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

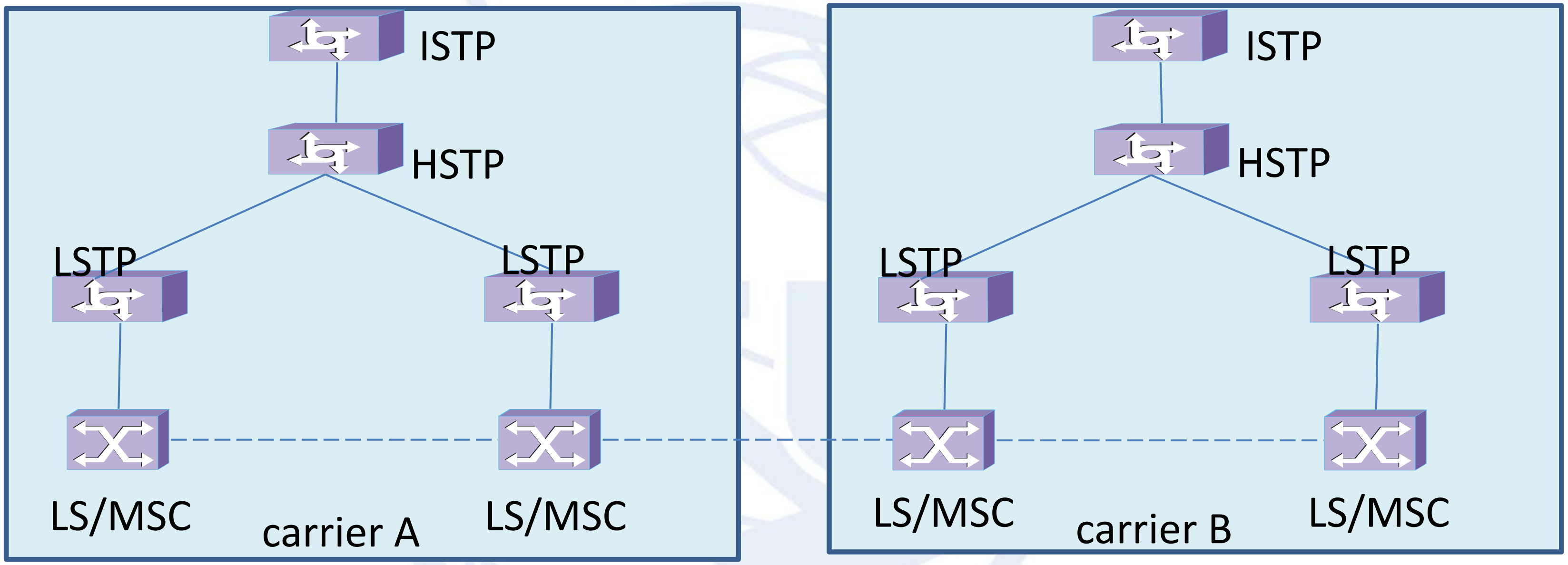
Alternative Solutions for the improvement of SS7 security

Minrui Shi
China Telecom
shimr@sttri.com.cn

Content

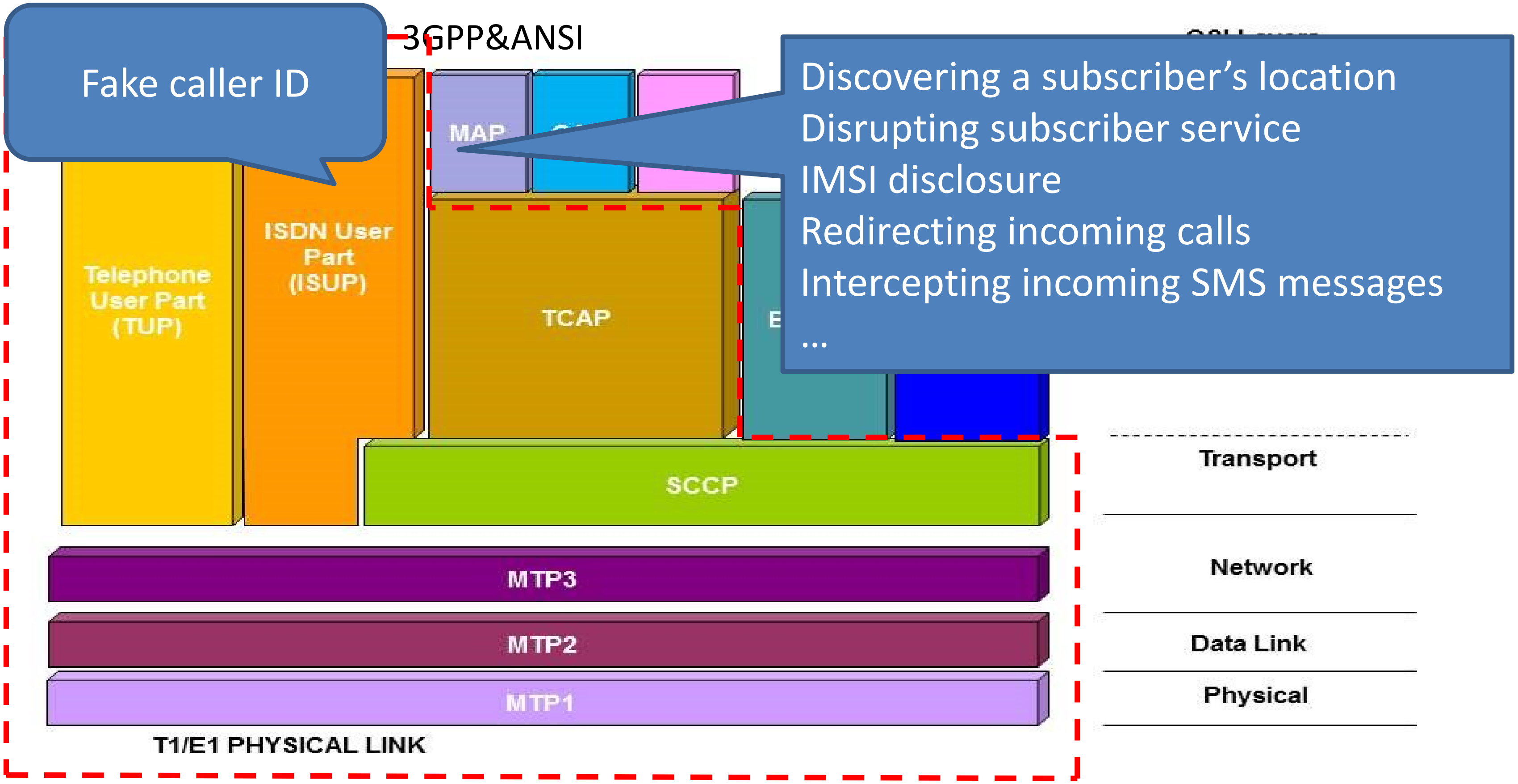
- Overview
- Security issues of ISUP and solutions
- Security issues of MAP and solutions
- Suggestion and conclusion

Signaling architecture



	China Mobile	China Telecom	China Unicom
Mobile	826.2M	197.9M	286.6M
3G/4G	481.7M	143.1M	183.8M
PTSN line		134.3M	73.8M
SPs	>3000	>5500	>3000

Protocol stack



Fake caller ID

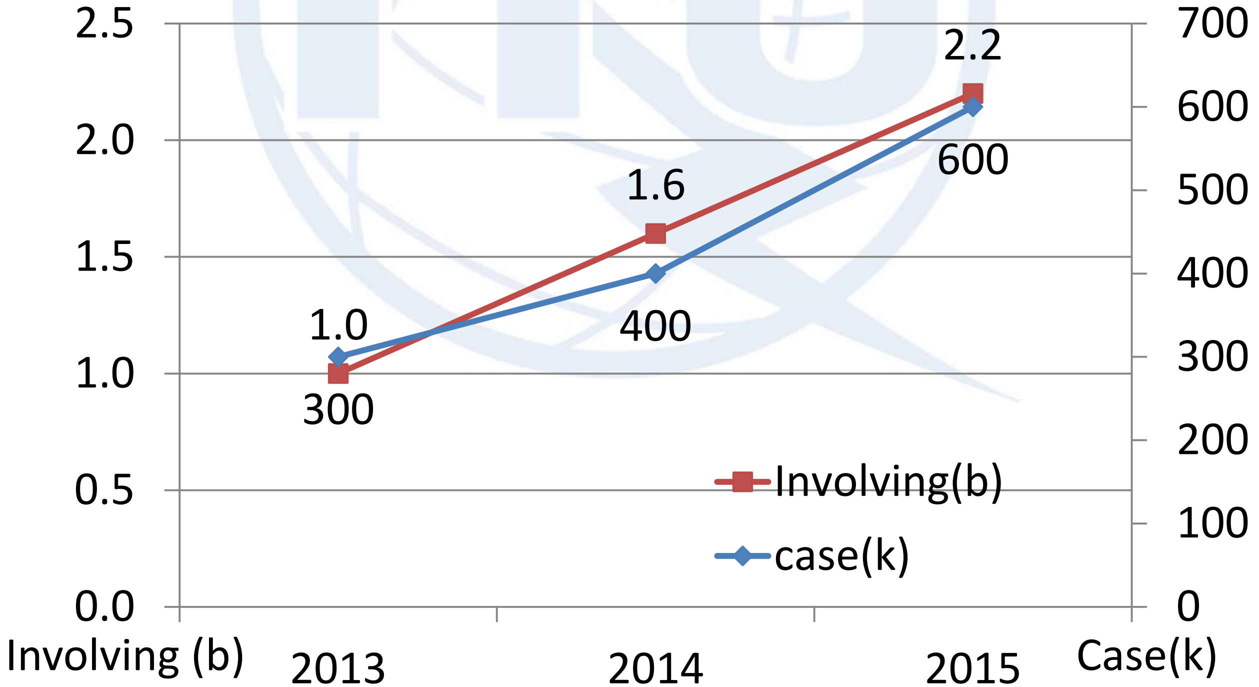
Discovering a subscriber’s location
Disrupting subscriber service
IMSI disclosure
Redirecting incoming calls
Intercepting incoming SMS messages
…

Content

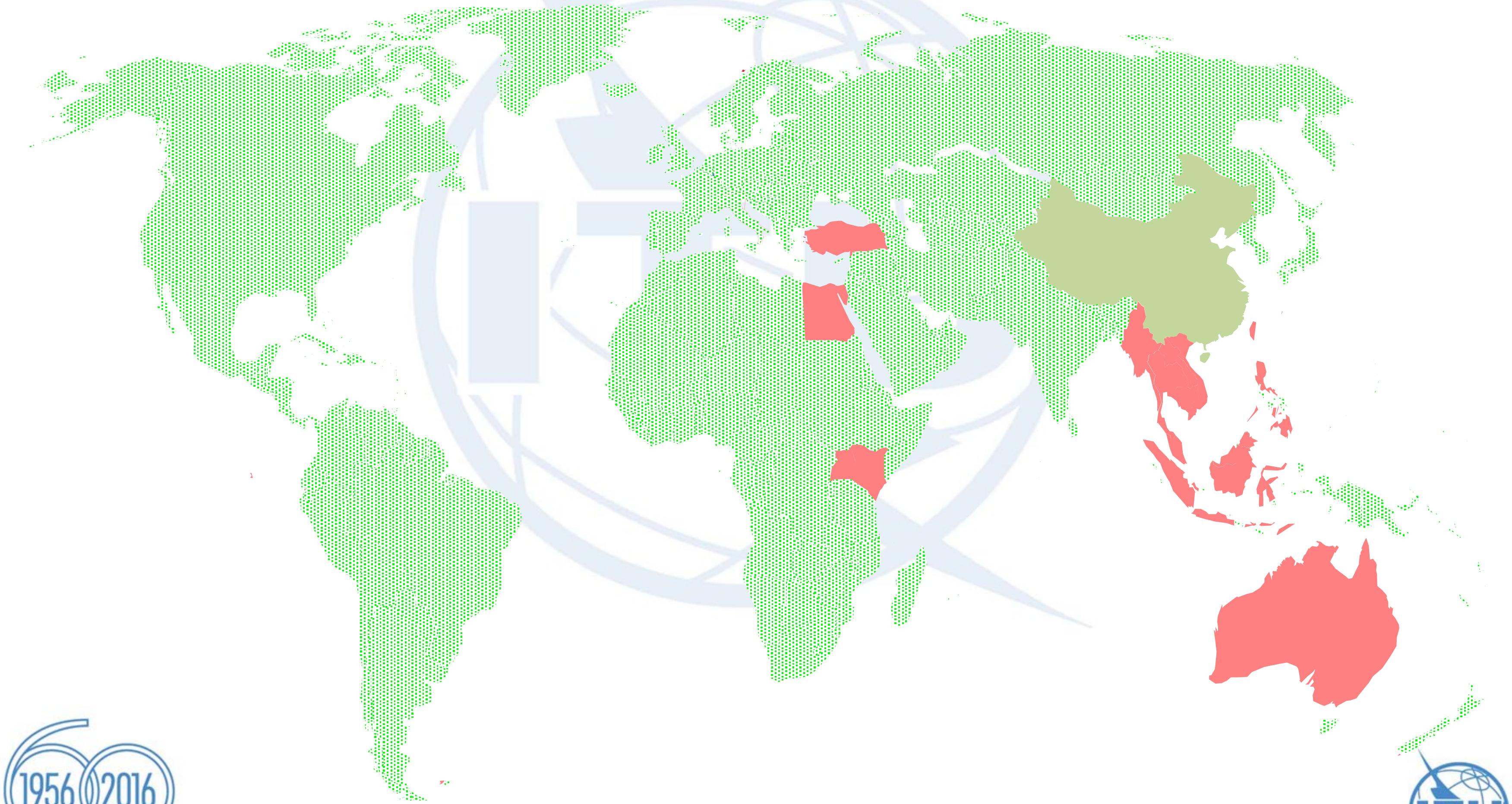
- Overview
- Security issues of ISUP and solutions
- Security issues of MAP and solutions
- Suggestion and conclusion

Prevalent fraud in China

- Criminals pose as government or cooperators staffs and call victim with a calling number which is registered by government or cooperators .
- Criminals fabricate a variety of reasons, such as tax rebates, money-laundering
- Trick the victim transfer money to the special account



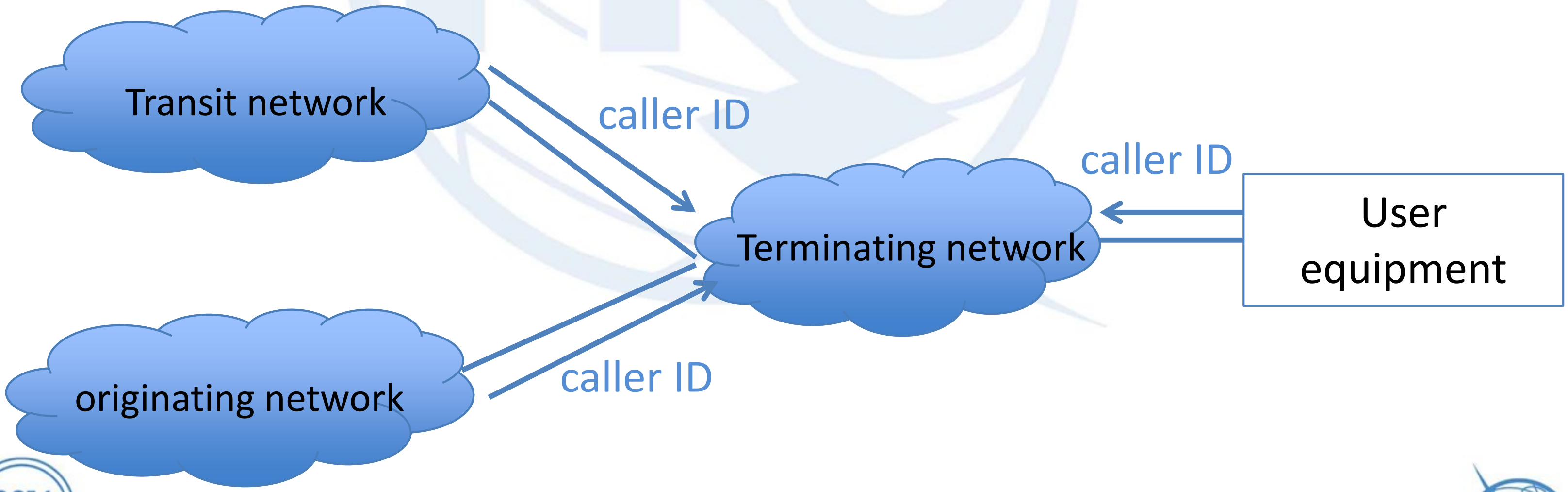
Where are the cheat calls coming from



CCITT / ITU-T

Main security issues of ISUP

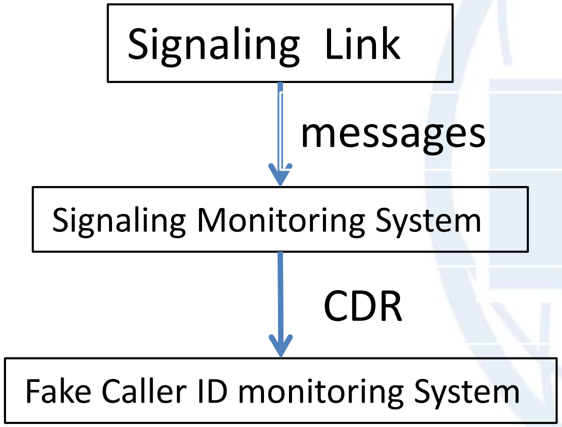
- A caller sends any caller ID by setup parameter CallingPartyNumber or GenericNumber without authentication and authorization for an outgoing call via ISUP.
- ISUP do not contain any caller ID verification mechanisms
- The carrier of the terminating network can only simply accept and forward the claimed caller IDs due to complex network structure and services.



Solution Alternatives

- Authenticating calls from users even if connect with SS7
- Monitoring incoming calls from interconnect carriers
  - signaling monitoring and analysis
    - Call duration is very short
    - Number of call attempt is large
  - Analysis behavior of called party： detect dual tone. Fraud calls often play a short voice message which indicate the recipient press “button” to transfer call to manual service.
- Call interrupting according to the black or white list
  - incoming international calls which caller ID "+86“ and special numbers (such as emergency, call center.)will be interrupted according black list.
  - Other Caller IDs in the black list

Call monitoring architecture and procedure



Signaling Link

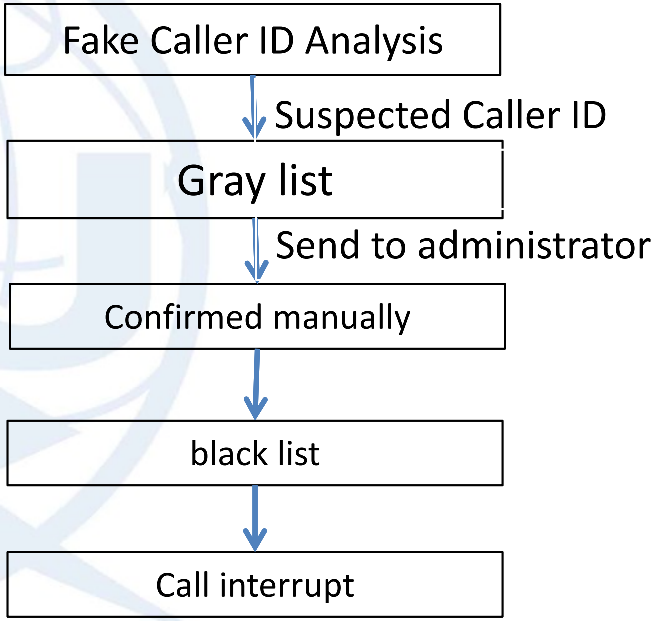
messages

Signaling Monitoring System

CDR

Fake Caller ID monitoring System

Monitoring architecture



Fake Caller ID Analysis

Suspected Caller ID

Gray list

Send to administrator

Confirmed manually

black list

Call interrupt

Call interrupt procedure

Content

- Overview
- Security issues of ISUP and solutions
- Security issues of MAP and solutions
- Suggestion and conclusion

Main security issues of PLMN

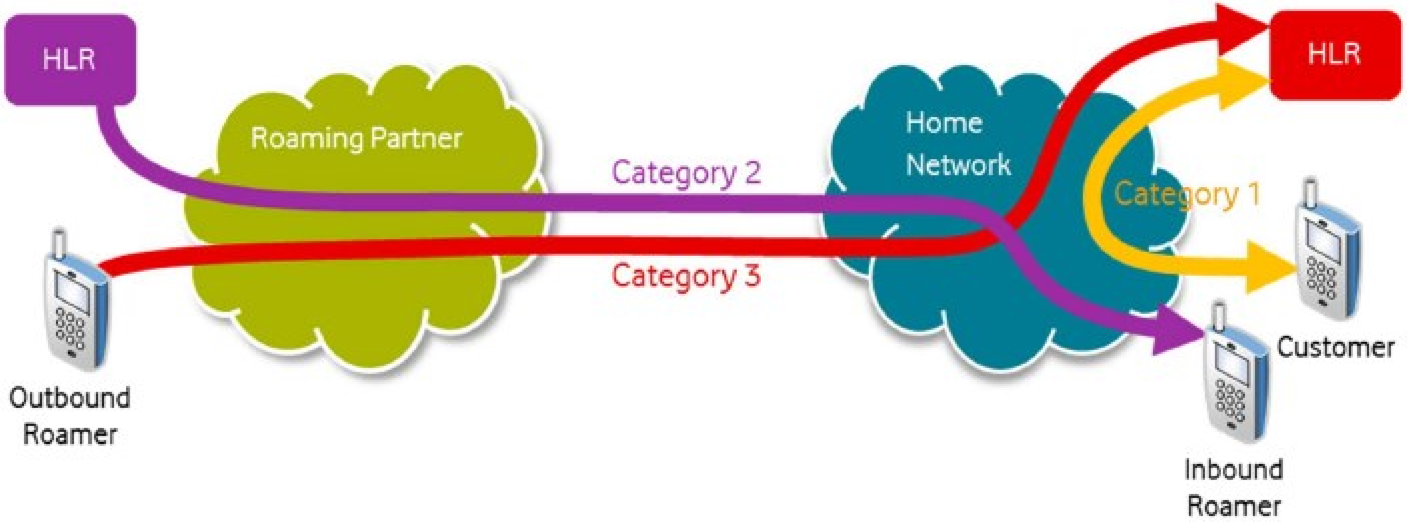
- MAP do not contain any verification mechanisms
- Encryption mechanism is not used in MAP
- Some MAP messages are used maliciously
- SPs connect each other via SS7 network in order to support mobile services

CCITT / ITU-T

Classifications in IR.82

GSMA IR.82 Security SS7 implementation on SS7 network guidelines v3.0

- **Threats have been classified by GSMA to 3 main categories:**
  - **Category 1 : Intra-PLMN (**Messages should only be received from within the same network **)**
  - **Category 2 : Inter-PLMN (**Messages should only be received from subscriber’s home network**)**
  - **Category 3: Inter-PLMN (**Messages Should only be received from subscriber’s visited network)
  - Category 4 (SMS)
  - **Category 5 (CAP)**



Filtering features implement

Features	HLR	SMSC	MSC/SGSN	STP	SS7 firewall
MAP Screening (Op, CgGT)	X		X	X	X
MAP Screening (Op, CgGT, IMSI)	X		X	X	X
Compare current VLR and Cg SCCP	X	X			X
Compare IMSI and HLR			X		X
Compare IMSI and SCP			X		X
SMS Home Routing	X	X			X
Check Location	X				X
Check CgGT spoofing				X	

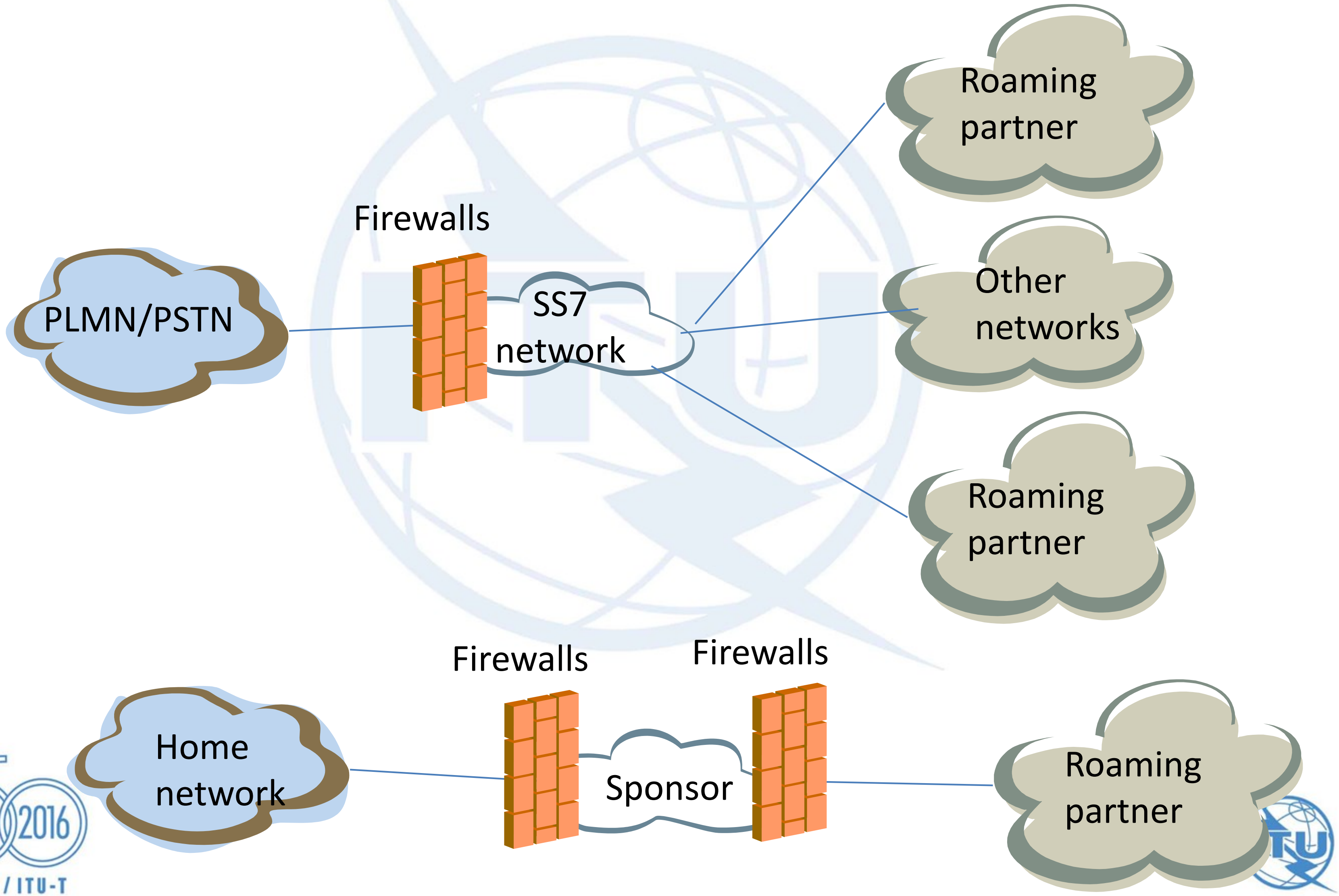
From： GSMA IR.82

Solution Alternatives

	Passive Monitoring Only	Active Filtering		
		Inside Network	Network Edge	
		Upgrade Existing MSCs and HLRs	Upgrade edge STPs (or gateway MSCs)	New Dedicated Element
Changes to network/signaling architecture	○ None	○ None	○ None	◔ Limited
Impact on other network elements	○ None	◕ Multiple	◔ Limited	◔ Limited
Initial Cost	◔ Low	◕ High	◑ Moderate	◑ Moderate
Cost of operating and maintaining solution	◔ Low	◕ High	◑ Moderate	◔ Low
Visibility of signaling	◕ Good	◔ Fragmented	◑ Moderate	◕ Good
Ease of implementation of filter rules	N/A	◔ Complex	◑ Moderate	◕ Good
Filtering capabilities	N/A	◑ Moderate	◑ Moderate	◕ Good
Network protection	N/A	◔ Limited	◑ Moderate	◕ Good
	Lacks active filtering so provides no protection. Protection requires further investment – so ultimately more expensive.	Distributed solution adds complexity and cost. Only protects interactions with some elements	STPs not designed for the task. Stateful (interactive) rules difficult (slow and costly) to support	Introduces a new element at the most beneficial location. Designed for signaling protection and monitoring

From： Securing the vulnerabilities exposed in SS7-XURA

Signaling firewalls implement



Other GSMA Recommendations

- FS.07 SS7 and SIGTRAN Network Security
- FS.11 SS7 Interconnect Security Monitoring Guidelines
- IR.82
- IR.71 SMS SS7 Fraud Prevention v5.0
- IR.70 SMS SS7 Fraud v4.0

Content

- Overview
- Security issues of ISUP and solutions
- Security issues of MAP and solutions
- Suggestion and conclusion

Actions for carrier

- introduce authentication and authorization in the SS7 access point connect with user
- Initiate monitoring first at the edge of network or external scanning with potential attack messages
  - identify characteristics of SS7 attacks
  - Address weakness of the network
- enhanced security
  - Block calls with illegal caller ID, messages of non-roaming-partners and messages from CAT 1(IR.82)
  - Introduce more complex filter features(CAT 2&3)
- Long term
  - Consistency analysis and block new attacks

Challenges to ISUP

- Caller ID is complex and changing all the time
- Users have the right to communicate freely, carrier has no right to interrupt calls.
  - Legal or illegal usually are hard to be identified
  - Interrupting calls should be confirmed by the administrator
  - Carriers can only give alert to mobile phone with SMS or USSD by data analysis
  - Lack of warning method for fixed line

Violation may has resulted before the call interruption

Challenges to MAP

- Protect outbound customers dependent on roaming partners.
- Guidelines for CDMA carriers(ANSI MAP and WIN) are required
- Some status related filter features will be difficult to implement in SG firewalls and expensive implemented by SPs
- Diameter and SIP has similar vulnerabilities as SS7 and is coming now

conclusion

- It is hard to implement enhanced protocols.
- Parameters related to caller ID should be defined detail in international calls in order to reduce transmitting fake caller ID.
- Initiate monitoring and filtering should be done immediately
- Carrier should detail analyzed SS7 vulnerabilities to reduce SS7 risks and attacks
- Diameter security should be moved forward

Thank you for your attention

1956 2016

CCITT / ITU-T