - Built for redudant, high availability
- Bad
  - In a nice-people only network
  - Without thinking about attackers
  - Thinking only about fraud, not denial of service
  - Fuzzing with IP fuzzer
  - Not fuzzing higher-level protocols

Threat environment

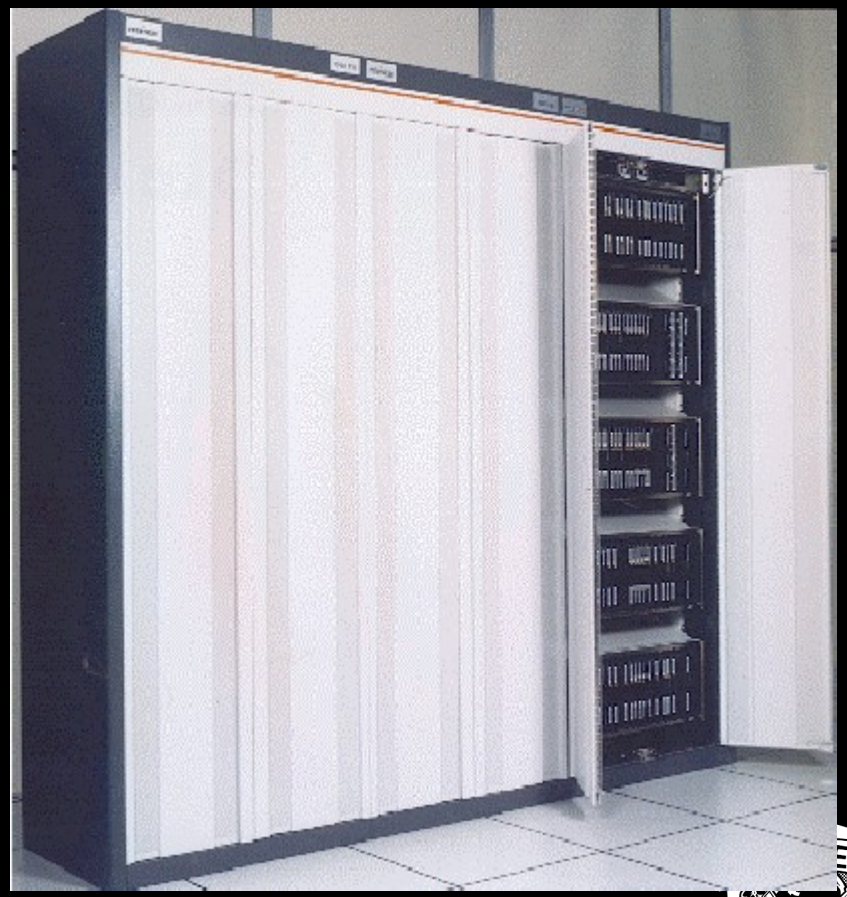
An example of Real vs. Fake in Telecom products

P1 Security
Priority One Security

SIM_NO	IMSI_NO	PUK	KI	ENCRYPTED_KIVALUE
89[redacted]0[redacted]516	427[redacted]424014	34[redacted]32373832	73A[redacted]36114BDEC0D[redacted]23A	A##551B[redacted]B2EDCB1E71B4EBA919AF4
89[redacted]0[redacted]524	427[redacted]424015	35[redacted]36323537	F6F[redacted]A3163B711B5[redacted]EE8	A##9397[redacted]BAD0FDA6DF82CA0F0ABC1
89[redacted]0[redacted]557	427[redacted]424018	33[redacted]32373339	1EA[redacted]69D5EF110EF[redacted]A66	A##8A5E[redacted]C9E9BE69358513A5AE65B
89[redacted]0[redacted]565	427[redacted]424019	35[redacted]31323335	483[redacted]3154C3051A[redacted]31D	A##0D9D[redacted]26EBAF626930AE4BF6A96

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.



Why the resistance?

Feeling like the 1980s

- Slow vendor response
- Customer (Operators) don’t get the vulnerability information
- Security through obscurity even still publicly acknowledged
- Patching boxes make them unsupported
- Lack of SDLC
- Only less than 10 actors (vendor and operator combined) are up to date in term of security

Filtering on SS7

- Also known as filtering
- Filtering on SSN nearly inexistant
  - Less than 5 operators are accurate in term of filtering
- No filtering on addresses
  - Impossible by protocol specification
- Indian Mobile Network Operator CTO
  - “Screening?”

Why is it not fixed?

- Was a lack of tools to show the problems
- Resistance in Operators
- Resistance in Vendors
- Resistance in Industry Association
- Lack of access to researchers (Network, equipment)
- Difficult trust in smaller vendor (big 5 only)
- Lack of support of government, national security projects

Resistance of Operators

- Loss of image
- Email vs. SMS trust factor
- Public acceptance
- Inquiry of regulators
- India example
- Running Nessus on Telecom network is not Telecom Security
- Lack of knowledge due to Vendors

Resistance of Vendors

- “Our turf only”
- IPR is their job security
- Outsourcing & TIO
- Even getting documentation is difficult for customers
- Know they are not doing SDLC right
- Know many existing tools are legacy-level

Resistance of Industry Associations

- Tech focus or Legal focus
  - Look at the leader of some security groups
- Protect the image
- Barrier to entry for new tech
- Protection of the main vendors
- “Inbreeding” feeling
- “Ownership” of the security groups by vendors

It is changing

How to improve? - Strategic

- National, government-led telecom monitoring TSIRT
- Operator TSOCs
- Telecom Vulnerability information feed (VKB)
- Telecom Specific Equipment certification (TCERT TCNE1)
- Adhere to TCERT (Operator, Gov, Researcher)
- Periodic perimeter scanning

How to improve?

- External pentesting (SS7, IMS, LTE)
- Recognize the perimeter
- Open up industry association
- Use specific fuzzer
- Arrival of Open Source
- Pressure of Internet-based traffic
- Specific initiatives (TCERT)

Conclusion

- Improvement in progress
  - Research, TCERT, Scans, Awareness
- Vendors lagging
  - Even preventing security
- Few operators are current on security
  - Most react to crashes only

Questions?

P1 Security
Priority One Security

TROOPERS
MAKE THE WORLD A SAFER PLACE

P1 Security
Priority One Security

Philippe.Langlois@p1sec.com

Thanks (We’re HIRING! :)

TROOPERS
MAKE THE WORLD A SAFER PLACE