Preventing SS7 Based Attacks Using TCAP Security

10th Annual Signalling Systems for Future Telecoms Forum, 28 January 2009

Umut Ersoy

Signalling Senior Manager

Vodafone Teknoloji, Turkey

vodafone

Contents

- Overview of Potential Vulnerabilities of GSM and SS7
  - GSM Network and Security
  - SS7 and Security
  - SS7 based security Threats
- TCAP Handshaking
  - Overview
  - For MT SMS
  - For MO SMS

Contents

- TCAPsec
  - Overview
  - Network Architecture
  - SS7 Security Gateway (SS7-SEG)
  - Security Association
  - Structure of a Protected TCAP Message
- Enabling Security on Real Life Applications
  - Sending SM to invalid network nodes
  - Basic spam filtering in the SMSC
  - Hatihati prevention
  - MO Spoofing solutions
  - SMS Firewall / MT SMSR

Overview

- Security – always a major topic in communications
- Important for customers
  - Pay for someone else
  - False identity
  - Stolen private information
- Important for regulatory bodies
  - Rights of customers
- Important for vendors
  - Product stability
- Especially important for operators
  - Customer dissatisfaction
  - Service Outage
  - Losing revenue
  - Penalties

Overview – GSM Network and Security

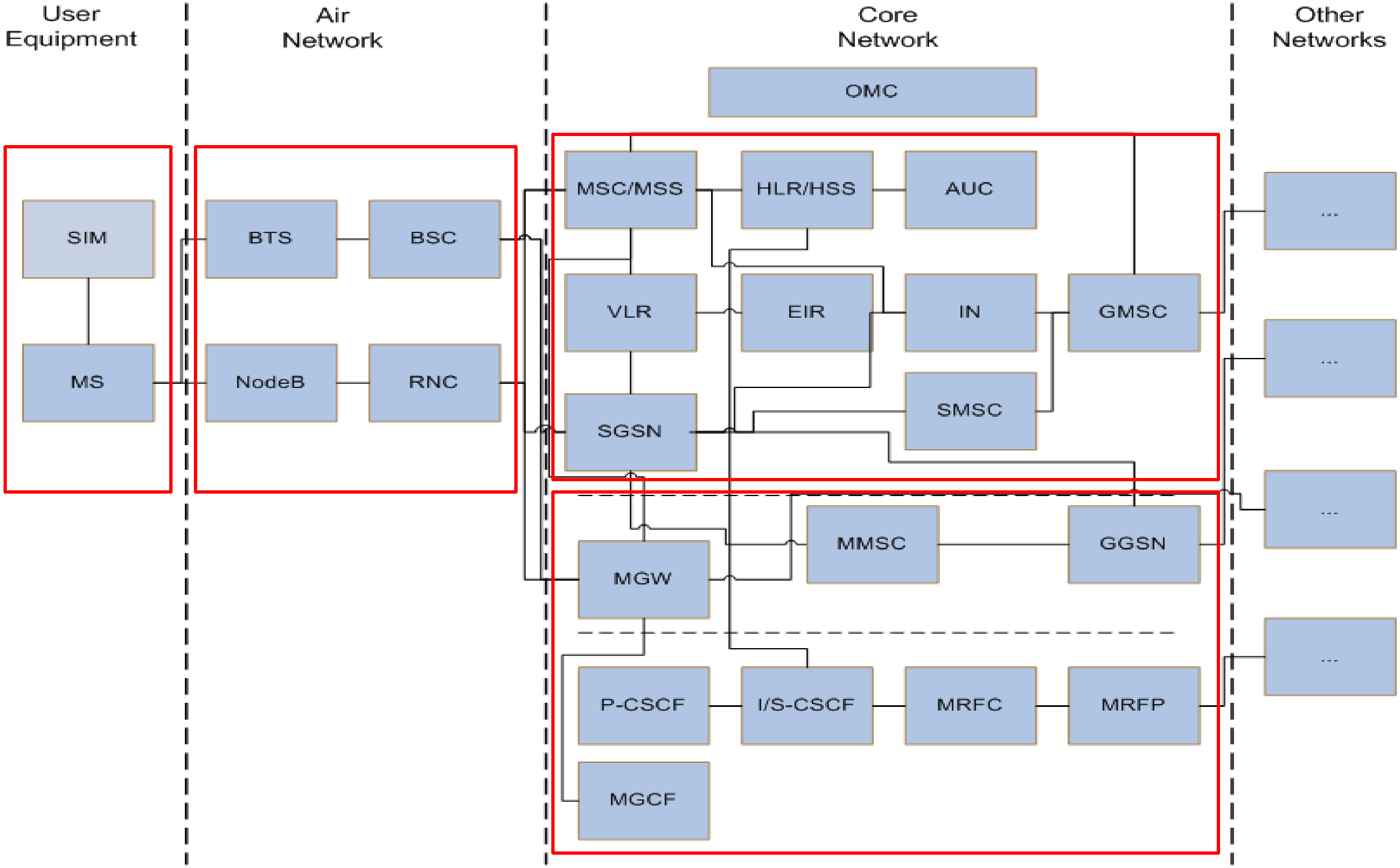
3GPP is standardizing more and more measures to increase security of the GSM in every new GSM release. Some examples:

- Release 99
  - TS 33.102 3G security; Security architecture
  - TS 35.202 Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification
- Release 4
  - TS 33.200 3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security
  - TS 35.206 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification

Overview – GSM Network and Security

- Release 5
  - TS 33.203 3G security; Access security for IP-based services
  - TS 33.210 3G security; Network Domain Security (NDS); IP network layer security
- Release 6
  - TS 33.310 Network Domain Security (NDS); Authentication Framework (AF)
  - TS 33.234 3G security; Wireless Local Area Network (WLAN) interworking security
- Release 7
  - **TS 33.204 3G Security; Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) user security**
  - **TS 29.204 Signalling System No. 7 (SS7) security gateway; Architecture, functional description and protocol details**
- Release 8
  - TS 33.401 3GPP System Architecture Evolution (SAE); Security architecture

Overview – GSM Network and Security



Overview – SS7 and Security

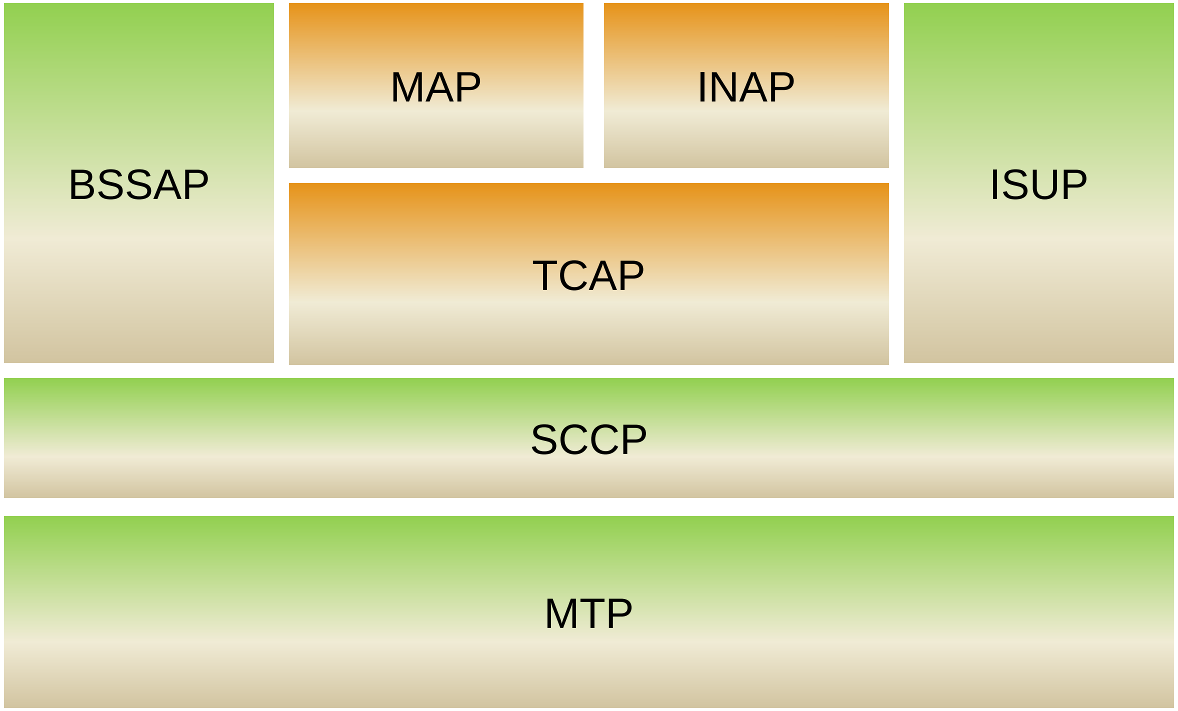
Absence of security in SS7 is identified as a weakness, but not seen as a problem.

- Existing trust relationships amongst Telcos,
- Closed networks,
- Only experts are working and monitoring networks.

Today networks are changing and protection for SS7 is becoming a necessity.

- The opening of the network for various (smaller) interconnect parties and service providers,
- IP access to SS7 networks,
- Less experts available to monitor networks,
- More SMS service providers connecting to network, increasing the possibilty of sending wrong messages without any purpose or trying to abuse the network.

Overview – SS7 and Security



- TCAP and protocols based on TCAP are more vulnerable to fraud.
  - – Don’t need end to end physical connections
  - – Used in inter-PLMN communications

Overview – SS7 based Security Threats - Spoofing

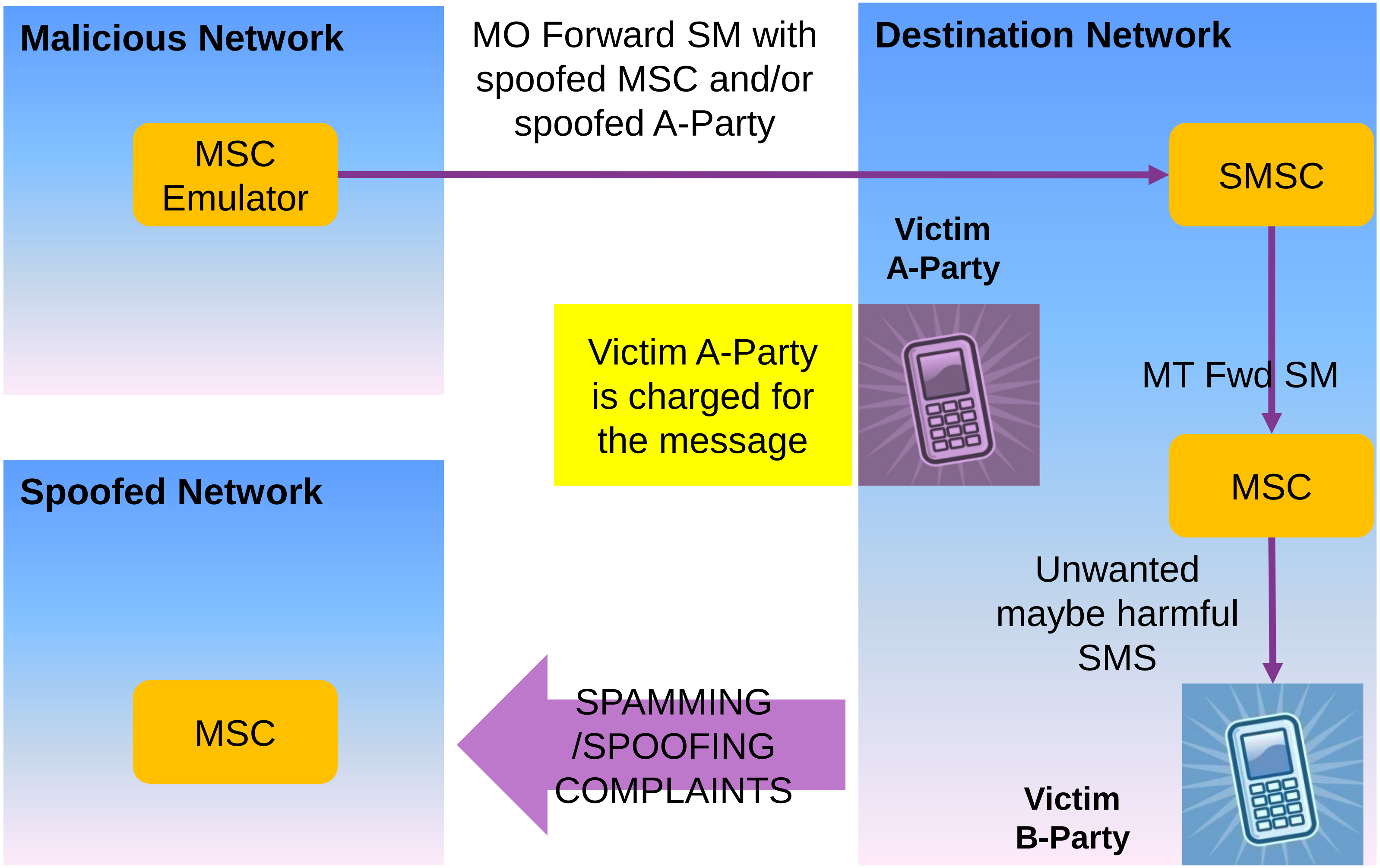
Definition:

- Illegal use of HPLMN SMSC by a 3rd party.
- An MO SMS with a manipulated A-MSISDN (real or wrong) is coming into the HPLMN network from a foreign VLR (real or wrong SCCP Address).
- If the billing is made from the SMS-C data, the real subscriber will be invoiced.

Precaution:

- HPLMN can check the originator MSISDN (to verify if it's a real or not).
- HPLMN can check if the VLR location stored in the HLR is in the same range with the requesting SCCP address.

Overview – SS7 based Security Threats - Spoofing



Malicious Network
MSC Emulator
MO Forward SM with spoofed MSC and/or spoofed A-Party
Destination Network
SMSC
Victim A-Party
Victim A-Party is charged for the message
MT Fwd SM
MSC
Spoofed Network
MSC
Unwanted maybe harmful SMS
SPAMMING /SPOOFING COMPLAINTS
Victim B-Party

Overview – SS7 based Security Threats - Faking

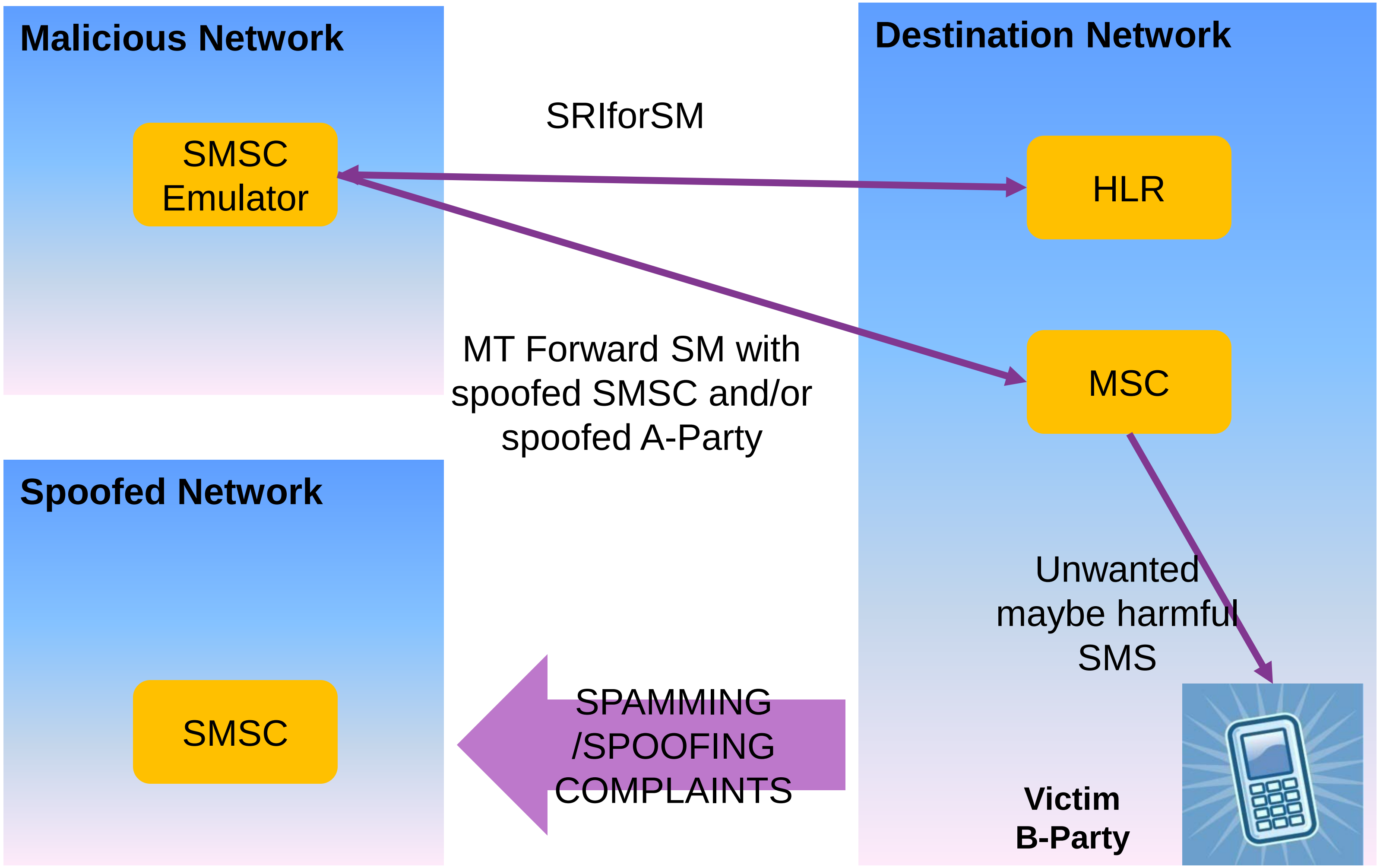
Definition:

- Also known as MT spoofing.
- A fake SMS is originated from the international SS7 network.
- SCCP/MAP addresses are manipulated.
- SCCP/MAP addresses are wrong or copied from a real existing SMSC.
- SMS can be sent to a real subscriber (recovering IMSI) or to a wrong IMSI (only to generate traffic).

Precaution:

- Controlling access to the SS7 network,
- Supervision of foreign SMSC traffic.

Overview – SS7 based Security Threats - Faking



Malicious Network

SMSC Emulator

SRIforSM

Destination Network

HLR

MT Forward SM with spoofed SMSC and/or spoofed A-Party

MSC

Spoofed Network

SMSC

Unwanted maybe harmful SMS

SPAMMING /SPOOFING COMPLAINTS

Victim B-Party

Overview – SS7 based Security Threats - Spamming

Definition:

- Subscriber receives unwanted SMS.
- Sender can be valid.
- SMS can be billed correctly.
- SMS is submitted by a mobile phone or by a third party connected to the SMSC.
- Only real detection method is customer complaints.

Precaution:

- Repetitive content check,
- SMS Firewall / MT SMS Router.

Overview – SS7 based Security Threats - Others

Flooding

Definition:

- Massive load of messages to one or more destinations.
- The only parameter is the number of messages sent.
- May cause DoS.

Precaution:

- Supervision of traffic.

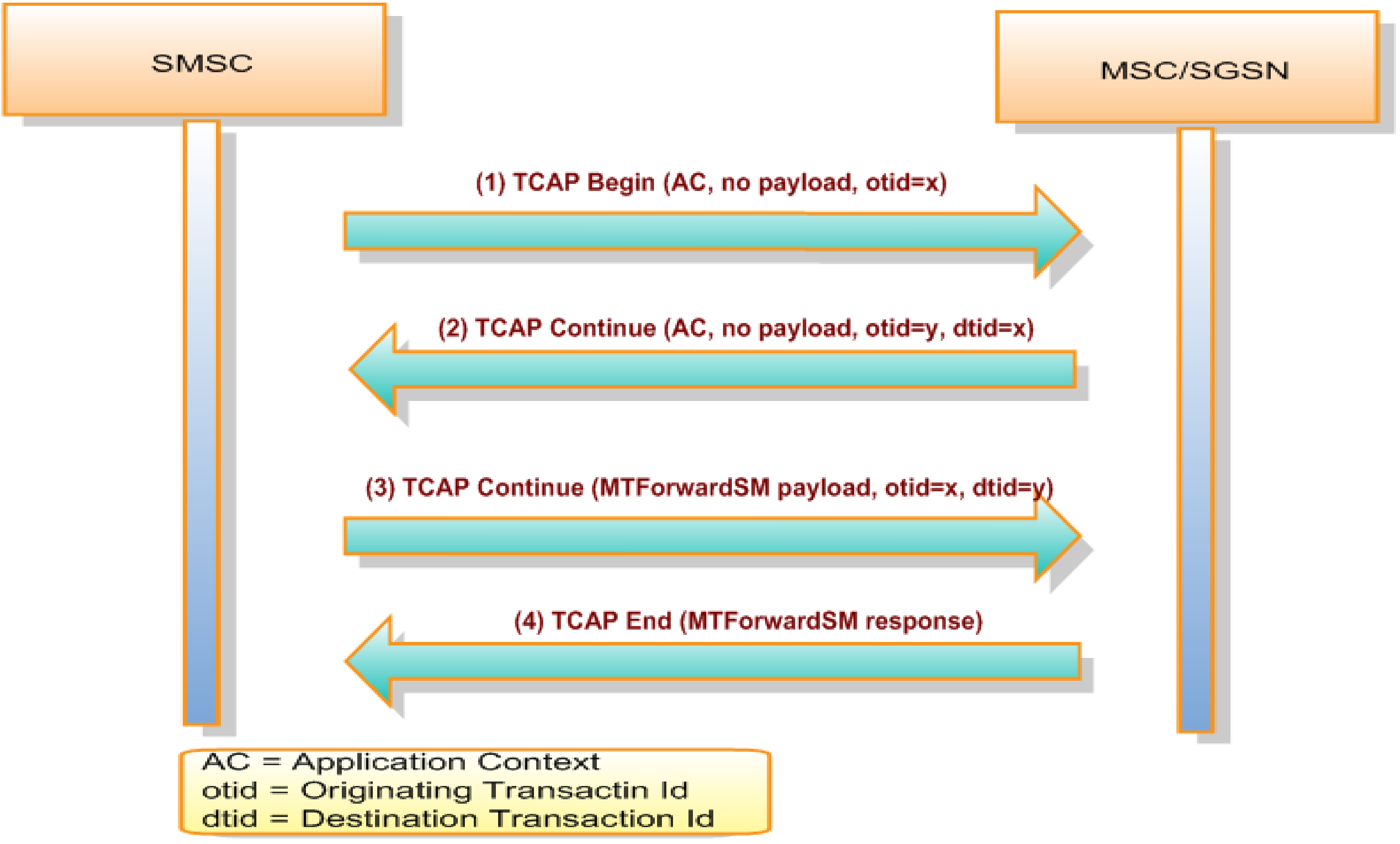
Mobile Viruses

- e.g. Hatihati
- Unwanted signaling
- Stolen private information

TCAP Handshaking - Overview

- Defined in **3GPP TS 33.204** 3G Security; Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) user security (Release 7) as an Annex (a short/medium term solution).
- To be used for **SMS transfers.**
- A limited level of authenticity is provided.
- Prevents spamming and spoofing for MO and MT SMS transfer cases.
- MSC/SGSN and SMSC behaviors should be modified.
- Based on using special transaction sequences.

TCAP Handshaking – MT SMS


SMSC
MSC/SGSN
(1) TCAP Begin (AC, no payload, otid=x)
(2) TCAP Continue (AC, no payload, otid=y, dtid=x)
(3) TCAP Continue (MTForwardSM payload, otid=x, dtid=y)
(4) TCAP End (MTForwardSM response)

AC = Application Context
otid = Originating Transactin Id
dtid = Destination Transaction Id

Sending MT ForwardSM with TCAP Handshaking

TCAP Handshaking – MT SMS

1. Receiving node should verify whether received SMSC address (contained in SM-RP-OA field in the 3rd message) is in the same operators range with the SCCP Calling Party address of the 1st message.

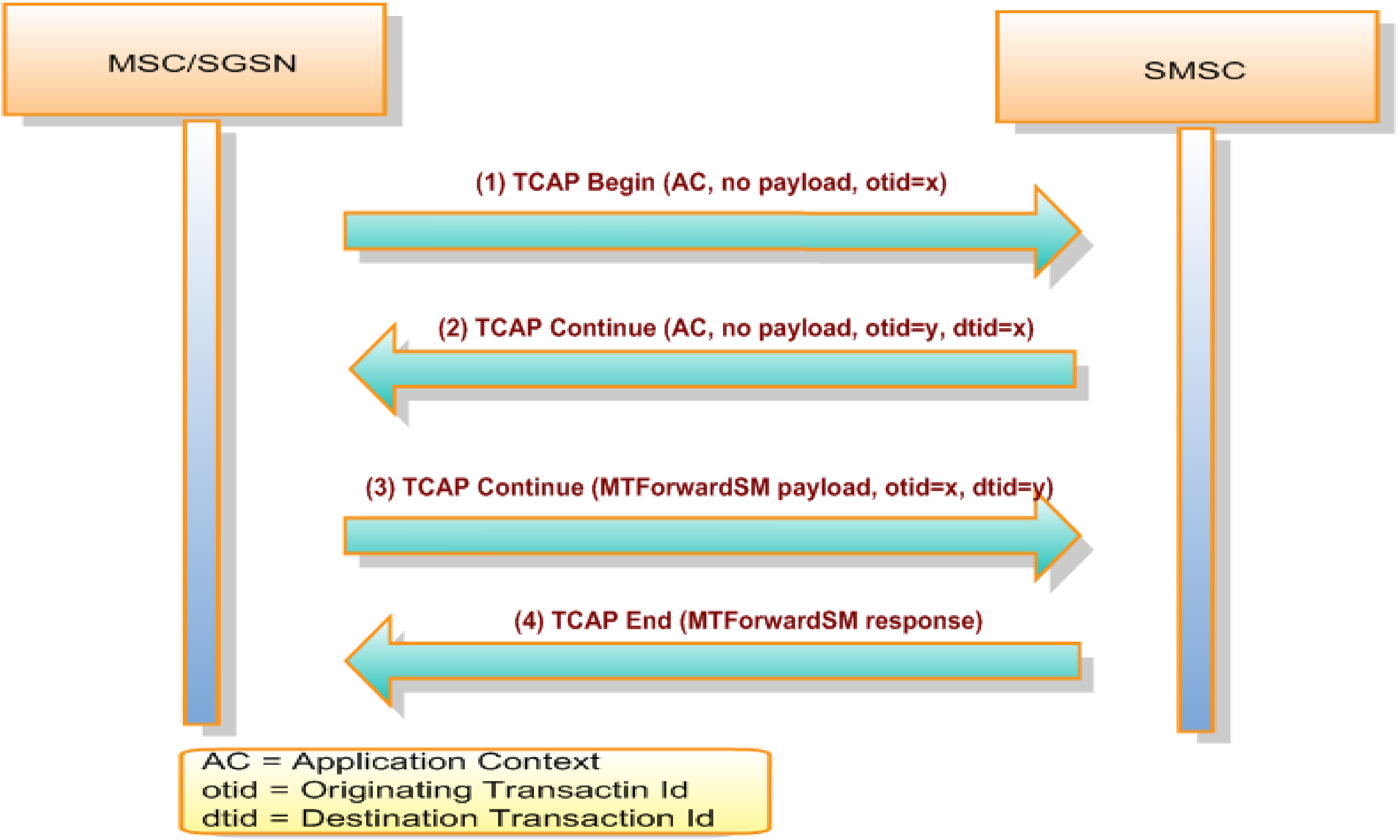
2. In order to counteract transaction id prediction,

   a. Either receiving node should ensure that the destination transaction ID is not predictable,

   b. Or receiving node should wait for n seconds before processing the 3rd message to ensure that a possible TC_ABORT can be processed before the 3rd message.

3. Receiving node should maintain a trusted operators table. If an MT SMS comes from one of those operators without TCAP Handshaking, it should be rejected.

TCAP Handshaking – MO SMS


MSC/SGSN
SMSC
(1) TCAP Begin (AC, no payload, otid=x)
(2) TCAP Continue (AC, no payload, otid=y, dtid=x)
(3) TCAP Continue (MTForwardSM payload, otid=x, dtid=y)
(4) TCAP End (MTForwardSM response)

AC = Application Context
otid = Originating Transactin Id
dtid = Destination Transaction Id

Sending MO ForwardSM with TCAP Handshaking

TCAP Handshaking – MO SMS

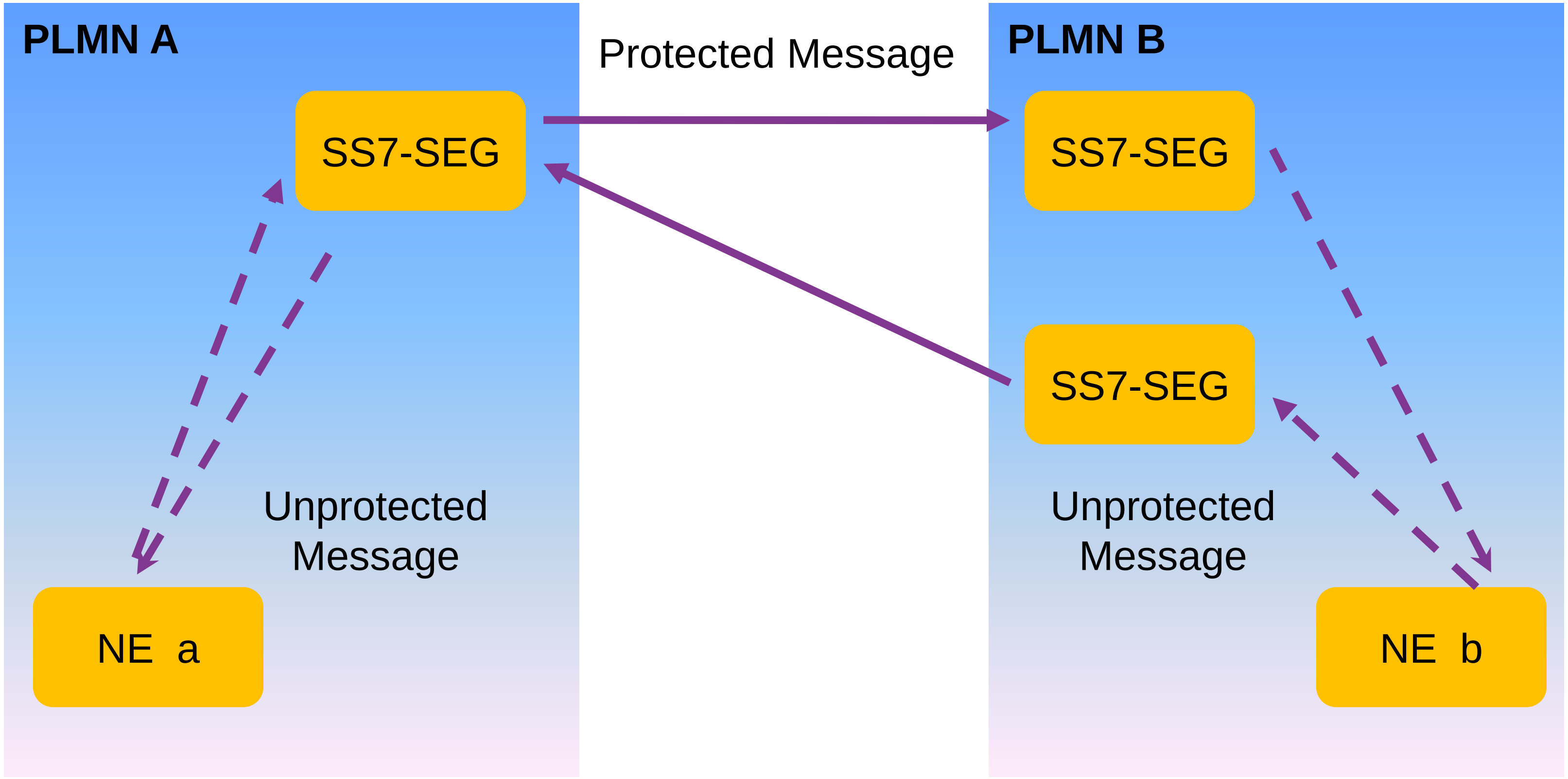
1. Receiving node should verify that the VLR address corresponding the MSISDN (contained in SM-RP_OA field of the 3rd message) is in the same operators range with the SCCP Calling Party address of the 1st message. This can be asked from HLR.
2. In order to counteract transaction id prediction,
   a. Either receiving node should ensure destination transaction ID is not predictable,
   b. Or receiving node should wait n seconds to ensure there is no aborts following.
3. Receiving node should maintain a trusted operators table. If an MO SMS comes from one of those operators without TCAP Handshaking, it should be rejected.

TCAPsec - Overview

- Defined in **3GPP TS 33.204** 3G Security; Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) user security (Release 7).
- To be used for **all TCAP transactions.**
- Authentication and optional encryption between operators.
- Using SS7_SEG (Security Gateway) is necessary.
- Does not validate TCAP user payload content. Additional measures may be needed.
- Benefit of applying TCAPsec will gradually increase as more interconnected operators apply TCAPsec.

TCAPsec – Network Architecture

- End to end architecture
- Hub and spoke architecture



TCAPsec – SS7 Security Gateway

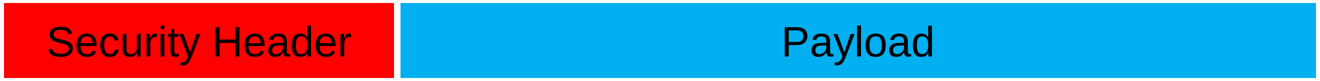
- An SS7 Security Gateway (SS7-SEG) is a network node defined in 3GPP **TS 29.204** Signalling System No. 7 (SS7) security gateway; Architecture, functional description and protocol details document.
- An SS7-SEG is located at the border of a PLMN and is responsible for,
  - protection of leaving (i.e. outbound) messages,
  - protection checking of entering (i.e. inbound) messages.
- An SS7-SEG maintains 2 databases.
  - SPD-SEG (policy information),
  - SAD-SEG (SA information).
- An outbound message is protected according to the destination address , the policy information and the existing SA corresponding to that address.
- An inbound message is unprotected or blocked according to the originating address, the policy information and the existing SA corresponding to that address.

TCAPsec – Security Association

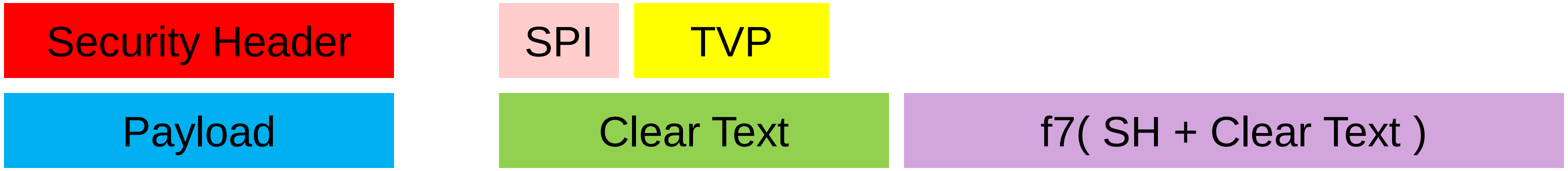
- Before protection can be applied, at least one Security Association (SA) needs to be established between the respective SS7-SEG.
- A Security Association consists of:
  - DNI - Destination Network Id (CC+NDC),
  - ONI - Origin Network Id (CC+NDC),
  - SPI - Security Parameters Index (32 bit value).
- A Security Parameters Index (SPI) identifies:
  - SEA – Security Gateway Encryption Algorithm Index (f6),
  - SEK – Security Gateway Encryption Key,
  - SIA – Security Gateway Integrity Algorithm Index (f7),
  - SIK – Security Gateway Integrity Key,
  - SA Hard Expiry Time,
  - SA Soft Expiry Time.

TCAPsec – Structure of a Protected TCAP Message

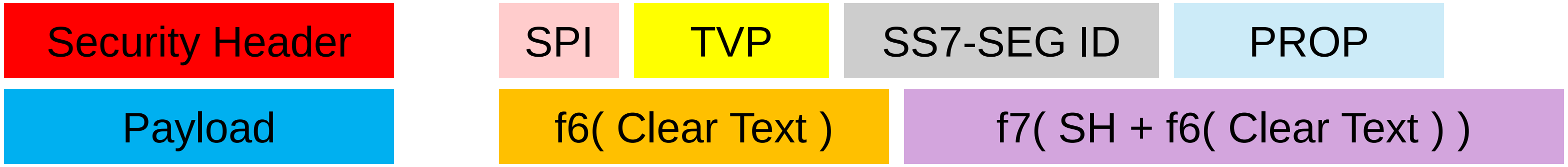
- A protected TCAP messages is sent as a Unidirectional TCAP message without a dialogue portion, with one invoke component. Operation Code=90 (SecureTransport). ParameterPart (SecureTransportArg) filled with original SCCP Info, original TCAP Info and protected Payload.
- Protected payload has 2 sections:



- Each section consists of different parameters according to the protection mode.
- Protection Mode 1: Integrity, Authenticity



- Protection Mode 2: Confidentiality, Integrity, and Authenticity



Enabling Security On Real Life Applications

- TCAP Handshaking and TCAPsec mechanisms are defined in 3GPP specifications.
- SS7-based security attacks were happening before TCAP security measures were decided.
- Those attacks were tried to be prevented by,
  - Special (vendor specific) security additions to network elements,
  - Special (vendor specific) security additions to applications,
  - SCCP/MAP policy changes specific to the threat,
  - Log analysis.

Enabling Security On Real Life Applications

Sending SM to invalid network nodes:

- MO SMS message (MOForwardSM) is sent directly to SM Service Center.
- Theoretically this message can be sent to any known GT in the network.
- Customers who want to send free SMS usually were trying all consecutive Service Center addresses in the same range with the actual SC address.
- When MOForwardSM is received by a test SMSC, SMS message may be delivered for free.
- When MOForwardSM is received by a different node (e.g. IN), unplanned traffic is generated and the node may crash if designed poorly.
- SMSC address check on the MSCs was initiated. (An MSC feature)
- GT translation in the GMSC were modified so that SMSC nodes cannot be reached by their actual GTs but by virtual numbers.

Enabling Security On Real Life Applications

Basic spam filtering in the SMSC:

- Advertorial and spam SMS messages were being sent from the same originator to many customers causing dissatisfaction.
- All MSISDNs in a range were being tried sequentially. This increases undelivered SMS counts.

- Basic antispamming feature was developed in the SMSCs.
- SMS messages submitted from the same originator are counted and if the count is bigger than a predefined limit for a predefined amount of time, they are rejected.

Enabling Security On Real Life Applications

Hatihati prevention:

- Hatihati virus was sending millions of messages to the same destinations each day.
- Unaware customers were being charged.
- SS7 links were being utilized unnecessarily.

- SMS messages destined to the specific numbers were barred to avoid charging.
- SMSCs were modified to send successful delivery reports to the infected phones so that they stop sending more SMS.

Enabling Security On Real Life Applications

MO Spoofing solutions:

- An international node was submitting SMS messages.
  - at first with a valid A-Party MSISDN but a wrong MSC address,
  - then with both a valid A-Party and a valid MSC address (A-Party location is retrieved from the HLR with SRIForSM).

- A modification was made on the SMSCs so that A-Party location is retrieved from the RWM system databases or from the HLR using SRIForSM if the subscriber is roaming and checked with the originating SCCP address of the incoming MOFwdSM message.
- GT translations are modified so that MOFwdSM messages from the international links can be identified. If an MOFwm SM message with an A-Party number located in the HPLMN comes, it is rejected.

Enabling Security On Real Life Applications

SMS Firewall / MT SMS Router:

- SMS Faking, Spoofing, Spamming, Flooding.

- SMS Firewall / MT SMS Router:
  - All MT SMS traffic is routed to SMS Firewall by means of HLR, GMSC or STP.
  - SRIForSM / FSM correlation.
  - IMSI scrambling.
  - Validation of SCCP and MAP layer addresses.
  - Spam filtering (SMS content and volume analysis).
  - Filtering rules based on detailed statistics.

Conclusion

- TCAP Handshaking is a short/medium term solution, effective only for some SMS related security threats but easy to apply.
- TCAPsec is a medium/long term solution, more difficult to apply but useful for different TCAP based attacks.
- These two TCAP security mechanisms are defined in 3GPP specifications and will show their value as more operators will begin to use them. Therefore operators and vendors should take action to implement these measures as soon as they can.
- These two are not the only precautions. For specific scenarios, other specific and effective solutions can be found.

Thank you

Umut Ersoy
Signalling Senior Manager
Vodafone Teknoloji, Turkey
Email: umut.ersoy@vodafone.com