ITU Workshop on “SS7 Security”
Geneva, Switzerland
29 June 2016

SS7 Security – How to Fill in the Standardization Gap,

Giulio Maggiore
ETSI TC INT Chairman, TIM
giulio.maggiore@telecomitalia.it

1956 2016
CCITT / ITU-T

Agenda

- SS7 security Map
- Main procedure affected
- Impact to standardization
- Closing Remarks

Chaos Communication Congress (CCC) Hamburg, 27th – 30th December 2015

One focus was SS7 vulnerability with 3 presentations

- Tobias Engel, “SS7: Locate. Track. Manipulate.”
- Karsten Nohl, “Mobile self-defense”
- **Laurent Ghigonis and Alexandre De Oliveira, “SS7map : mapping vulnerability of the international mobile roaming infrastructure”** https://www.youtube.com/watch?v=SfPC9IHCW-U

SS7 Security Program

- Mobile Network Operators rely on a network different from Internet that interconnects operators and other parties, to allow calls to work between operators especially when you are in another country (roaming).
- This is what is called the **"SS7 network" a.k.a. "International Roaming Infrastructure",** that by it's nature, transmits confidential customers and operators information.
- In **SS7map website (http://ss7map.p1sec.com/)**, **the first cartography of SS7 International Roaming Infrastructure vulnerabilities** is shown, to push the industry to react, and show to all of customers **the security level of the infrastructure** we are all using.
- It's time to have visibility on **which country is taking care of these issues** and protecting their population.

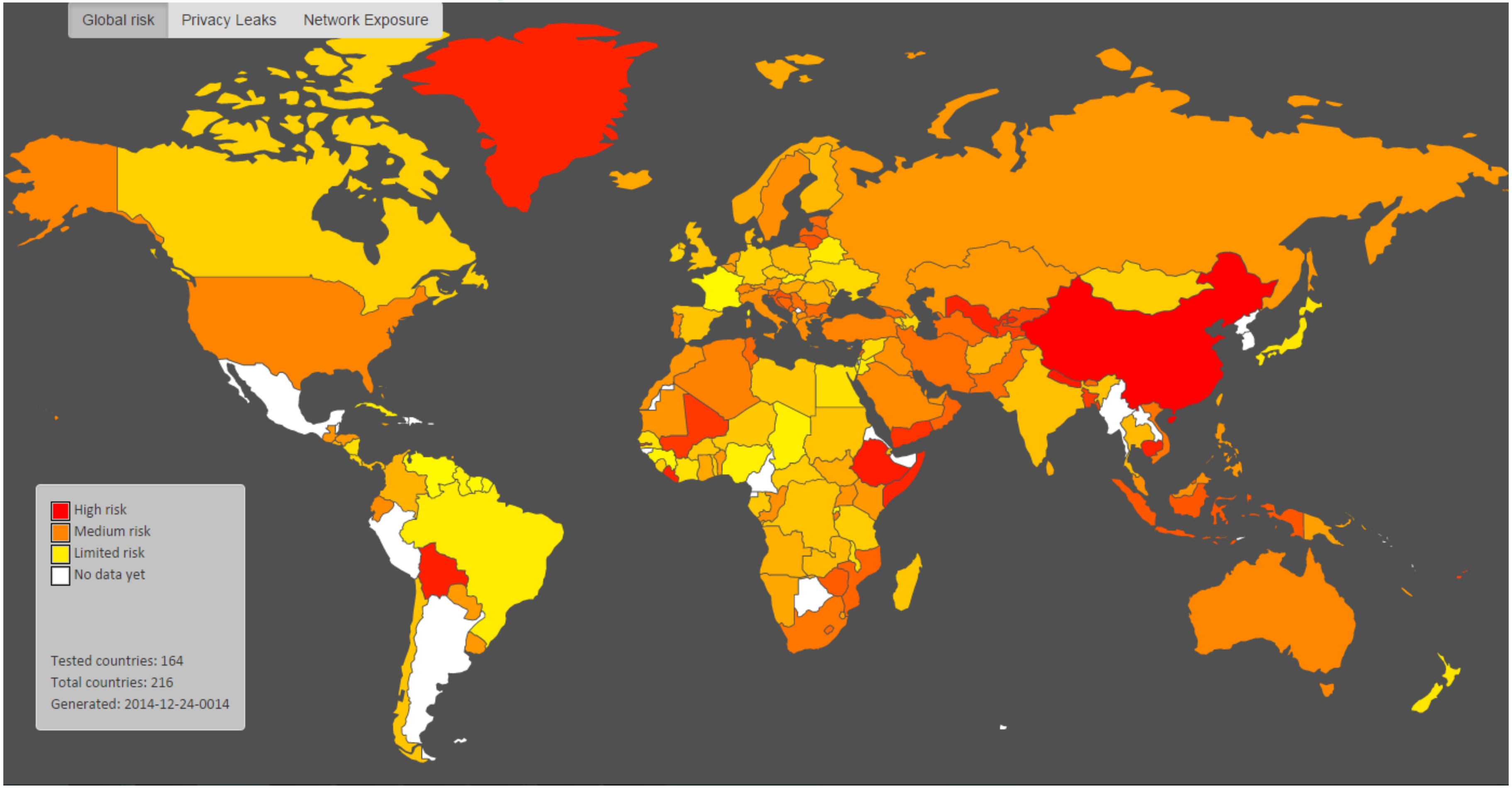
- **164 Country** in the World has been tested.
- Three categories of SS7 Map Ratings has been reported:
  - **Privacy Leaks**: how much private info of customers are leaked out to anyone on SS7 Network
  - **Network Exposure**: network elements exposed and security mechanism implemented by operators of a given country
  - **Global Risk**: mix of Privacy Leaks and Network Exposure, giving more importance to Privacy.

Privacy Leaks and Network Exposure

- **Privacy Leaks** regroup leaks of customers information of all operators in a country:
  - Subscriber location leak
  - Subscriber private information (identifiers, cryptographic keys, postpaid/prepaid status)
  - Subscriber communications confidentiality (decryption of SMS/calls using known attacks)

- In **Network Exposure** the main focus is the Core Networks of operators in a country:
  - Attack surface of the Operators (network topology, identification of the network Elements)
  - Network misconfigurations allowing attackers to modify data
  - Bypass of Network security mechanisms

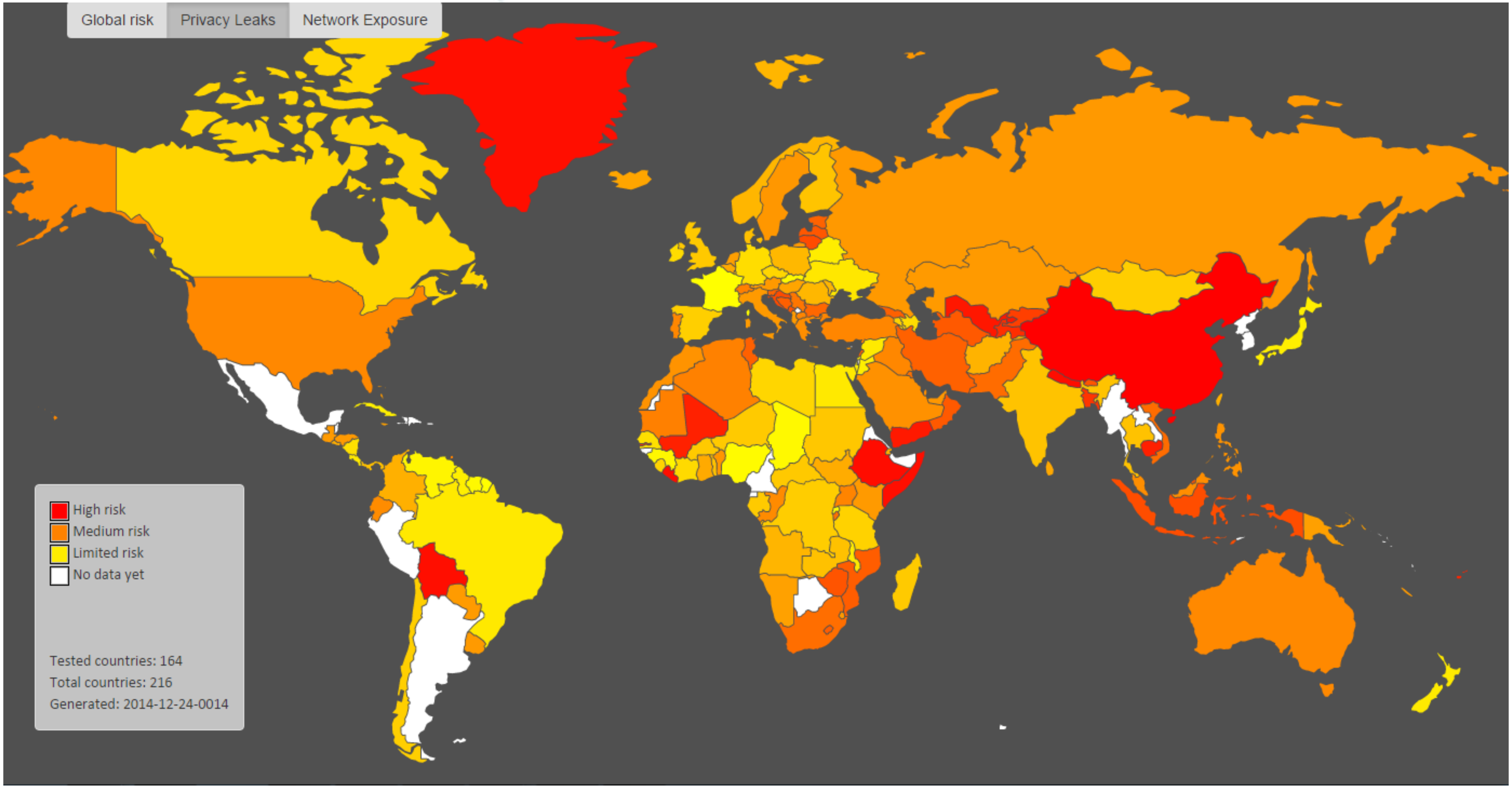
SS7 Map – Global Risk



🟥 High risk
🟧 Medium risk
🟨 Limited risk
□ No data yet

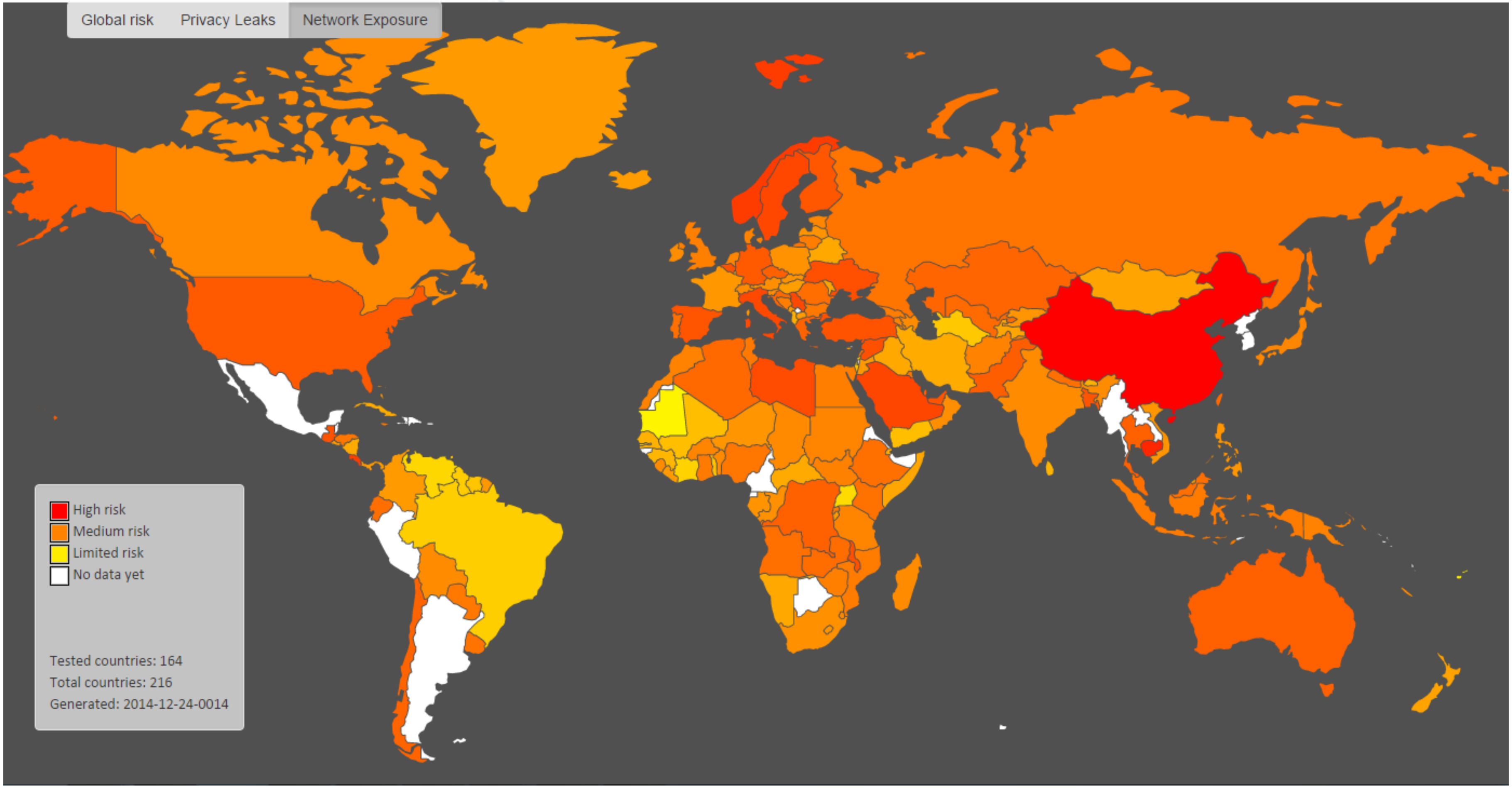
Tested countries: 164
Total countries: 216
Generated: 2014-12-24-0014

SS7 Map – Privacy Leaks



Tested countries: 164
Total countries: 216
Generated: 2014-12-24-0014

SS7 Map – Network Exposure



Tested countries: 164
Total countries: 216
Generated: 2014-12-24-0014

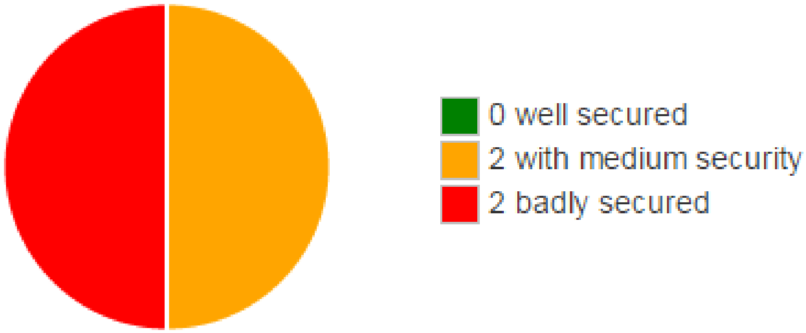
Country Ranking

Ranking	Country	Global Risk	Privacy Leaks	Network Exposure
1	Andorra	460.3	299	346.1
2	Suriname	554	299	721.1
3	Venezuela, Bolivarian Republic of	569.4	341.8	568.7
4	Luxembourg	573.9	314	725.5
5	France	577.2	237.7	1120.5
6	Guinea	620.3	325.4	854.4
7	Tonga	647.3	475.5	211.7
8	Rwanda	657.9	253.1	1366
9	Slovakia	666.7	299	1172
10	Cape Verde	670.2	427.7	542.3
11	Guyana	680.9	414	653.3
12	Chad	685.9	299	1248.4
13	Nigeria	701.4	275.9	1426
14	Israel	724.6	426.6	765.1
15	Brazil	751	472.8	640.3
98	Italy	2116.2	1326.9	1830.3
113	USA	2316	1518.5	1671.3

- Test on **small countries like Andorra, Suriname, Venezuela** has shown the **lowest global risk scores**.
- Country size of these nations makes easier the protection from the most part of security attacks on the network.
- Considering the **first «wide nation»** in terms of size and population**, France shows the best global risk score** during the test.
- **Italy** is only **98th in the ranking** with a global risk score of about 2.100.
- **Brazil is in a good position** (15th) behind Nigeria and Israel.

SS7 Security Level - Italy

Operators tested



4 surveyed operator / 5 operators

TIM

3

vodafone

WIND

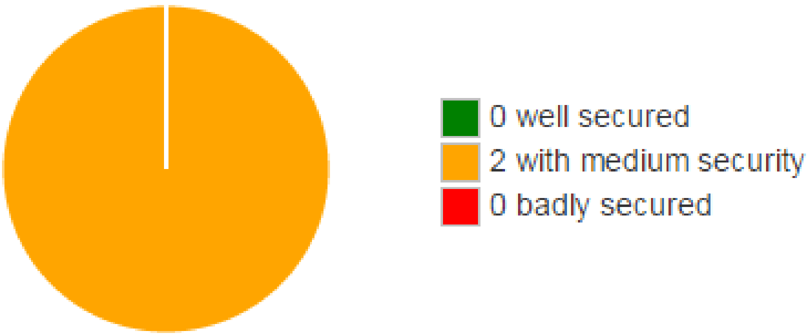
Global Risk	**98 / 164** 2.116,2
Privacy Leaks	**89 / 164** 1.326,9
Network Exposure	**158 / 164** 1.830,3

ELSACOM

No assigned frequency for this operator

SS7 Security Level - Brazil

Operators tested



2 surveyed operator / 4 operators

TIM

Claro

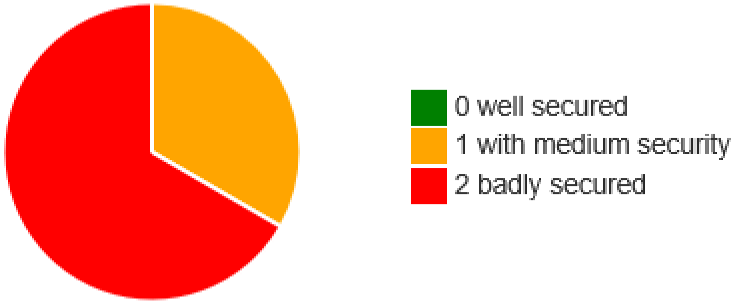
vivo

oi

Global Risk	**15 / 164** 751
Privacy Leaks	**21 / 164** 472,8
Network Exposure	**9 / 164** 640,3

SS7 Security Level - Switzerland

Operators tested



3 surveyed operator / 4 operators

swisscom

Sunrise

Salt Mobile SA

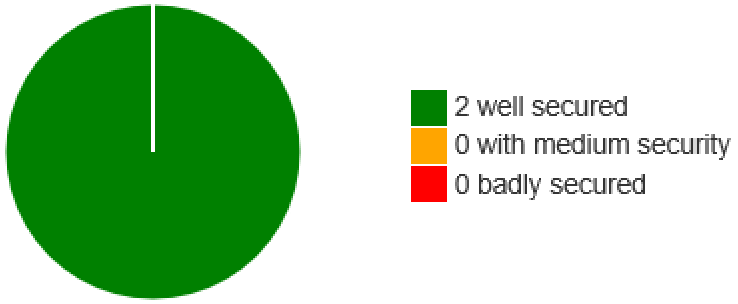
1956 2016
CCITT / ITU-T

Lycamobile
Call the world for less

Global Risk	114 / 164 2326,8
Privacy Leaks	116 / 164 1614,8
Network Exposure	83 / 164 1232

SS7 Security Level - Luxembourg

Operators tested



2 surveyed operator / 5 operators

POST LUXEMBOURG Group

tango

1956 2016 CCITT / ITU-T

orange

LOL LUXEMBOURG ONLINE

Global Risk	**4 / 164** 573,9
Privacy Leaks	**8 / 164** 314
Network Exposure	**14/ 164** 725,5

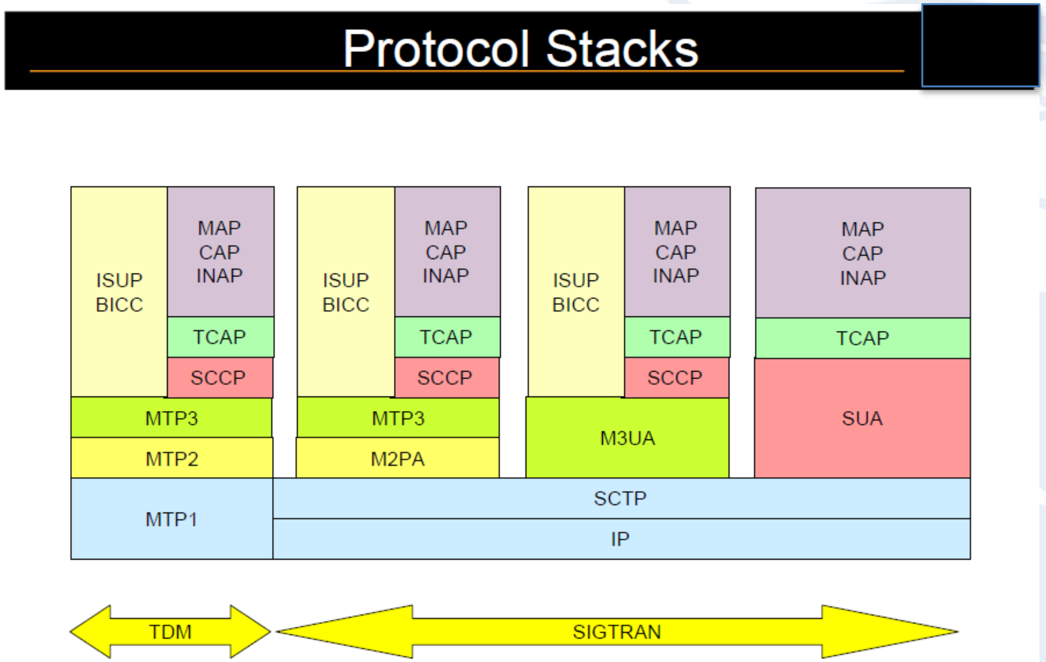
P1 Security SS7map actual

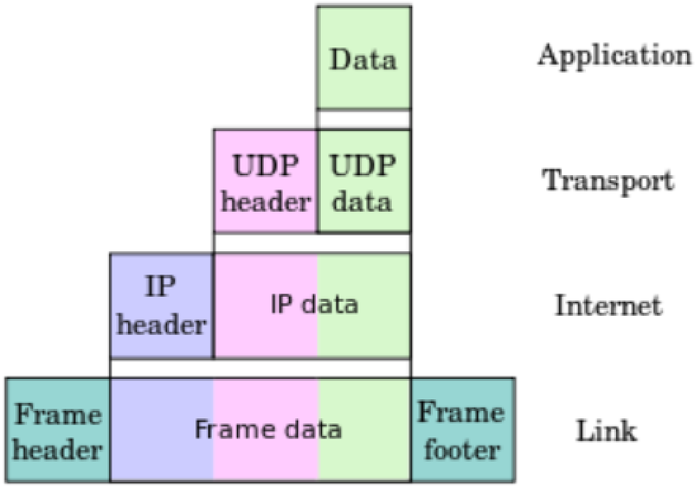
SS7map 164 Countries Tested: http://ss7map.p1sec.com

Luxembourg	**4:**	**http://ss7map.p1sec.com/country/Luxembourg/**
France	**5:**	**http://ss7map.p1sec.com/country/France/**
UK	**48:**	**http://ss7map.p1sec.com/country/United%20Kingdom/**
Poland	**59:**	**http://ss7map.p1sec.com/country/Poland/**
Norway	**69:**	**http://ss7map.p1sec.com/country/Norway/**
Italy	**98:**	**http://ss7map.p1sec.com/country/Italy/**
Portugal	**111:**	**http://ss7map.p1sec.com/country/Portugal/**
Switzerland	**114:**	**http://ss7map.p1sec.com/country/Switzerland/**
Turkey	**115:**	**http://ss7map.p1sec.com/country/Turkey/**
Slovenia	**124:**	**http://ss7map.p1sec.com/country/Slovenia/**

1956 2016
CCITT / ITU-T

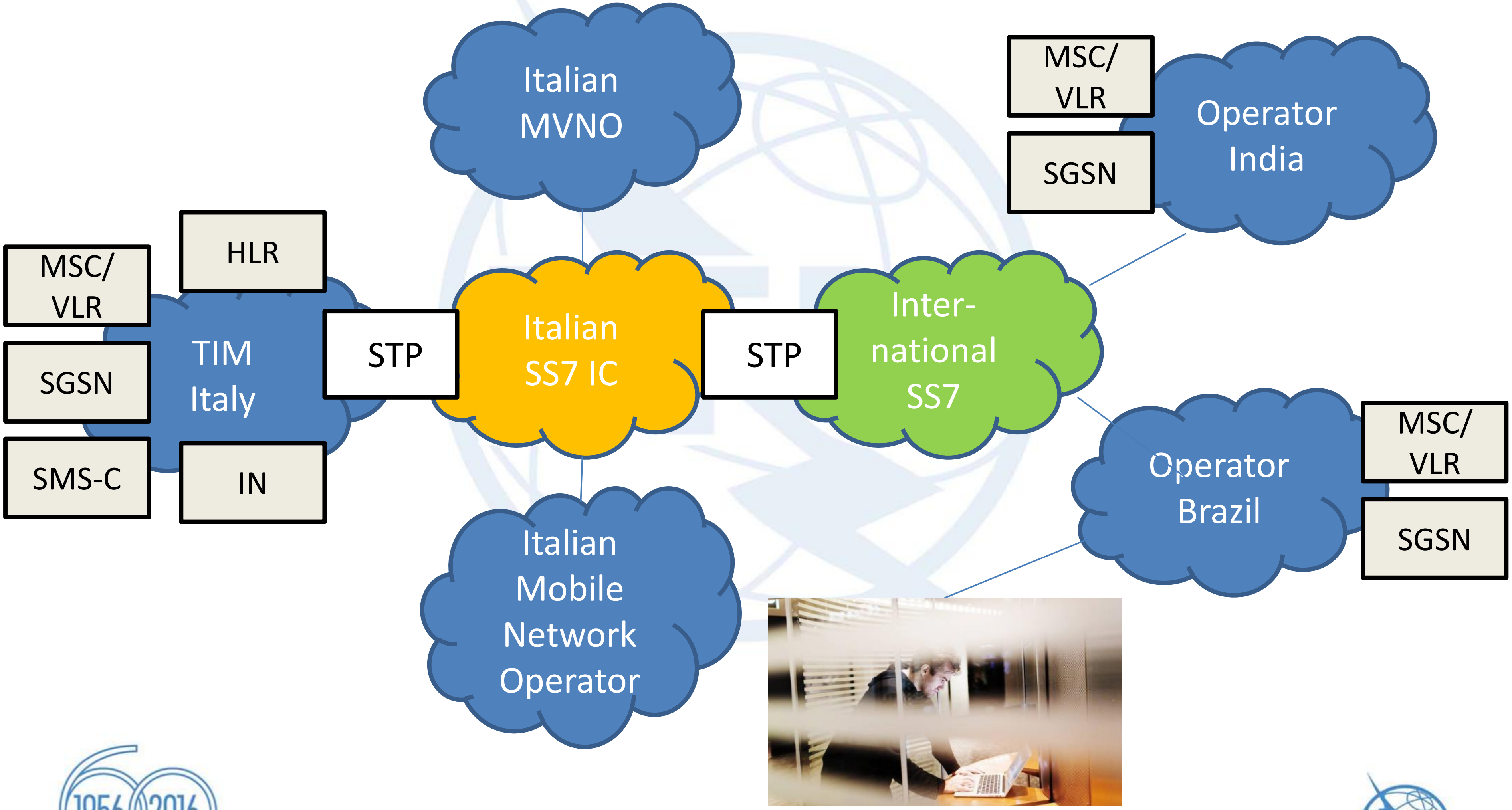
SS7 versus Internet





IMSI: 242 01 305 xxxxxxx	↔	Bank Account/ Visa Number
Global title: 47 9000 0950	↔	IP address: 87.238.54.132
Subsystem: 006 (HLR)	↔	Port number: 80 (http)

SS7 networks



Italian MVNO

MSC/ VLR

SGSN

Operator India

HLR

MSC/ VLR

SGSN

SMS-C

IN

TIM Italy

STP

Italian SS7 IC

STP

Inter-national SS7

Operator Brazil

MSC/ VLR

SGSN

Italian Mobile Network Operator

How P1 Security tested:

- P1 Security SS7map probes are located in the network of multiple operators using GT inside the range of the operators but not published in IR21

- Starting point for the attack is subscribers MSISDN collected from public open sources.

- The answer to the attack contains subscriber‘s individual information and network topology information (GT‘s)

MAP Mesage	Description	Input SCCP	Input MAP
SRISM	Send Routing Info for SM	MSISDN	MSISDN
ATI	Any Time Interrogation	MSISDN	MSISDN
SendIMSI	Send IMSI	MSISDN	MSISDN
SRI	Send Routing Info	MSISDN	MSISDN
PSI	Provide Subscriber Info	GT-VLR	IMSI
SAI	Send Authentication Info	MSISDN	IMSI
InterrogateSS	Interrogate Supplementary Services	MSISDN	IMSI

SCCP Example Request: Used GT Address format

```
********  SCCP (03/2001)
********    <General Fields>
********      Routing Label
********        Destination Point Code : DPC
********        Originating Point Code : OPC
0010----        Signalling Link Selection : 2
********    UNITDATA
********      Protocol class
----0001        Protocol class : 1
0000----        Message handling : 0 = no special options
********      Called Party Address
-------0        Point code indicator : 0h = address contains no signalling point code
------1-        SSN indicator : 1h = address contains a subsystem number
--0100--        Global title indicator : 4 = GT includes TT,NP,ES and NADI
-0------        Routing indicator : 0h = routing based on global title
0-------        Reserved for national use : 0h
00000110        Subsystem number : 6 = HLR
00000000        Translation type : 0 = unknown
----0010        Encoding scheme : 2 = BCD, even number of digits
0001----        Numbering plan : 1 = ISDN/telephony numbering plan (recommendation E.163 and E.164)
-0000100        Nature of address indicator : 4 = international number
********        Address information : MSISDN (or VLR for PSI)
********      Calling Party Address
-------0        Point code indicator : 0h = address contains no signalling point code
------1-        SSN indicator : 1h = address contains a subsystem number
--0100--        Global title indicator : 4 = GT includes TT,NP,ES and NADI
-0------        Routing indicator : 0h = routing based on global title
0-------        Reserved for national use : 0h
00000111        Subsystem number : 7 = VLR
00000000        Translation type : 0 = unknown
----0010        Encoding scheme : 2 = BCD, even number of digits
0001----        Numbering plan : 1 = ISDN/telephony numbering plan (recommendation E.163 and E.164
-0000100        Nature of address indicator : 4 = international number
********        Address information : xxxxxxxxxxxx
```

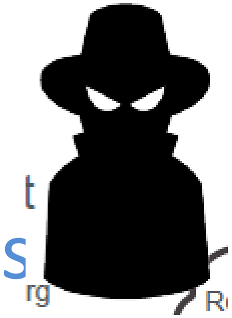
SCCP Example Response: Delivers GT of Operator

```
********  SCCP (03/2001)
********    <General Fields>
********      Routing Label
********        Destination Point Code : DPC
********        Originating Point Code : OPC
0000----        Signalling Link Selection : 0
********    UNITDATA
********      Protocol class
----0001        Protocol class : 1
1000----        Message handling : 8 = return message on error
********      Called Party Address
-------0        Point code indicator : 0h = address contains no signalling point code
------1-        SSN indicator : 1h = address contains a subsystem number
--0100--        Global title indicator : 4 = GT includes TT,NP,ES and NADI
-0------        Routing indicator : 0h = routing based on global title
0-------        Reserved for national use : 0h
00000111        Subsystem number : 7 = VLR
00000000        Translation type : 0 = unknown
----0010        Encoding scheme : 2 = BCD, even number of digits
0001----        Numbering plan : 1 = ISDN/telephony numbering plan (recommendation E.163 and E.164
-0000100        Nature of address indicator : 4 = international number
********        Address information : xxxxxxxxxxxx
********      Calling Party Address
-------0        Point code indicator : 0h = address contains no signalling point code
------1-        SSN indicator : 1h = address contains a subsystem number
--0100--        Global title indicator : 4 = GT includes TT,NP,ES and NADI
-0------        Routing indicator : 0h = routing based on global title
0-------        Reserved for national use : 0h
00000110        Subsystem number : 6 = HLR
00000000        Translation type : 0 = unknown
----0010        Encoding scheme : 2 = BCD, even number of digits
0001----        Numbering plan : 1 = ISDN/telephony numbering plan (recommendation E.163 and E.164
-0000100        Nature of address indicator : 4 = international number
********        Address information : VLR-GT
```

CCITT / ITU-T

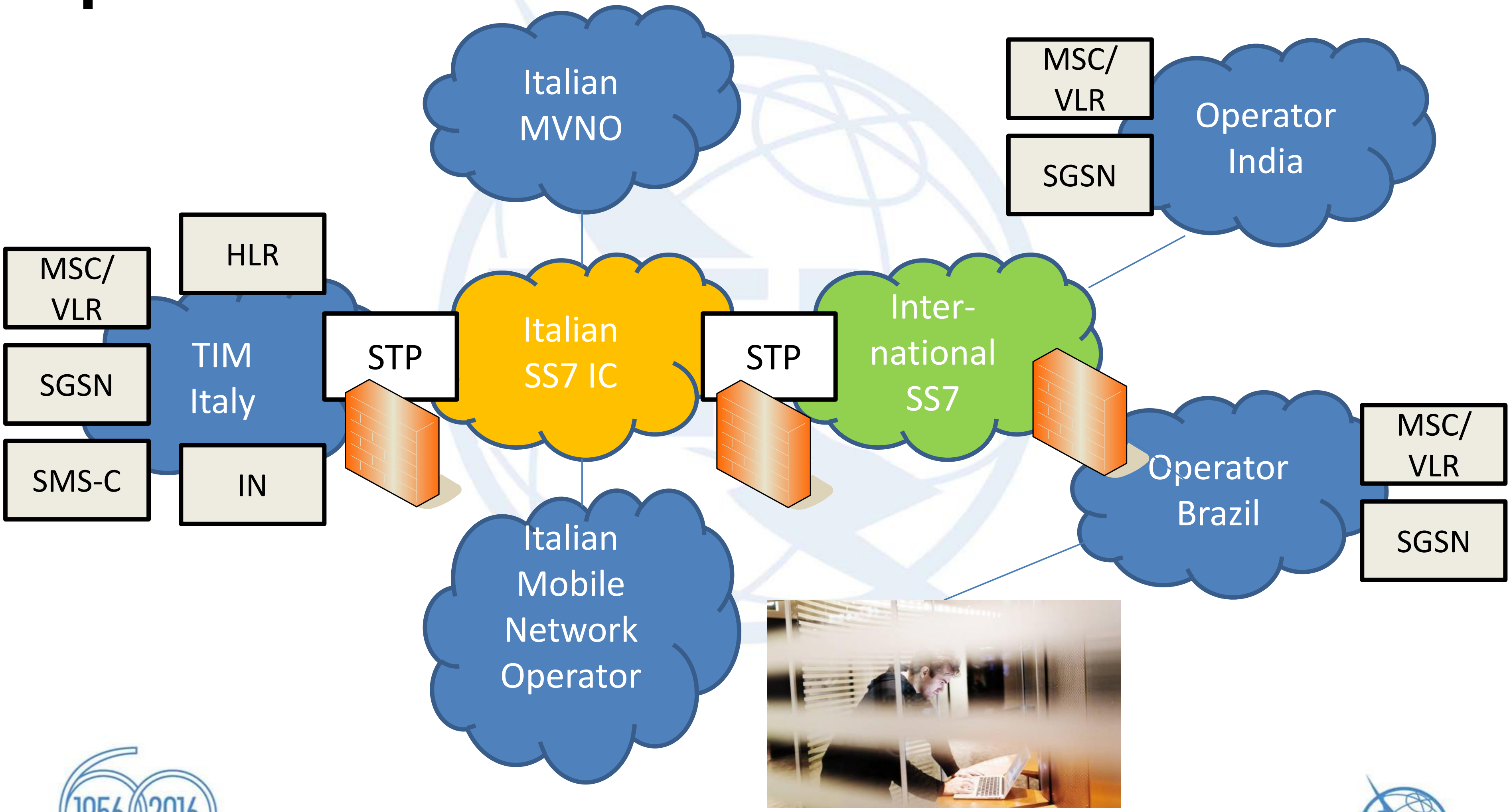
Standardization GAP

- MAP and SCCP Protocols are perfectly compliant to the SS7 standards
- It’s the way the protocols are used
- It’s the control of the authorised access



- New Functional elements are needed within SS7 architecture

SS7 networks – where to put the protection?



How to reduce Vulnerability

- Home Router hides real IMSI and VLR for SRISM
- All messages with MAP input MSISDN blocked
- → IMSI needs to be known to attack or track a specific subscriber

MAP Mesage	Description	Input SCCP	Input MAP
SRISM	Send Routing Info for SM	MSISDN	MSISDN
ATI	Any Time Interrogation	MSISDN	MSISDN
SendIMSI	Send IMSI	MSISDN	MSISDN
SRI	Send Routing Info	MSISDN	MSISDN
PSI	Provide Subscriber Info	GT-VLR	IMSI
SAI	Send Authentication Info	MSISDN	IMSI
InterrogateSS	Interrogate Supplementary Services	MSISDN	IMSI

Possible improvements (waiting for standardization)

- Blocking of unauthorized MAP operations on interconnect by using Message Screening on STP

- Introduction of Home Routing in SMSC Hide of Real-IMSI and VLR (SRISM)

Possible improvements (2)

Apply the following MAP Messages filtering - method silent reply:

MAP Message	GSMA List
Any Time Interrogation	YES
Send Routing Info	YES
Send IMSI	YES
Send Parameters	YES
Send Routing Info for GPRS	YES
Send Identification	YES
Any Time Subscriber Interrogation	YES
Any Time Modification	YES
Activate Trace Mode	NO
Register Password	NO
Get Password	NO
MAP check IMEI	NO
MAP Restore Data	NO
Provide Subscriber Location	NO
Send Routing Info for LCS	NO

Possible improvements (3)

- Dummy Cell for PSI
  If a PSI MAPv3 message is received in MSC/VLR from an external HLR either for a HPLMN subscriber or an inbound roamer, then the Cell Identity and/or the last 5 digits of the Location Number associated to a cell, if provided, will be replaced by value “00001”.
- Block PSI to own IMSI from external HLR
  Block PSI with IMSI MCCMNC* coming from external HLR. Gateway MSC is not an option as filtering on IMSI is not possible

Closing Remarks

- SS7 Security issues have been well identified
- Issues are not in the protocol itself but on how the protocols are used
- Standardidazione could deal with
  - SS7 Firewall
  - SS7 Routers
- Whitelist –SRISM SMS that can be received from non roaming partner, is there a realiable Service available to maintain the trusted GT‘s of SMSC worldwide
- Blocking functionality without block the service… PSI?!

1956 2016
CCITT / ITU-T

Closing Remarks (1)

- Remove all necessities to hand out a subscriber’s IMSI and current VLR/MSC to other Networks
- Home routing can be a good option for SMS,
- when SRISM is received it will be returned the address of SMS router and not MSC address
- Instead of subscriber IMSI only a correlation id will be returned that will be solved by SMS Router
- All MAP and CAP messages only needed in the network should be filtered at the network border
- What about diameter….?

It’s even worse….

But this is another story…

ITU

1956 2016

CCITT / ITU-T