POSITIVE TECHNOLOGIES

Attacks you can't combat:

Vulnerabilities of most robust mobile operators



Sergey Puzankov

DEFCON 神州 CHINA 1.0

About me



Telecom

18+ years in telecom industry



Security

7+ years in telecom security



Knowledge sharing

Research results & community contribution

@xigins

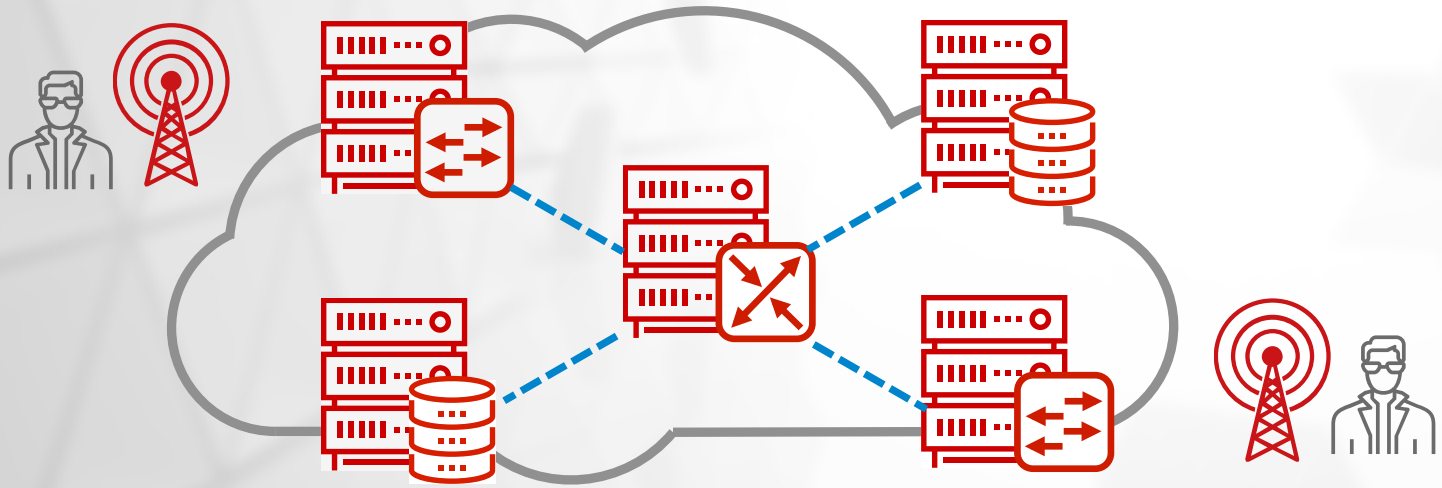
sergey_puzankov

spuzankov@ptsecurity.com



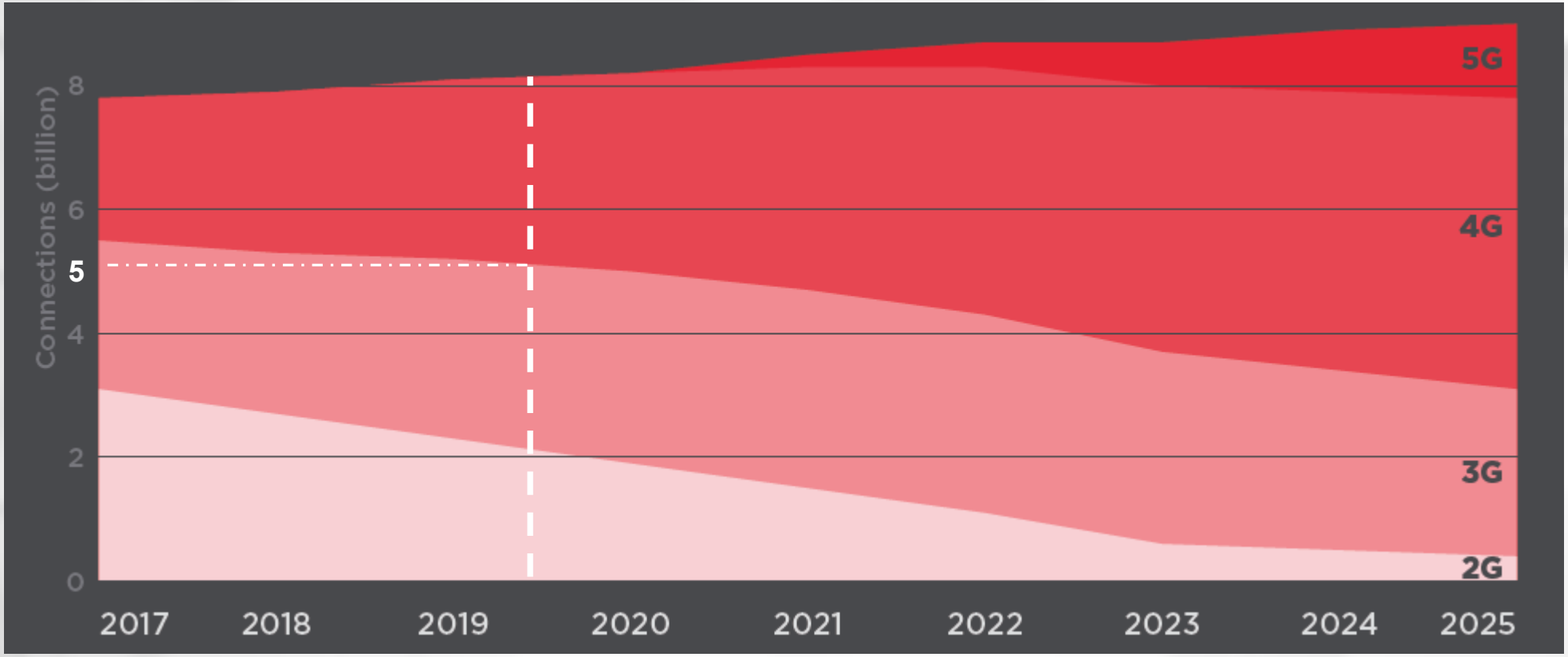
SS7 basics

SS7 (Signaling System No. 7) is a **set of telephony protocols** used to set up and tear down telephone calls, send and receive SMS messages, provide subscriber mobility, and more.



- Fixed telephony
- 2G/3G mobile networks
- Interconnection with next-generation networks

Who are potential targets?



© GSMA Intelligence 2018, Mobile connections by technology
https://www.gsmaintelligence.com/research/2018/02/infographic-mobile-connections-by-technology/656/

Now what can a Hacker do?

Intercept **private** **data, calls and SMS** messages

Easily

Track **location** of **VIPs** and **public** figures

From anywhere

Perform **massive denial of service** attacks



Take control of your **digital identity**

Any mobile operator

Get access to your **email and social media**

No special skills needed

Steal **money**

History of signaling security



SS7 development

Trusted environment. No security mechanisms in the protocol stack.

SIGTRAN (SS7 over IP) introduced. Security is still missing.



Scope grows

Growing number of SS7 connections, increasing amount of SS7 traffic.

No security policies or restrictions.

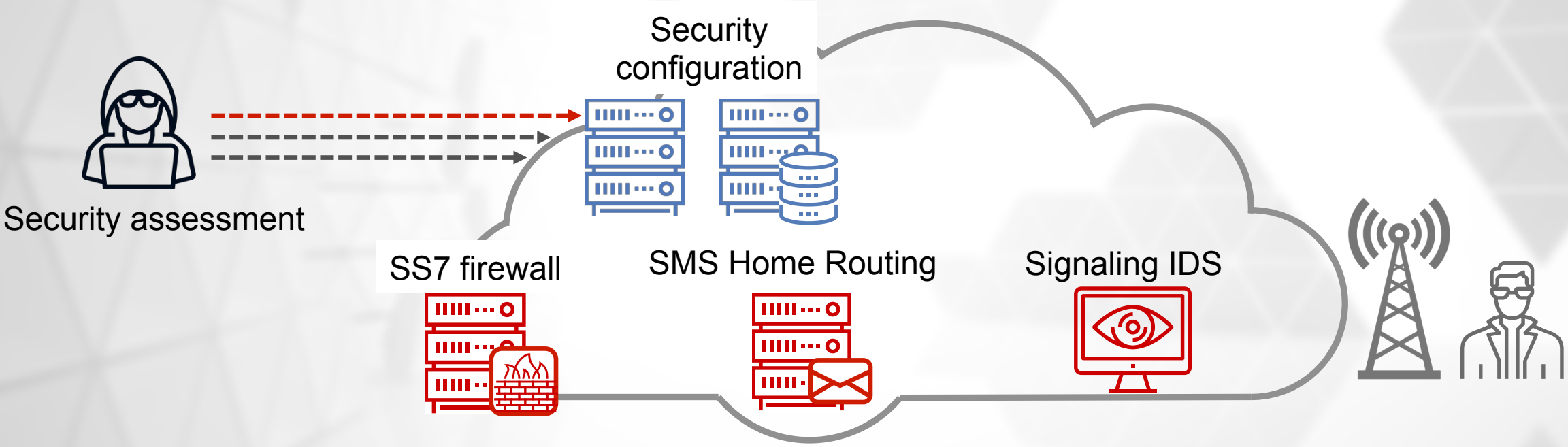


Not trusted anymore

Huge number of MNOs, MVNOs, and VAS providers.

SS7 widely used, Diameter added and spreading. Still not enough security.

Mobile operators and SS7 security

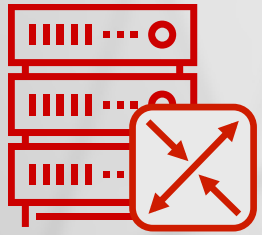


Basic nodes and identifiers

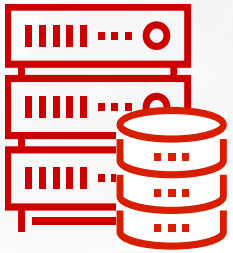
MSISDN — Mobile Subscriber Integrated Services Digital Number

GT — Global Title, address of a core node element

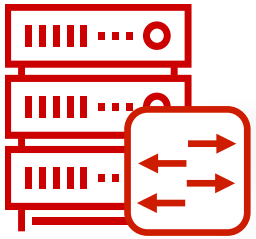
IMSI — International Mobile Subscriber Identity



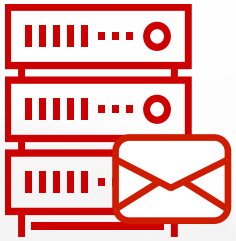
STP — Signaling Transfer Point



HLR — Home Location Register



MSC/VLR — Mobile Switching Center and Visited Location Register



SMS-C — SMS Centre

SS7 protocol stack

MAP

Mobile Application Part
is payload that contains an **operation code** and appropriate **parameters** such as **IMSI**, profile information, and location data.

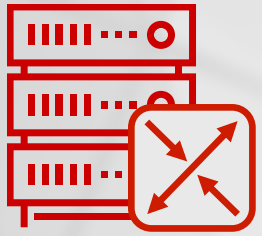
TCAP

Transaction Capabilities Application Part
is responsible for **transactions** and **dialogues** processing.

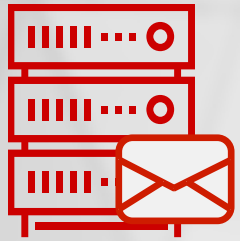
SCCP

Signaling Connection Control Part
is responsible for the **routing** of a signaling message by **Global Titles**.

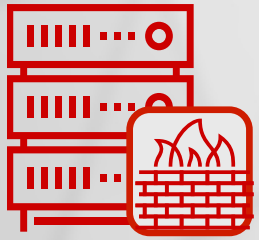
SS7 security means



Signaling Transfer Point
makes simple screening of signaling messages.

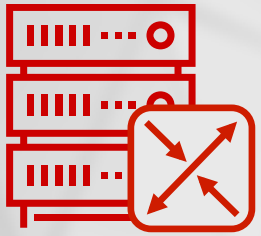


SMS Home Routing
is intended to prevent SMS fraud and hide IMSI identities.



SS7 firewall
is the most sophisticated signaling security tool that protects the network against a wide range of threats such as IMSI disclosure, location tracking, and traffic interception.

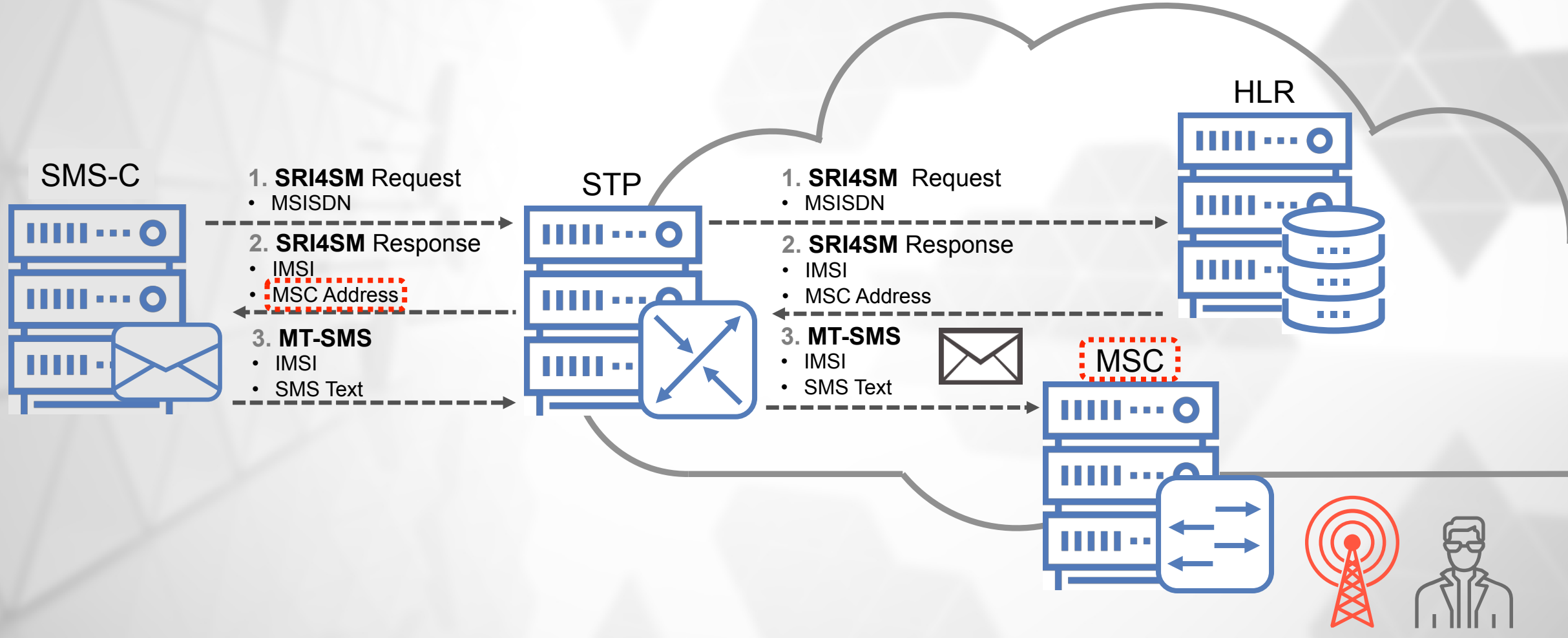
Signaling Transfer Point



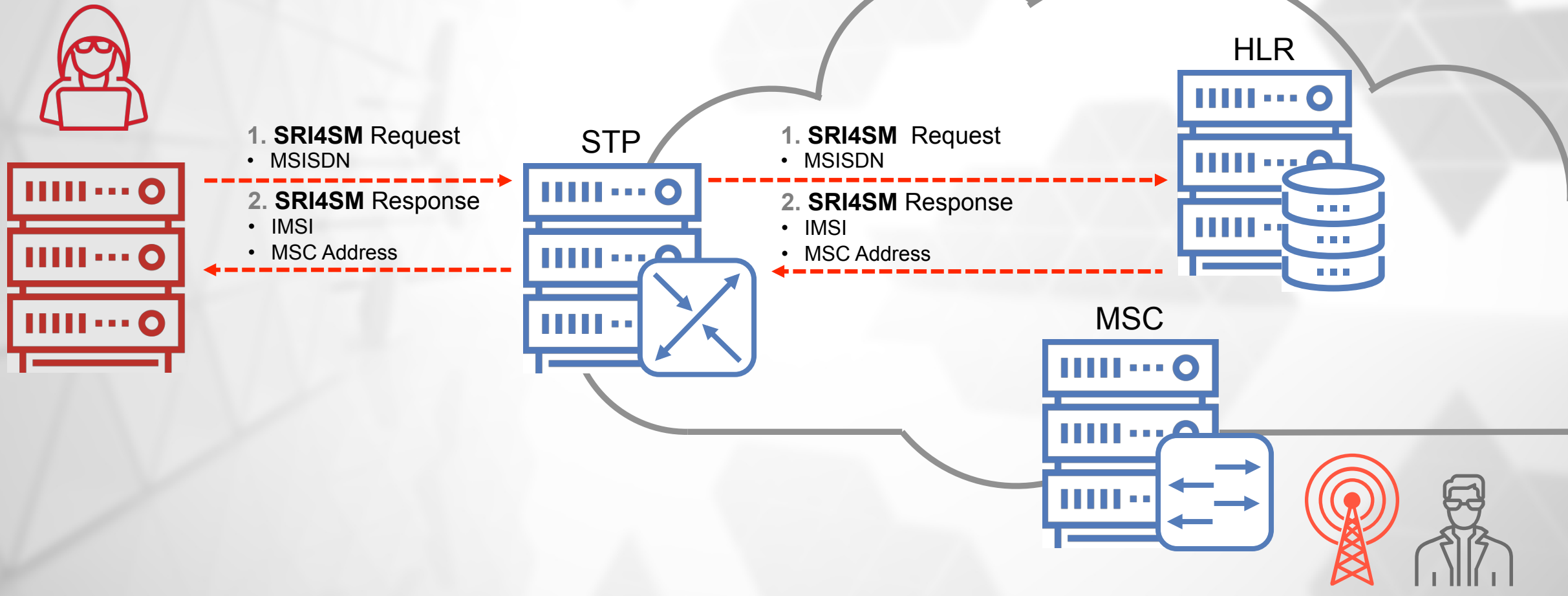
- **Signaling Transfer Point** is a router that relays SS7 messages between signaling end-points and other signaling transfer points.
- Usually the **STP** is a **border point** in a signaling network.
- It is possible to use the **STP** for the **screening of the ineligible** signaling traffic.
- **Screening rules** of the most STPs are **simple**, for instance, blocking a signaling message by a source address or redirecting a signaling message by an operation code.
- The **STP** looks through a signaling message layer by layer and applies a rule as soon as the **first appropriate pattern** is triggered.

SMS delivery process

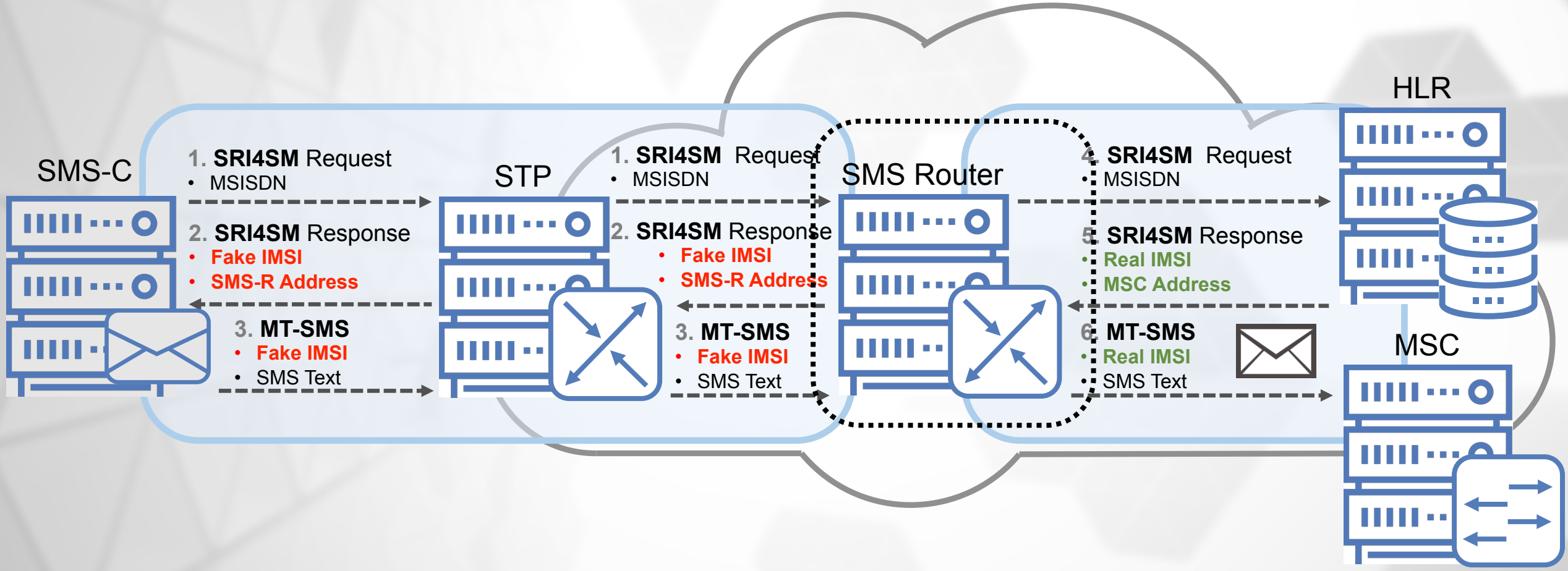
SRI4SM — SendRoutingInfoForSM



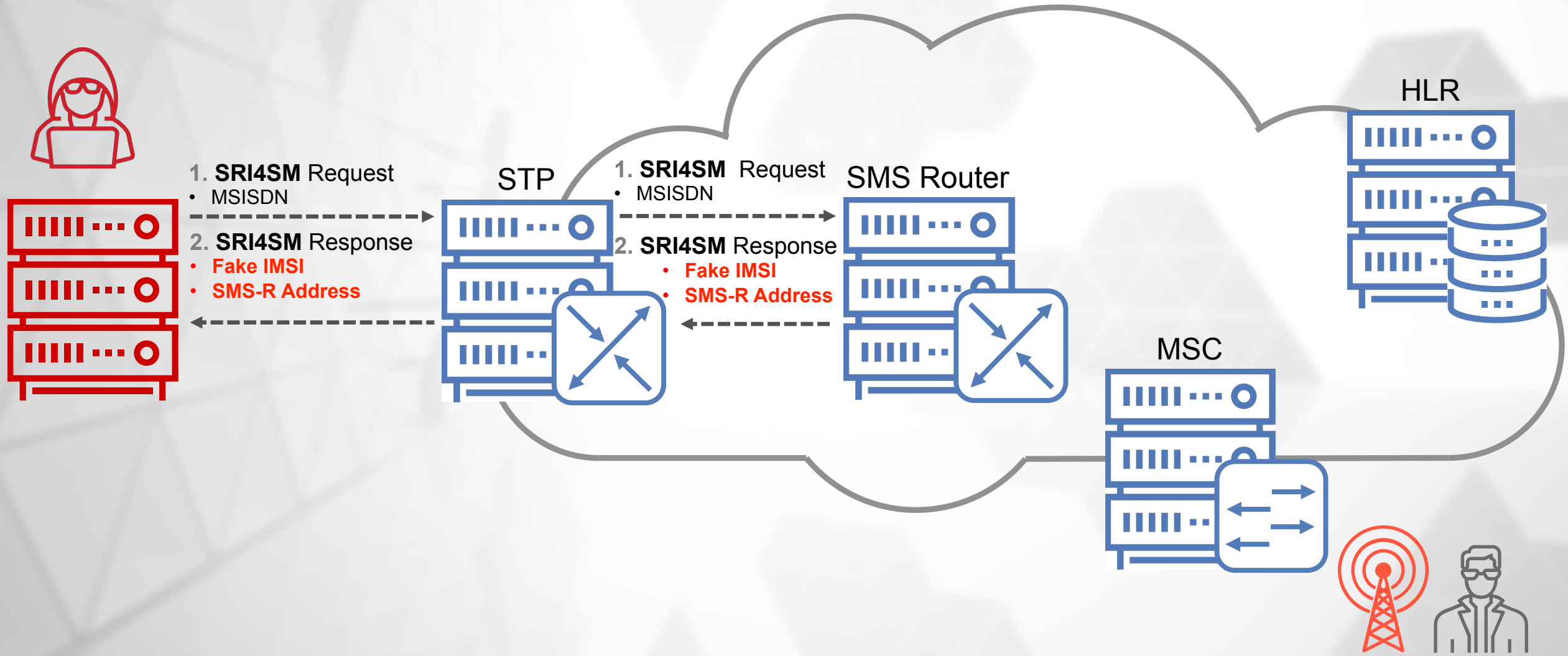
SRI4SM abuse by a malefactor



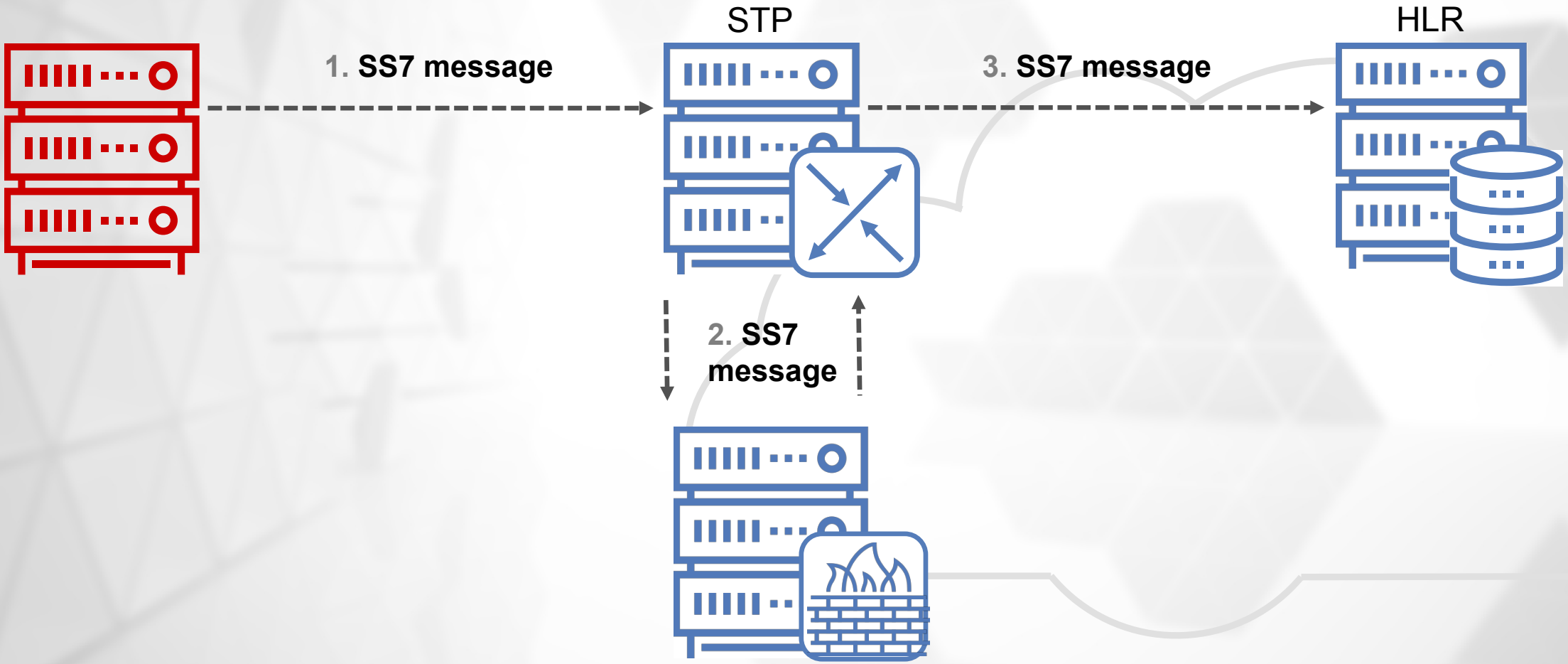
SMS Home Routing



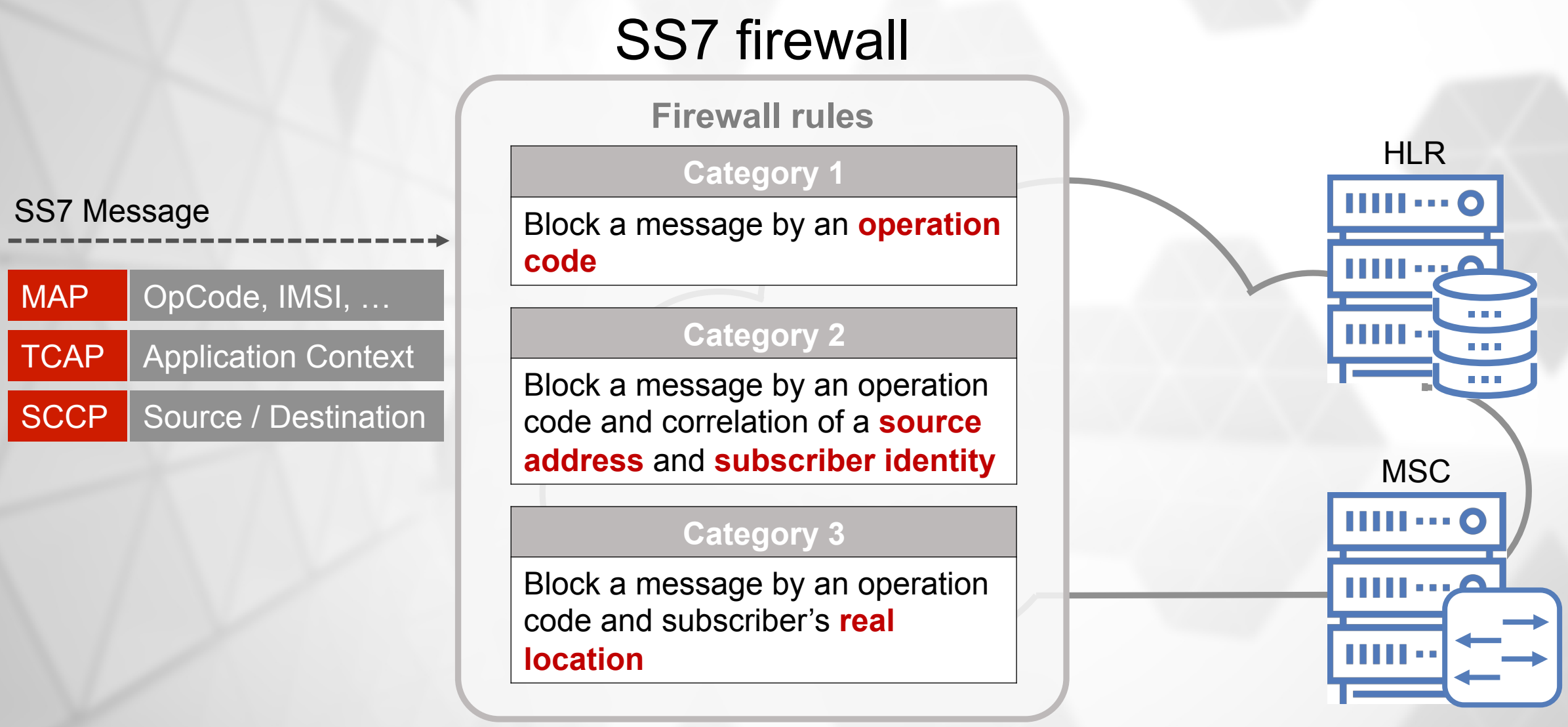
SMS Home Routing against malefactors



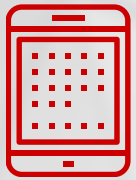
SS7 firewall: typical deployment scheme



SS7 firewall: blocking rules



SS7 attacks and vulnerabilities



IMSI disclosure via a malformed Application Context Name (ACN) parameter

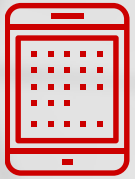


Location tracking via Operation Code Tag substitution



Voice call interception (MiTM) via a Double MAP vulnerability

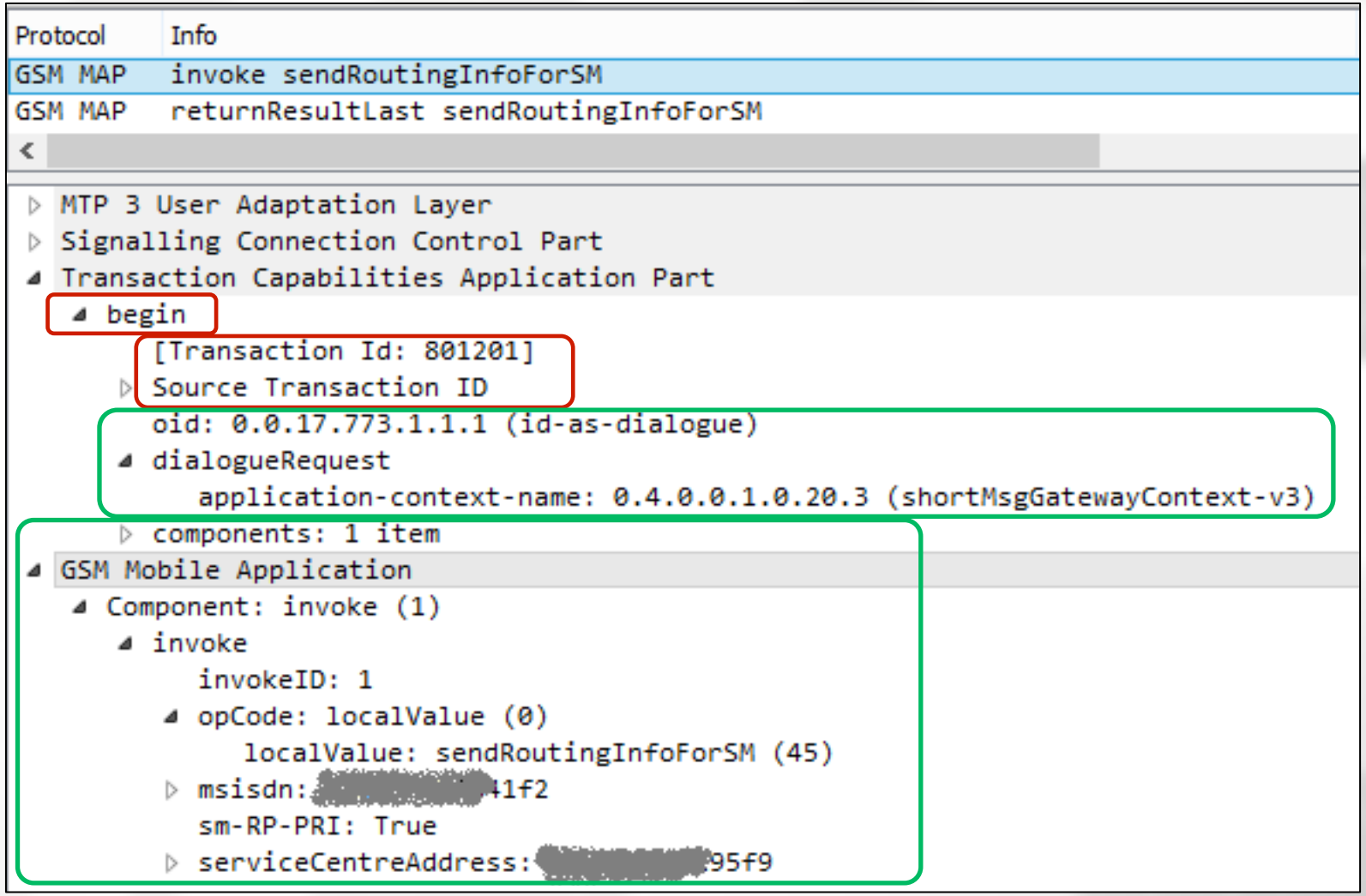
IMSI disclosure



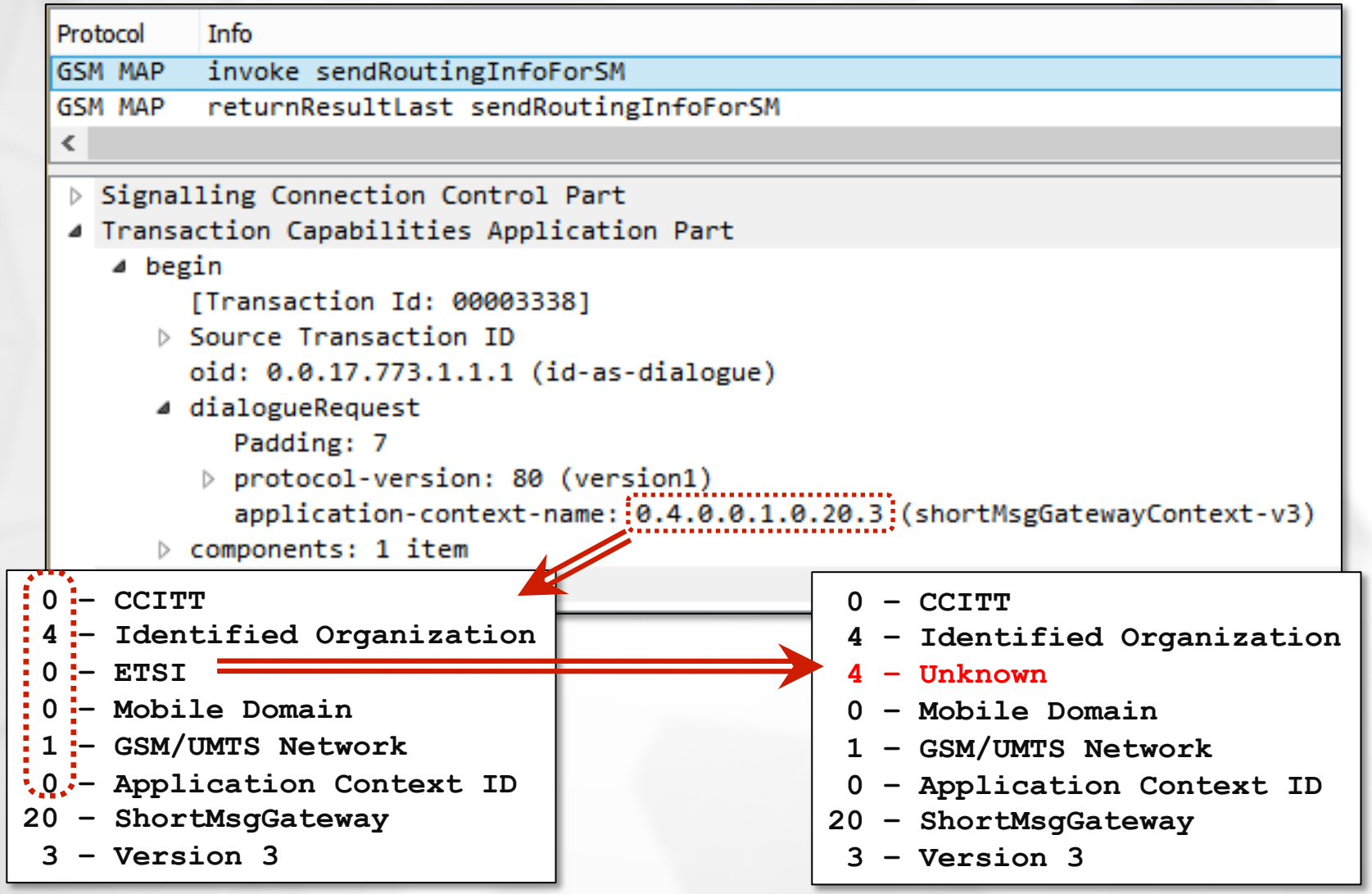
Exploitation of malformed ACN

TCAP protocol

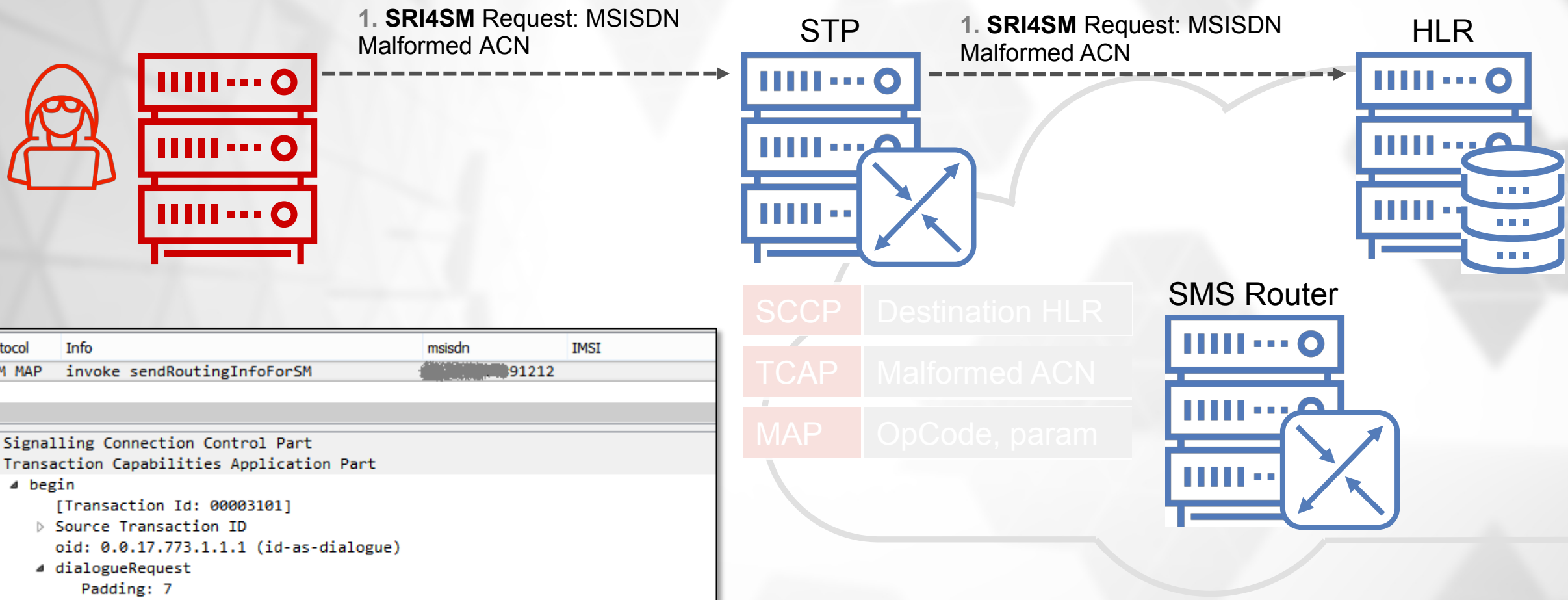
- TCAP Message Type — mandatory
- Transaction IDs — mandatory
- Dialogue Portion — optional
- Component Portion — optional



Changing ACN



IMSI disclosure via malformed ACN



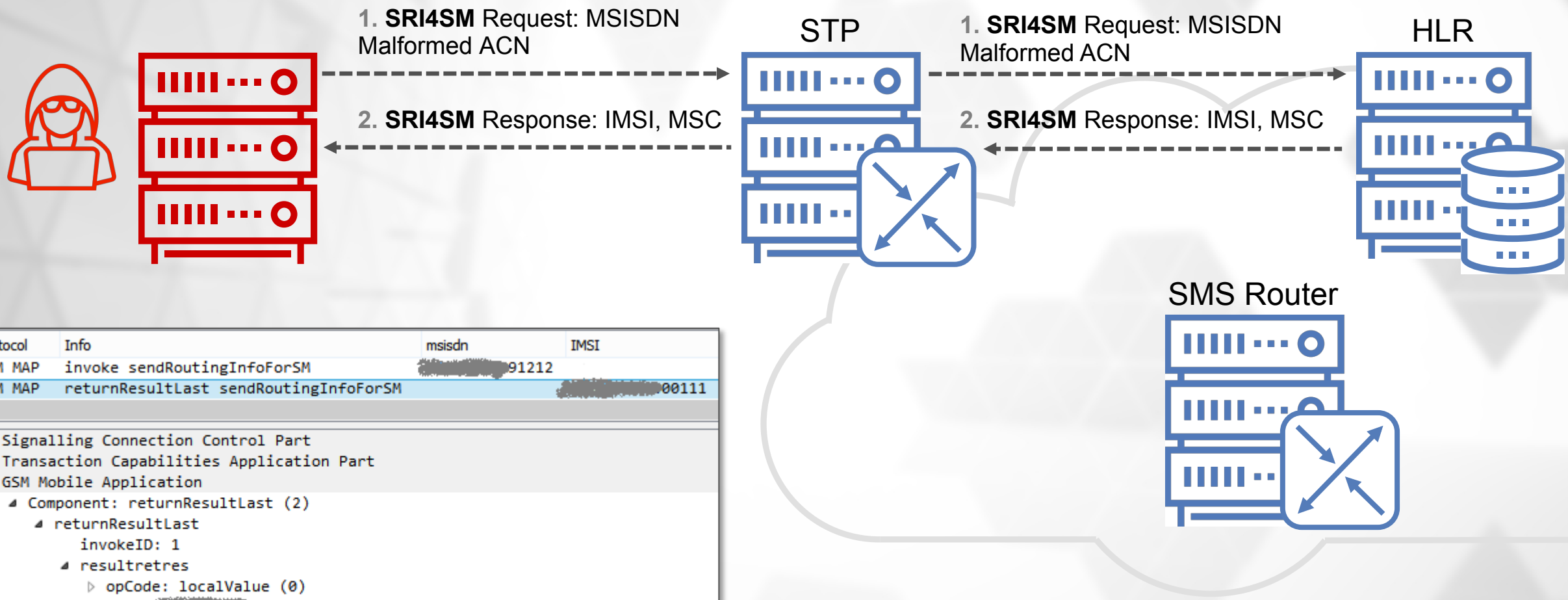
Protocol	Info	msisdn	IMSI
GSM MAP	invoke sendRoutingInfoForSM	[redacted]91212	

```
Signalling Connection Control Part
Transaction Capabilities Application Part
  begin
    [Transaction Id: 00003101]
    Source Transaction ID
    oid: 0.0.17.773.1.1.1 (id-as-dialogue)
    dialogueRequest
      Padding: 7
      protocol-version: 80 (version1)
      application-context-name: 0.4.4.0.1.0.20.3 (itu-t.4.4.0.1.0.20.3)
```

```
0080  00 11 86 05 01 01 01 a0  11 60 0f 80 02 07 80 a1
0090  09 06 07 04 04 00 01 00  14 03 6c 1f a1 1d 02 01
```

Malformed ACN

IMSI disclosure via malformed ACN

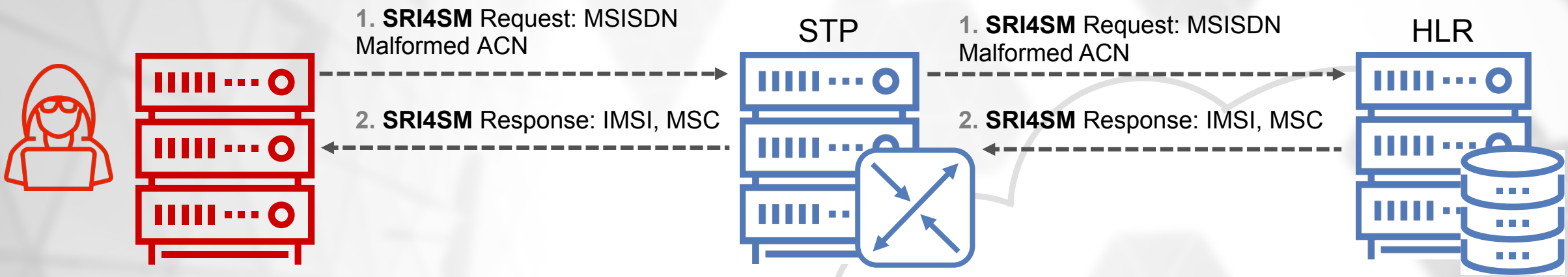


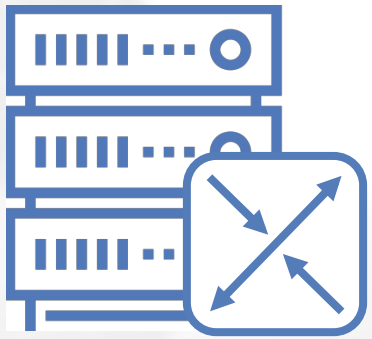
Protocol	Info	msisdn	IMSI
GSM MAP	invoke sendRoutingInfoForSM	[redacted]91212	
GSM MAP	returnResultLast sendRoutingInfoForSM		[redacted]00111

```
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
  Component: returnResultLast (2)
    returnResultLast
      invokeID: 1
      resultretres
        opCode: localValue (0)
        IMSI: [redacted]00111
        locationInfoWithLMSI
```

SMS Router bypassed

IMSI disclosure via malformed ACN





Protocol	Info	msisdn	IMSI
GSM MAP	invoke sendRoutingInfoForSM	[redacted]91212	
GSM MAP	returnResultLast sendRoutingInfoForSM		[redacted]00111
GSM MAP	invoke sendRoutingInfoForSM	[redacted]91212	
GSM MAP	returnResultLast sendRoutingInfoForSM		[redacted]00111

```
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
  ◢ Component: returnResultLast (2)
    ◢ returnResultLast
        invokeID: 1
      ◢ resultretres
        ▷ opCode: localValue (0)
        ▷ IMSI: [redacted]00111
        ▷ locationInfoWithLMSI
```

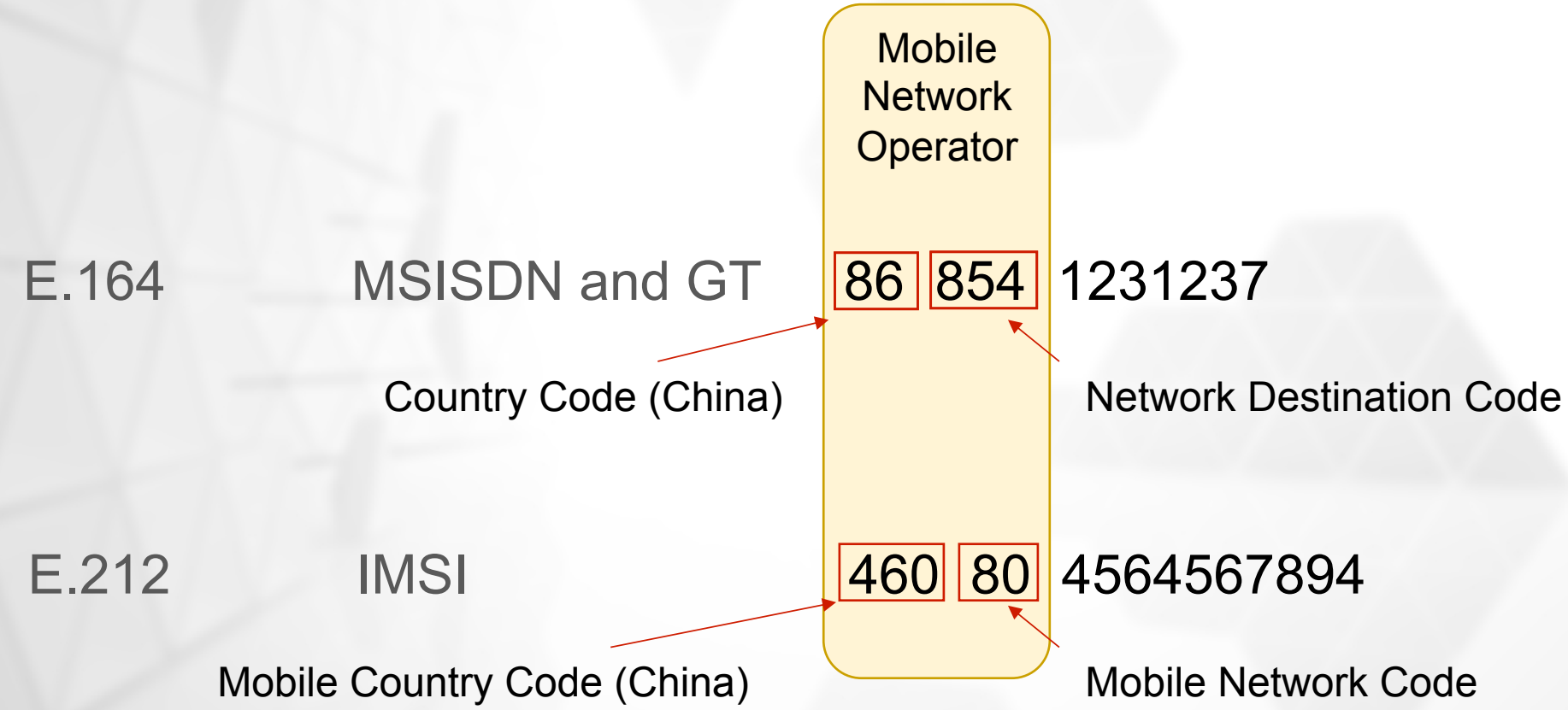
Equal IMSIs mean the SMS Home Routing solution is absent or not involved.

Location tracking

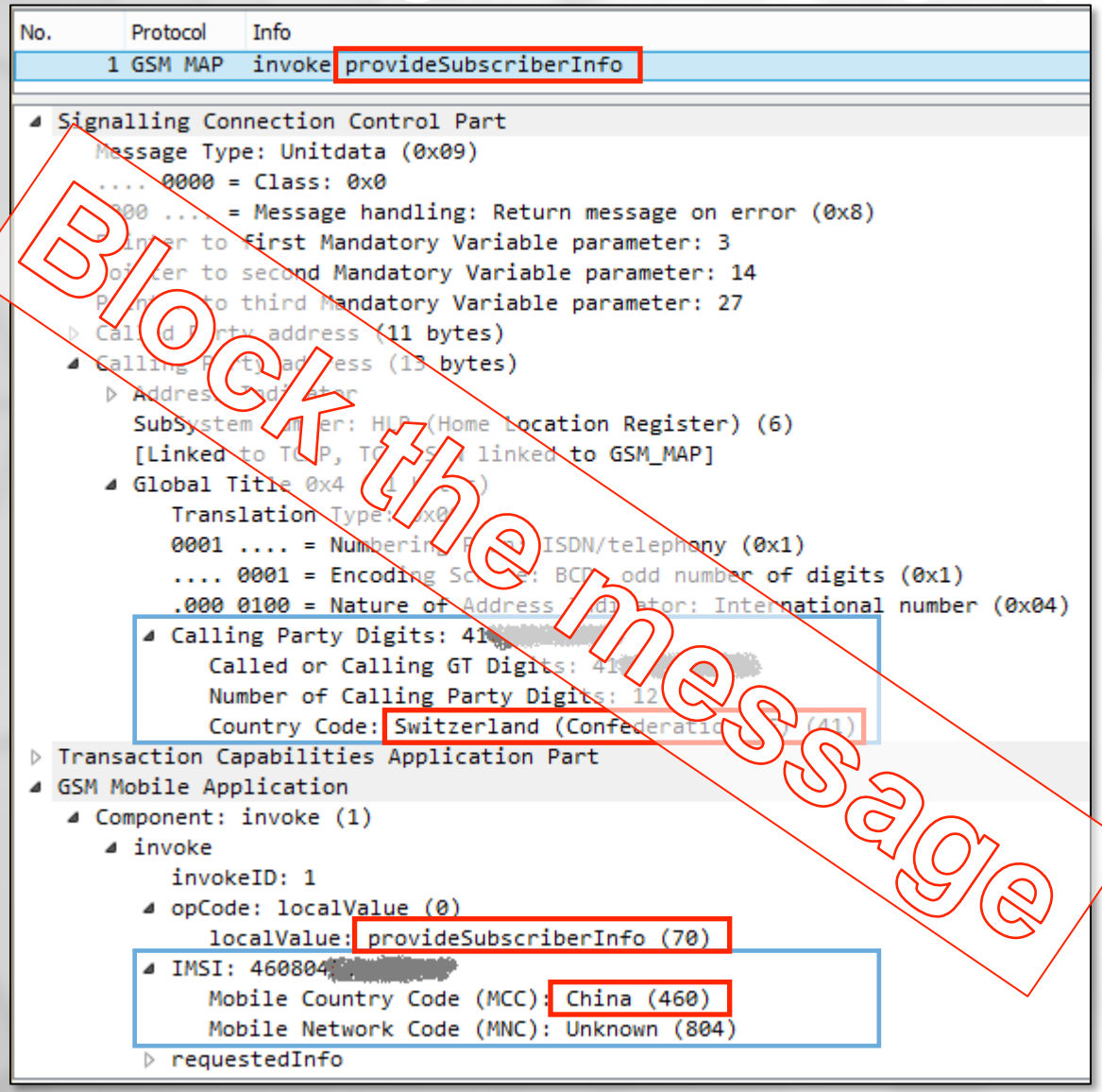


Substitution of Operation Code Tag

Numbering plans



Blocking rule: category 2



Block the message

Operation code

Category 2
Block a message by an operation code and correlation of a **source address** and **subscriber identity**

Source address

Switzerland ≠ China

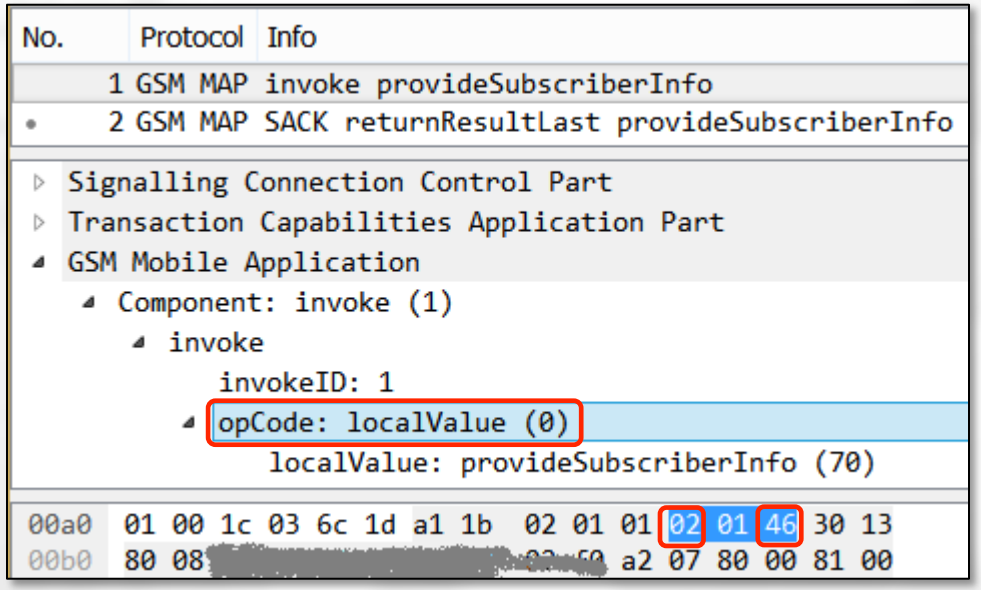
Subscriber identity

ITU-T Q.773 Recommendation

ITU-T Q.773 – Transaction capabilities formats and encoding

Table 22/Q.773 – Coding of Operation Code Tag

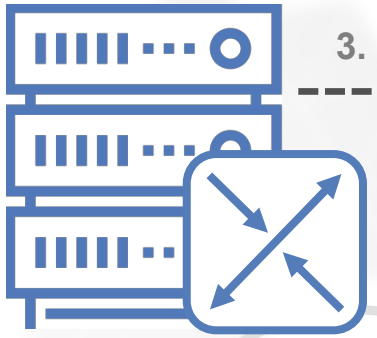
	H	G	F	E	D	C	B	A	
Local Operation Code Tag	0	0	0	0	0	0	1	0	= 2
Global Operation Code Tag	0	0	0	0	0	1	1	0	= 6



Location tracking via Global OpCode



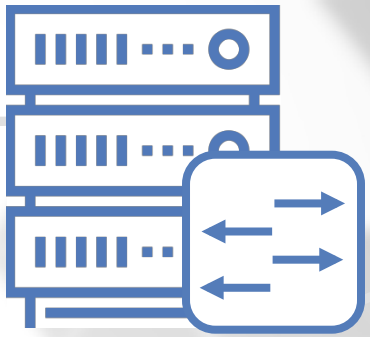
1. **PSI** with Global OpCode tag



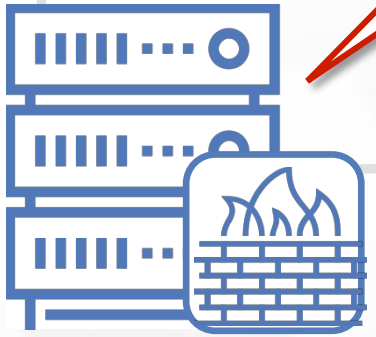
STP

2. **PSI** with Global OpCode tag

3. **PSI** with Global OpCode tag



MSC/VLR



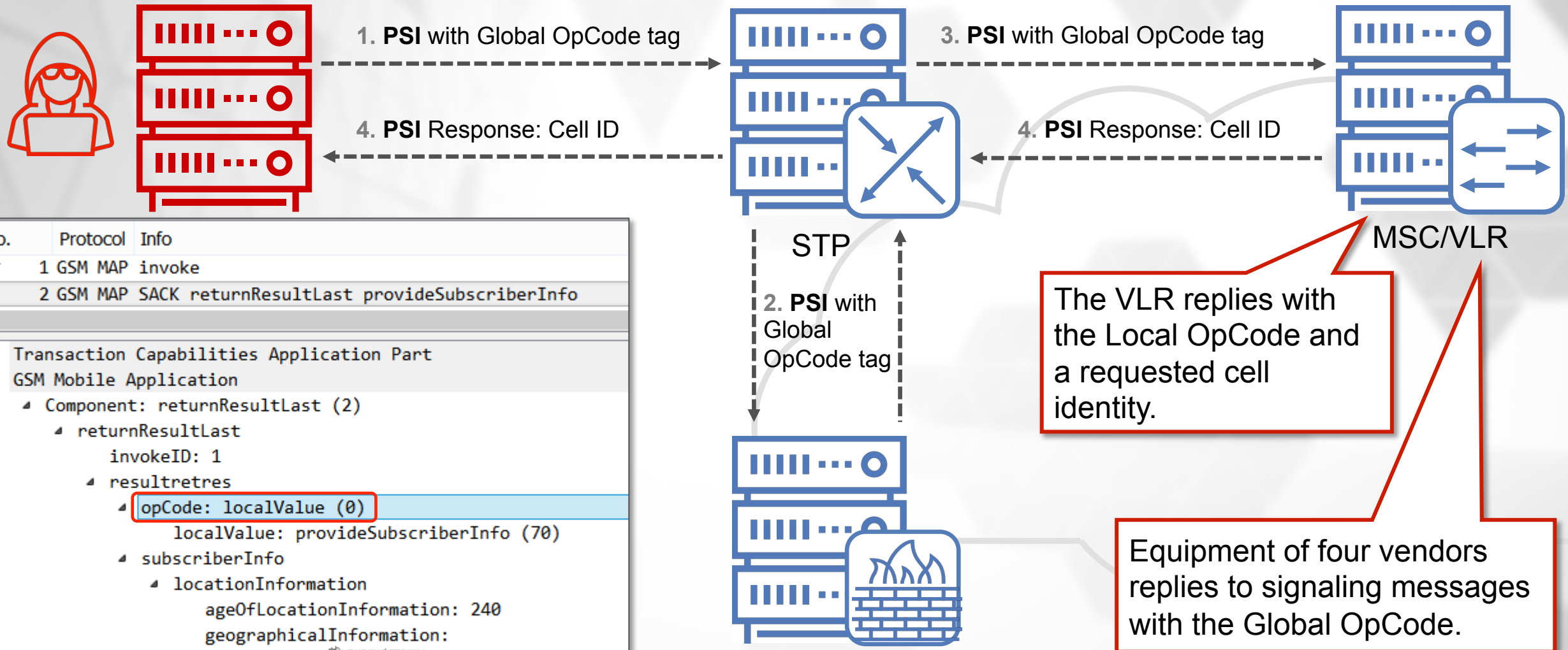
The SS7 FW is looking for a Local OpCode. Global OpCodes are ignored.

```
No.     Protocol  Info
      1 GSM MAP   invoke

  Signalling Connection Control Part
  Transaction Capabilities Application Part
  GSM Mobile Application
    Component: invoke (1)
      invoke
          invokeID: 1
        opCode: globalValue (1)
            globalValue: 1.30 (iso.30)

00a0  01 00 1c 03 6c 1d a1 1b  02 01 01 06 01 46 30 13
00b0  80 08 [redacted] 0 a2 07 80 00 81 00
```

Location tracking via Global OpCode




```
No.   Protocol  Info
    1 GSM MAP   invoke
    2 GSM MAP   SACK returnResultLast provideSubscriberInfo

Transaction Capabilities Application Part
GSM Mobile Application
  Component: returnResultLast (2)
    returnResultLast
      invokeID: 1
      resultretres
        opCode: localValue (0)
          localValue: provideSubscriberInfo (70)
        subscriberInfo
          locationInformation
            ageOfLocationInformation: 240
            geographicalInformation:
            vlr-number: [redacted]8169
            cellGlobalIdOrServiceAreaIdOrLAI: cellGlo
```

Voice call interception (MiTM)



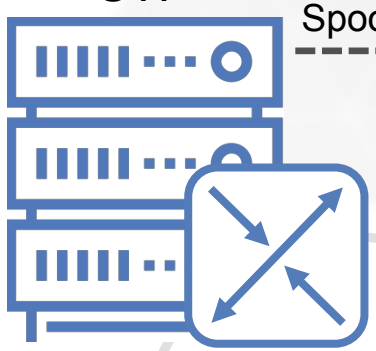
Exploitation of a Double MAP vulnerability

Voice call interception (MiTM)



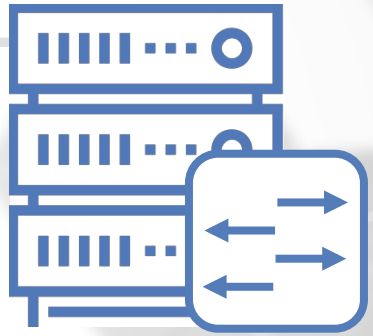
1. **InsertSubscriberData** Request: IMSI
Spoofed billing platform address

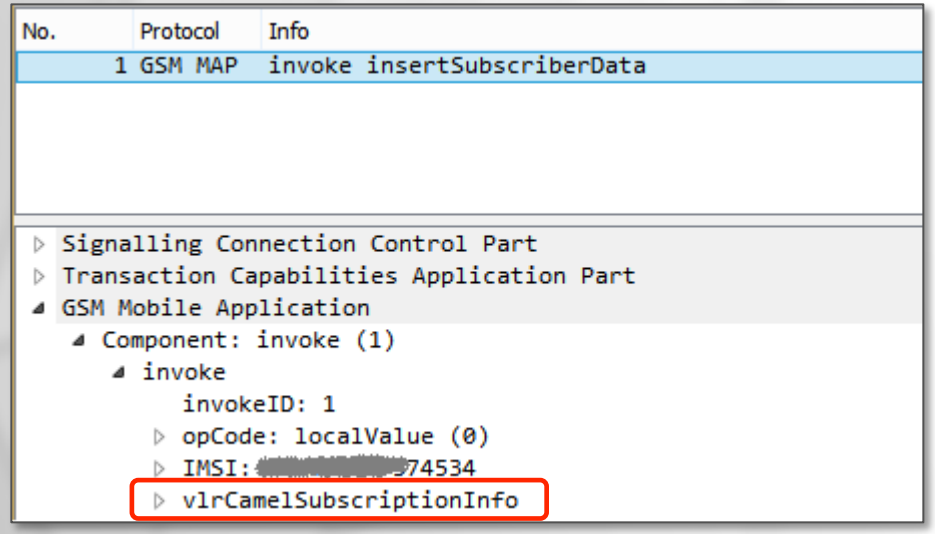
STP



1. **InsertSubscriberData** Request: IMSI
Spoofed billing platform address

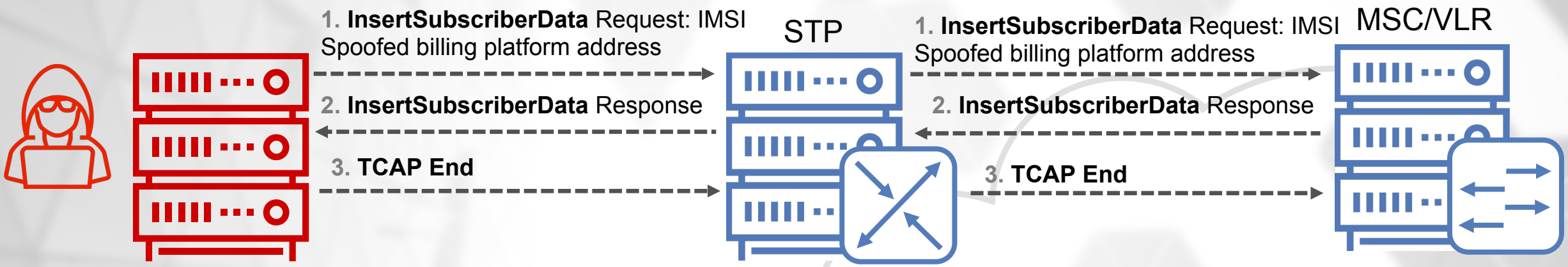
MSC/VLR







Voice call interception (MiTM)

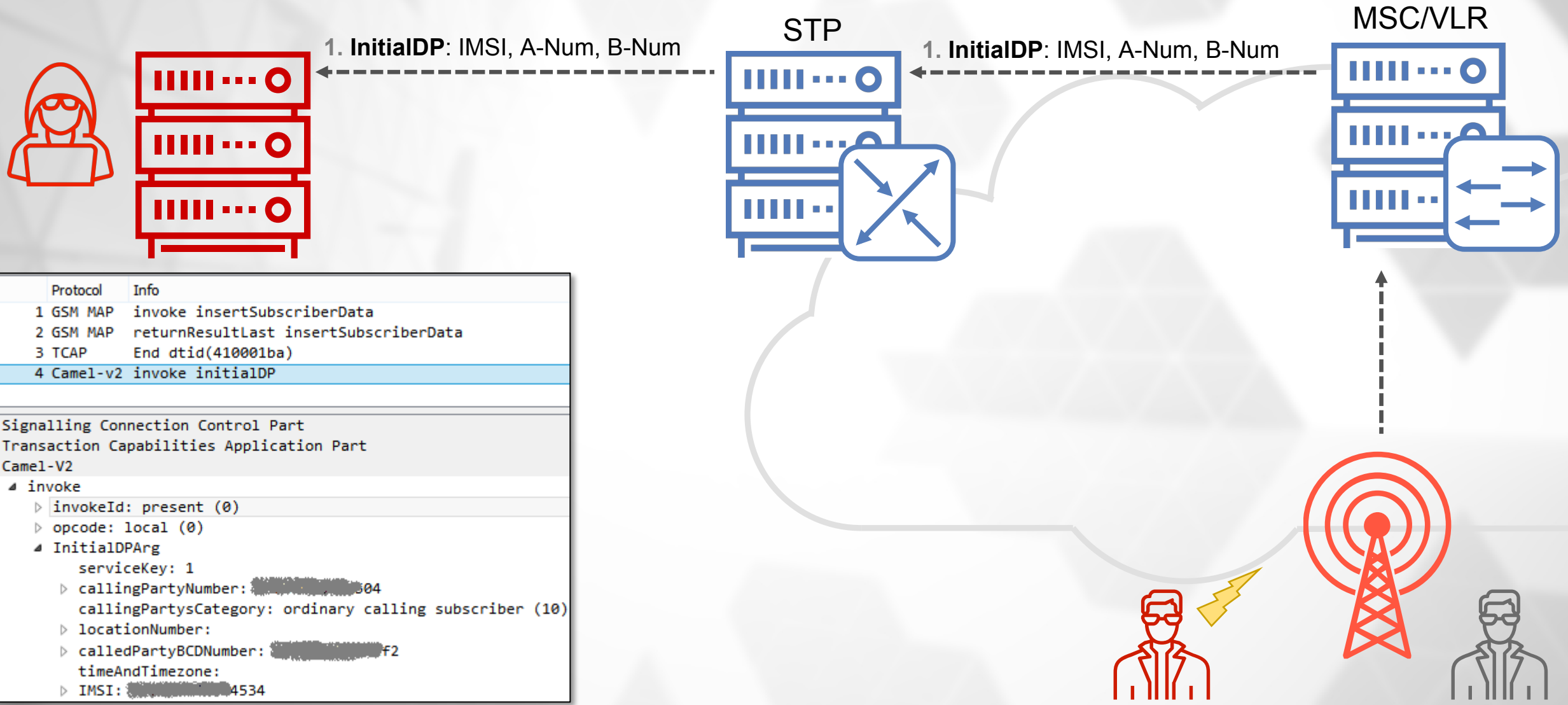


No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData
2	GSM MAP	returnResultLast insertSubscriberData
3	TCAP	End dtid(410001ba)

```
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
  ◢ Component: returnResultLast (2)
    ◢ returnResultLast
        invokeID: 1
      ◢ resultretres
        ▷ opCode: localValue (0)
          Padding: 4
        ▷ supportedCamelPhases: c0 (phase1, phase2)
```



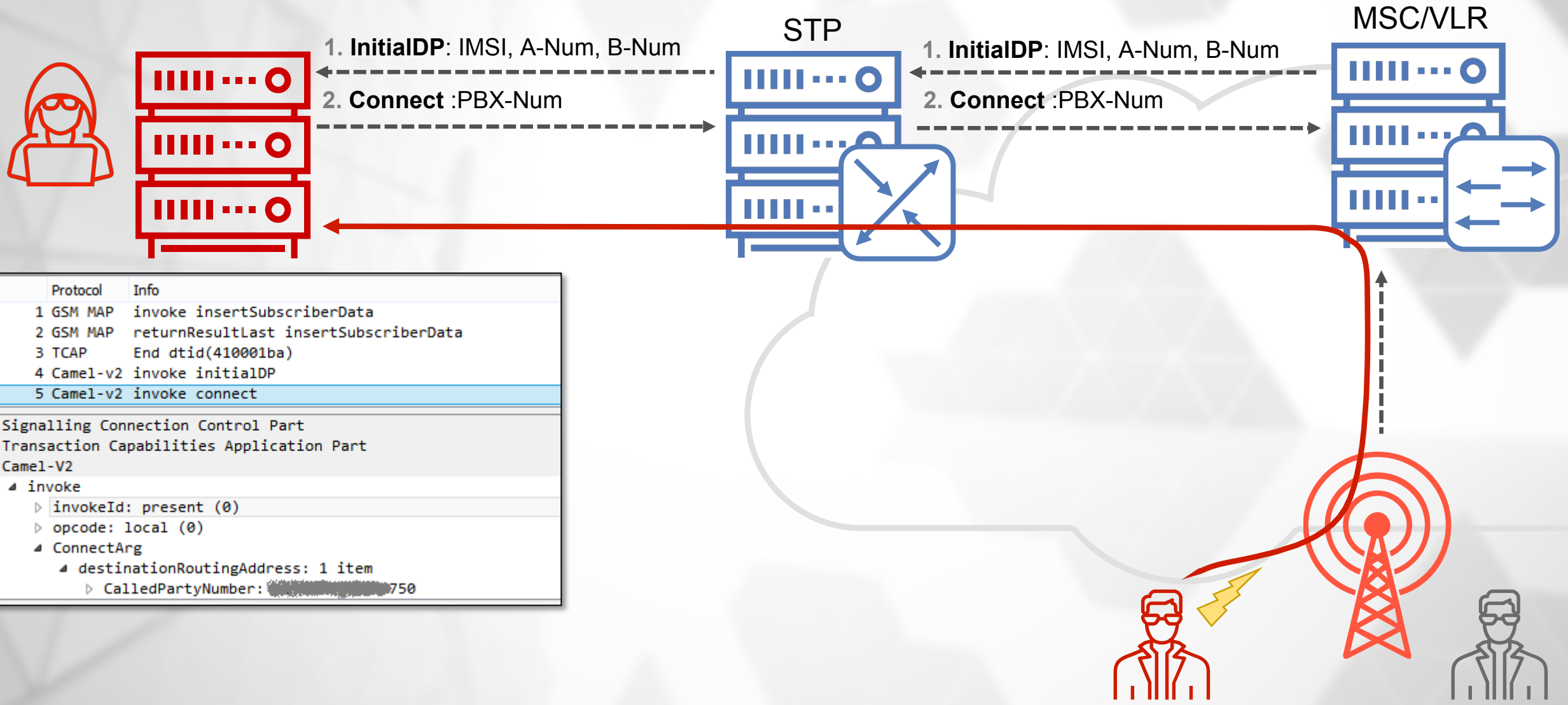
Voice call interception (MiTM)



No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData
2	GSM MAP	returnResultLast insertSubscriberData
3	TCAP	End dtid(410001ba)
4	Camel-v2	invoke initialDP

```
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ Camel-V2
  ◢ invoke
    ▷ invokeId: present (0)
    ▷ opcode: local (0)
    ◢ InitialDPArg
        serviceKey: 1
      ▷ callingPartyNumber: [redacted]504
        callingPartysCategory: ordinary calling subscriber (10)
      ▷ locationNumber:
      ▷ calledPartyBCDNumber: [redacted]f2
        timeAndTimezone:
      ▷ IMSI: [redacted]4534
```

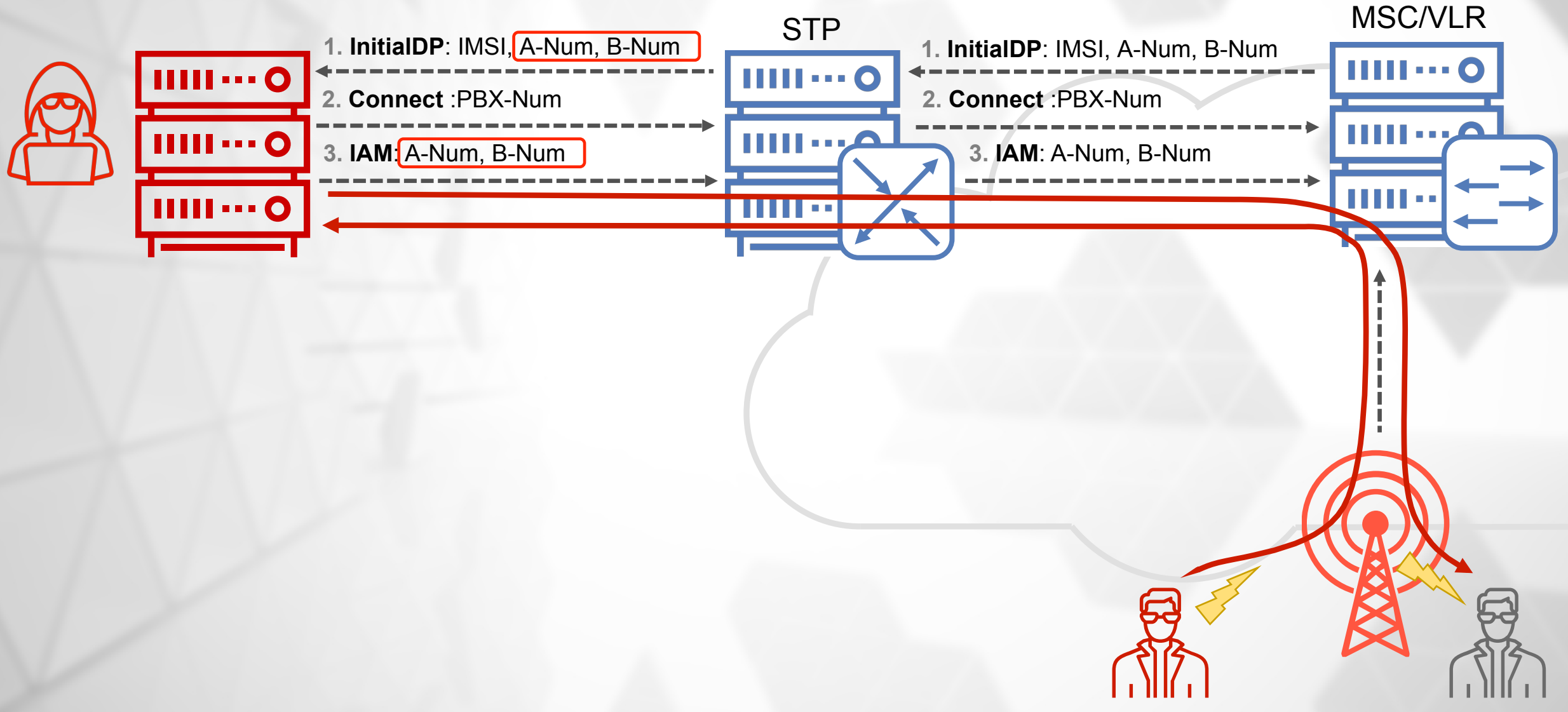
Voice call interception (MiTM)



No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData
2	GSM MAP	returnResultLast insertSubscriberData
3	TCAP	End dtid(410001ba)
4	Camel-v2	invoke initialDP
5	Camel-v2	invoke connect

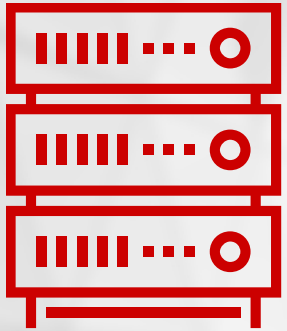
```
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ Camel-V2
  ◢ invoke
    ▷ invokeId: present (0)
    ▷ opcode: local (0)
    ◢ ConnectArg
      ◢ destinationRoutingAddress: 1 item
        ▷ CalledPartyNumber: [redacted]750
```

Voice call interception (MiTM)



SS7 FW against MiTM attack



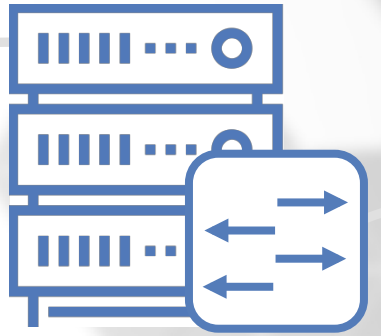


1. **InsertSubscriberData** Request: IMSI, Spoofed billing platform address

STP



MSC/VLR



2. **InsertSubscriberData** Request: IMSI, Spoofed billing platform address



The SS7 FW correlates the IMSI and source address and blocks the InsertSubscriberData message.

```
No.     Protocol  Info
      1 GSM MAP   invoke insertSubscriberData

  ◢ Calling Party address (11 bytes)
    ▷ Address Indicator
      SubSystem Number: HLR (Home Location Register) (6)
      [Linked to TCAP, TCAP SSN linked to GSM_MAP]
    ◢ Global Title 0x4 (11 bytes)
        Translation Type: 0x00
        0001 .... = Numbering Plan: ISDN/telephony (0x1)
        .... 0001 = Encoding Scheme: BCD, odd number of digits
        .000 0100 = Nature of Address Indicator: International
      ▷ Calling Party Digits: 41[redacted]
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 1
      ▷ opCode: localValue (0)
      ◢ IMSI: 460[redacted]
```

Switzerland ≠ China

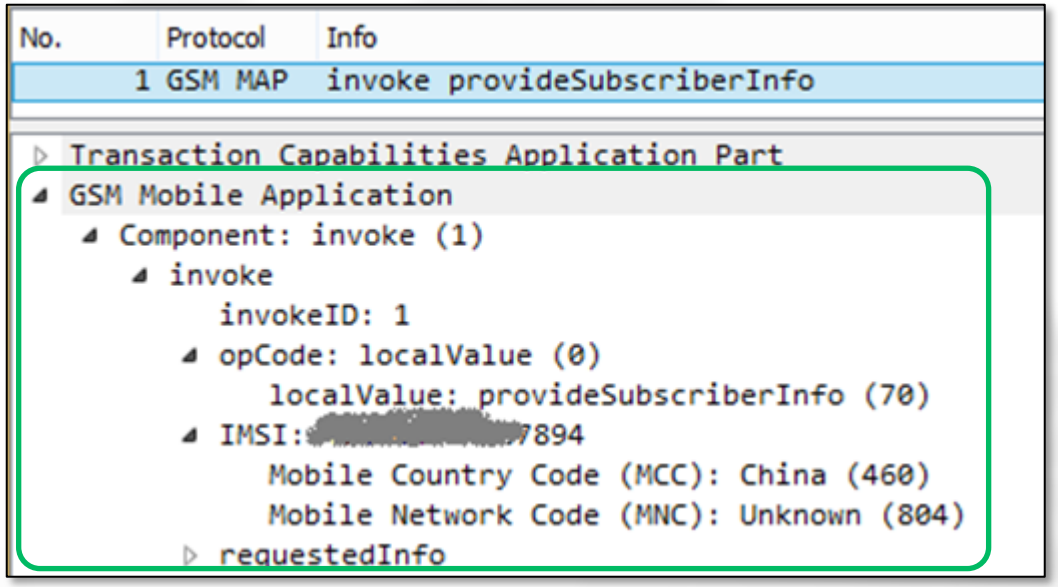






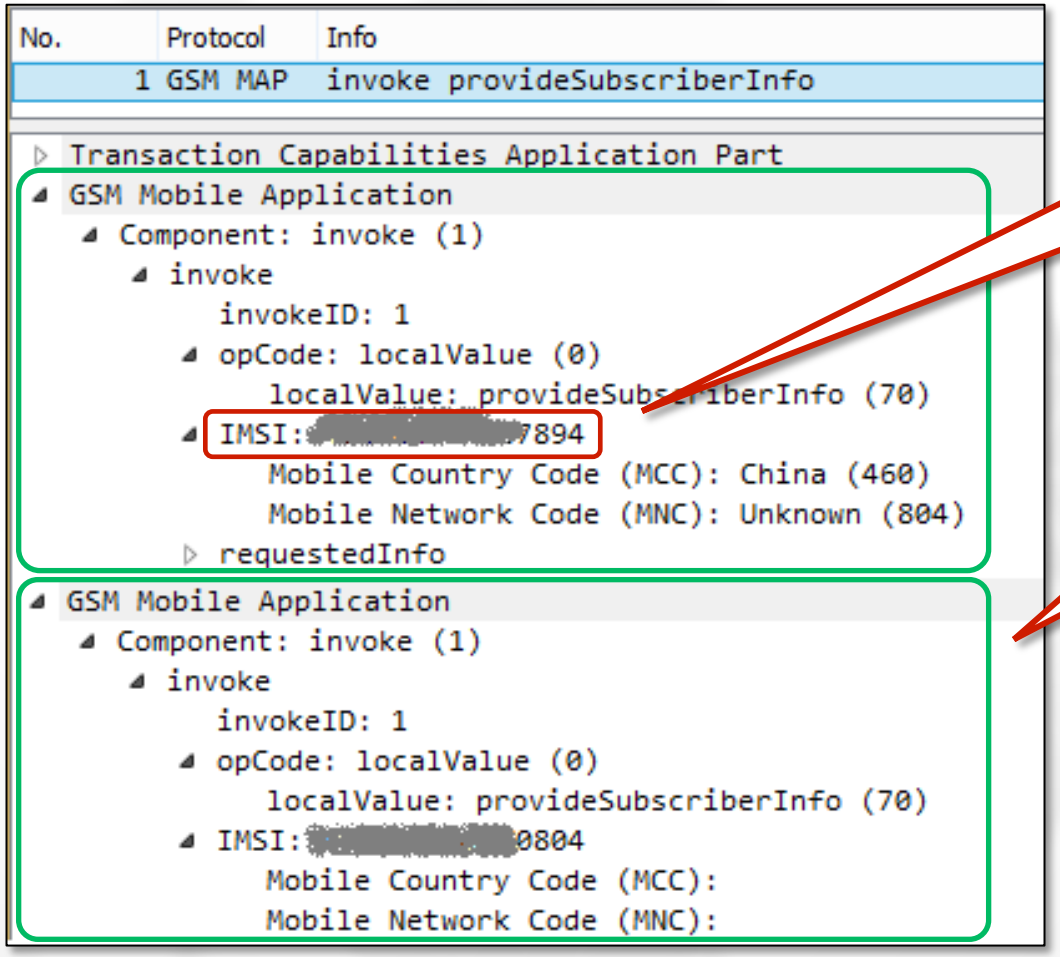
TCAP protocol

- TCAP Message Type — mandatory
- Transaction IDs — mandatory
- Dialogue Portion — optional
- Component Portion — optional



Double MAP component

- TCAP Message Type — mandatory
- Transaction IDs — mandatory
- Dialogue Portion — optional
- Component Portion — optional
  - Component 1
  - Component 2



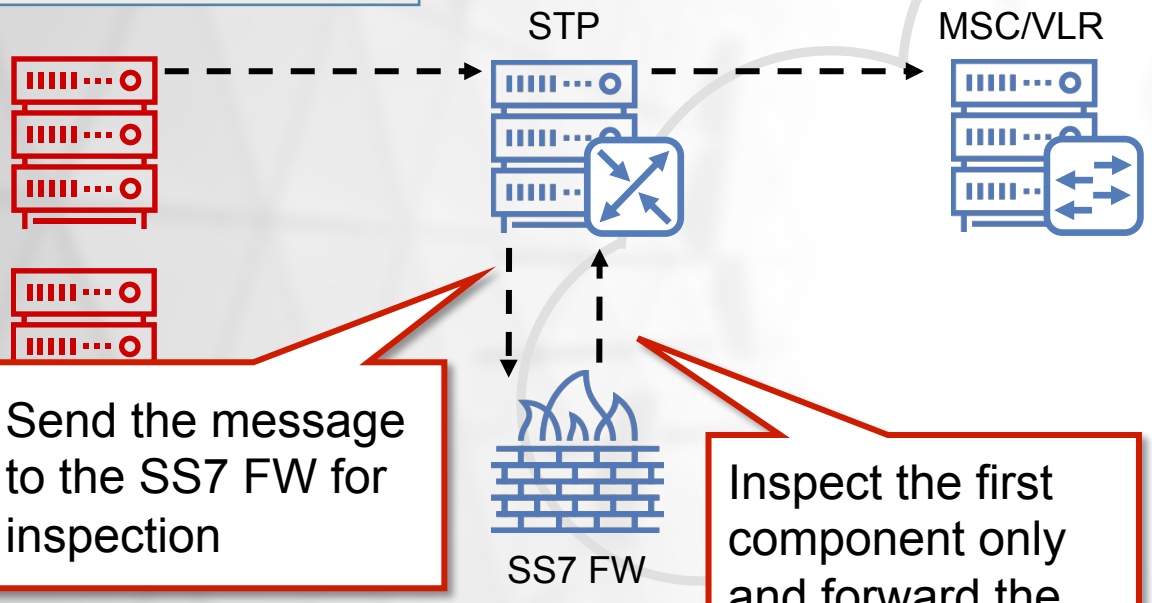
The SS7 FW checks a subscriber's ID in the first component considering the other data as a long payload not meant to be inspected.

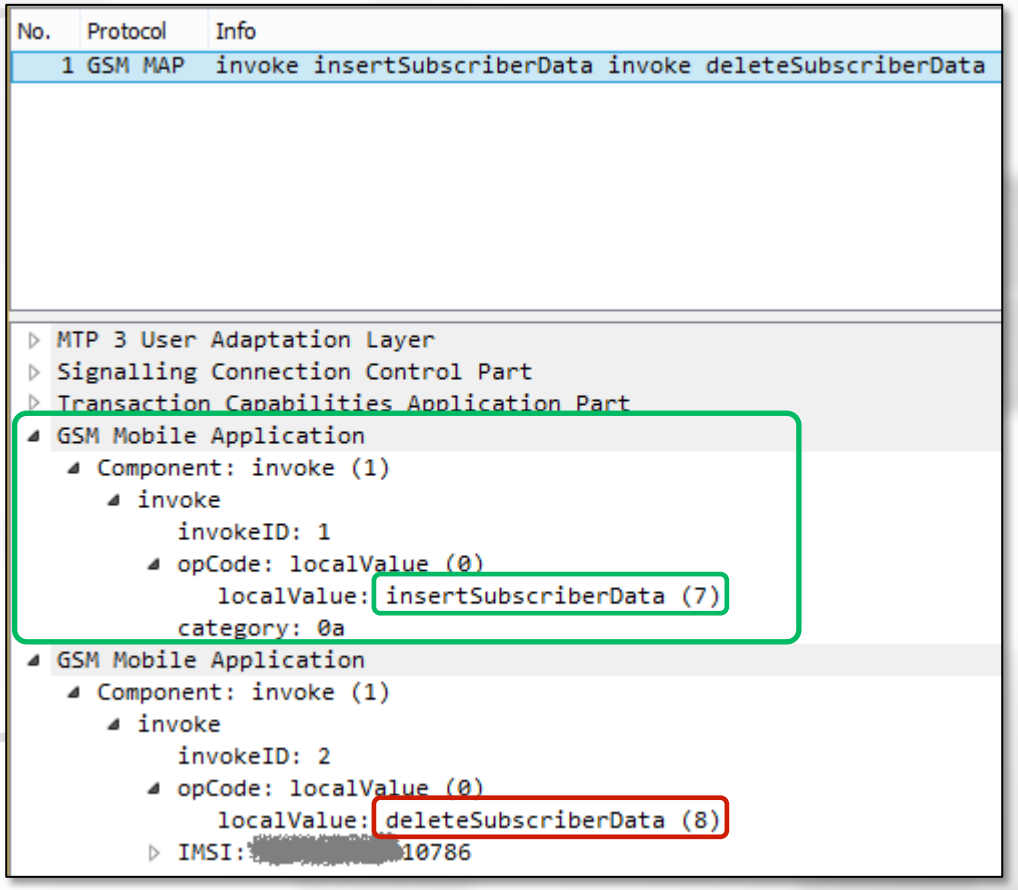
Double MAP in MiTM attack

TCAP Begin

InsertSubscriberData_REQ

DeleteSubscriberData_REQ



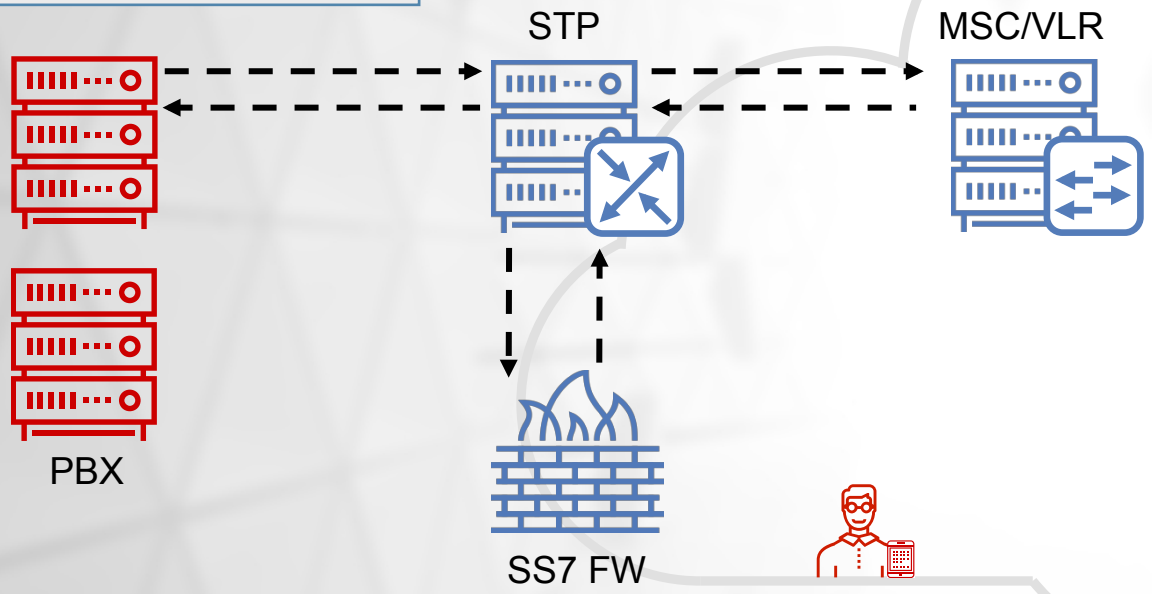


Double MAP in MiTM attack

TCAP Begin

InsertSubscriberData_REQ

DeleteSubscriberData_REQ



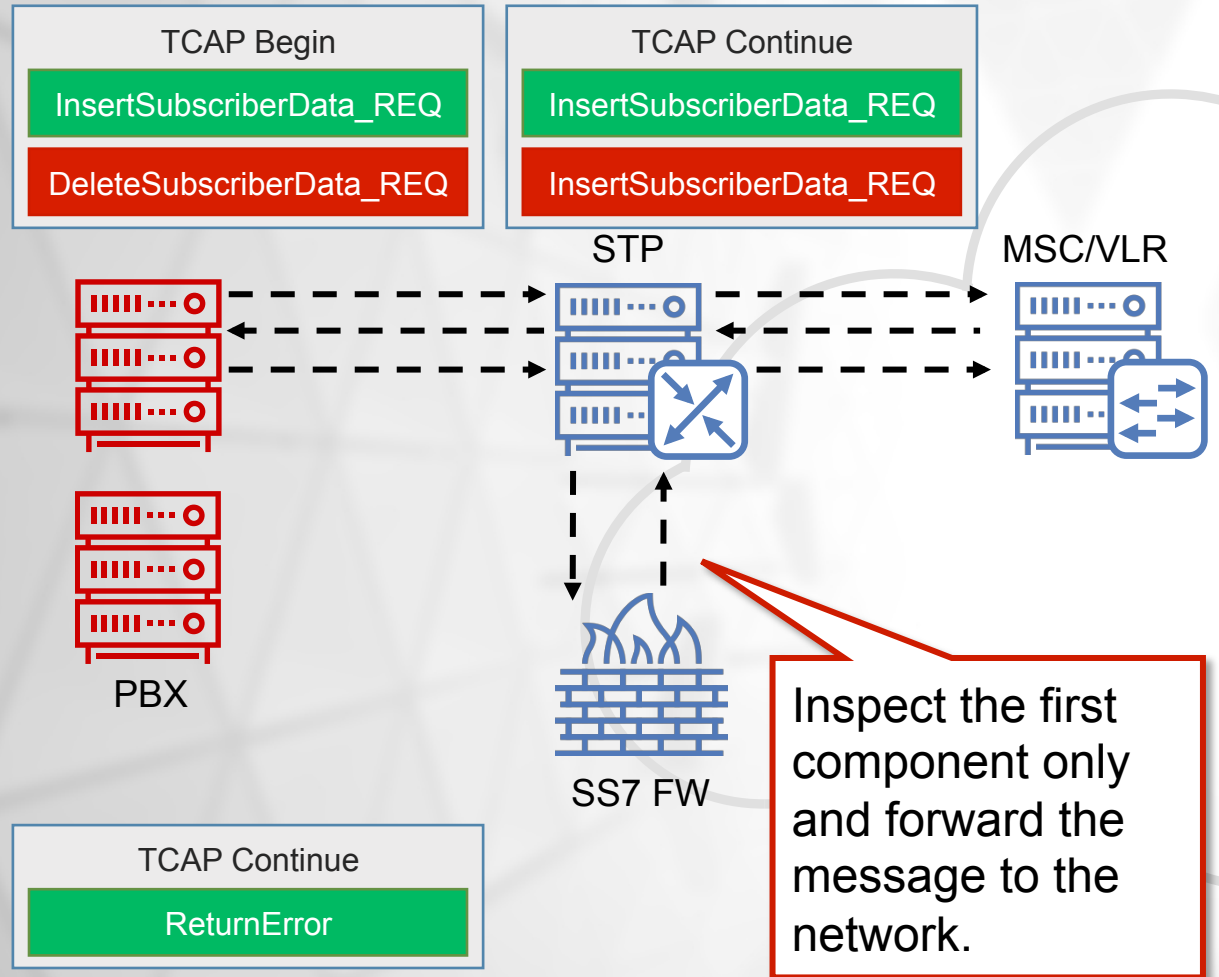
TCAP Continue

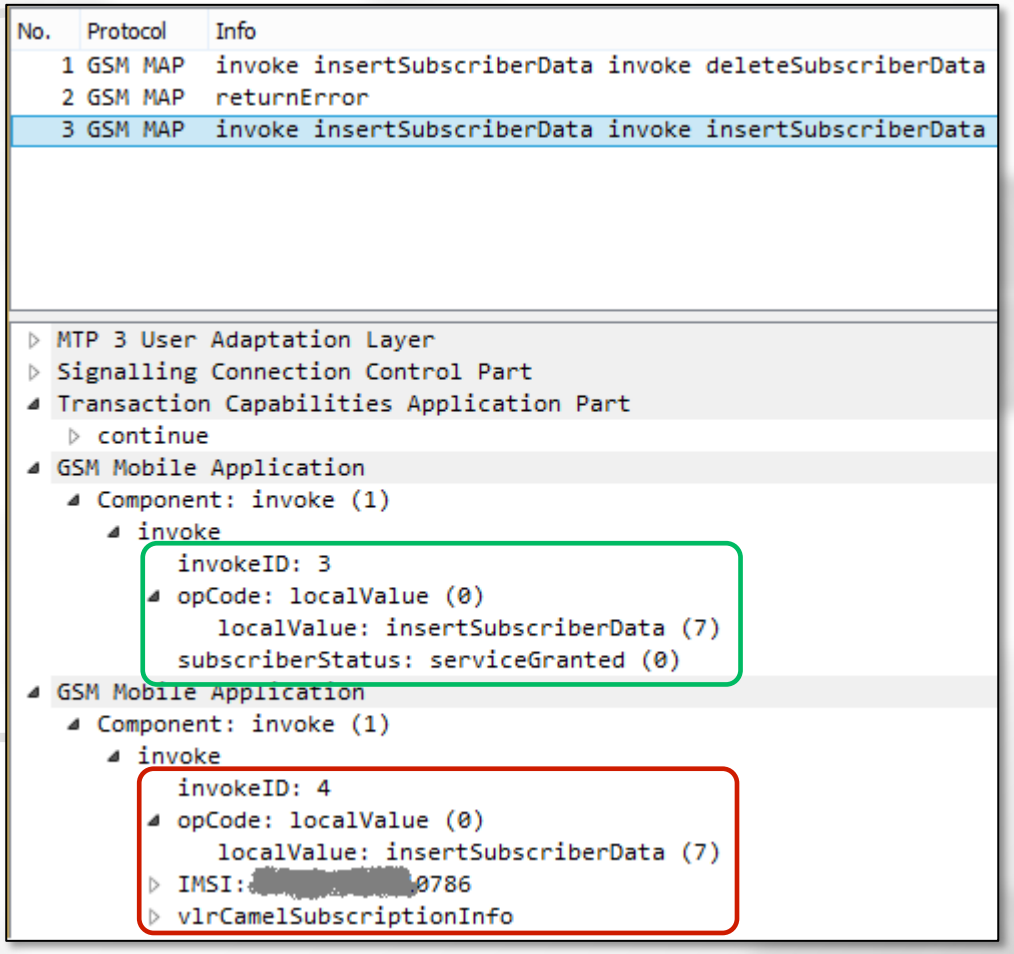
ReturnError

No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData invoke deleteSubscriberData
2	GSM MAP	returnError

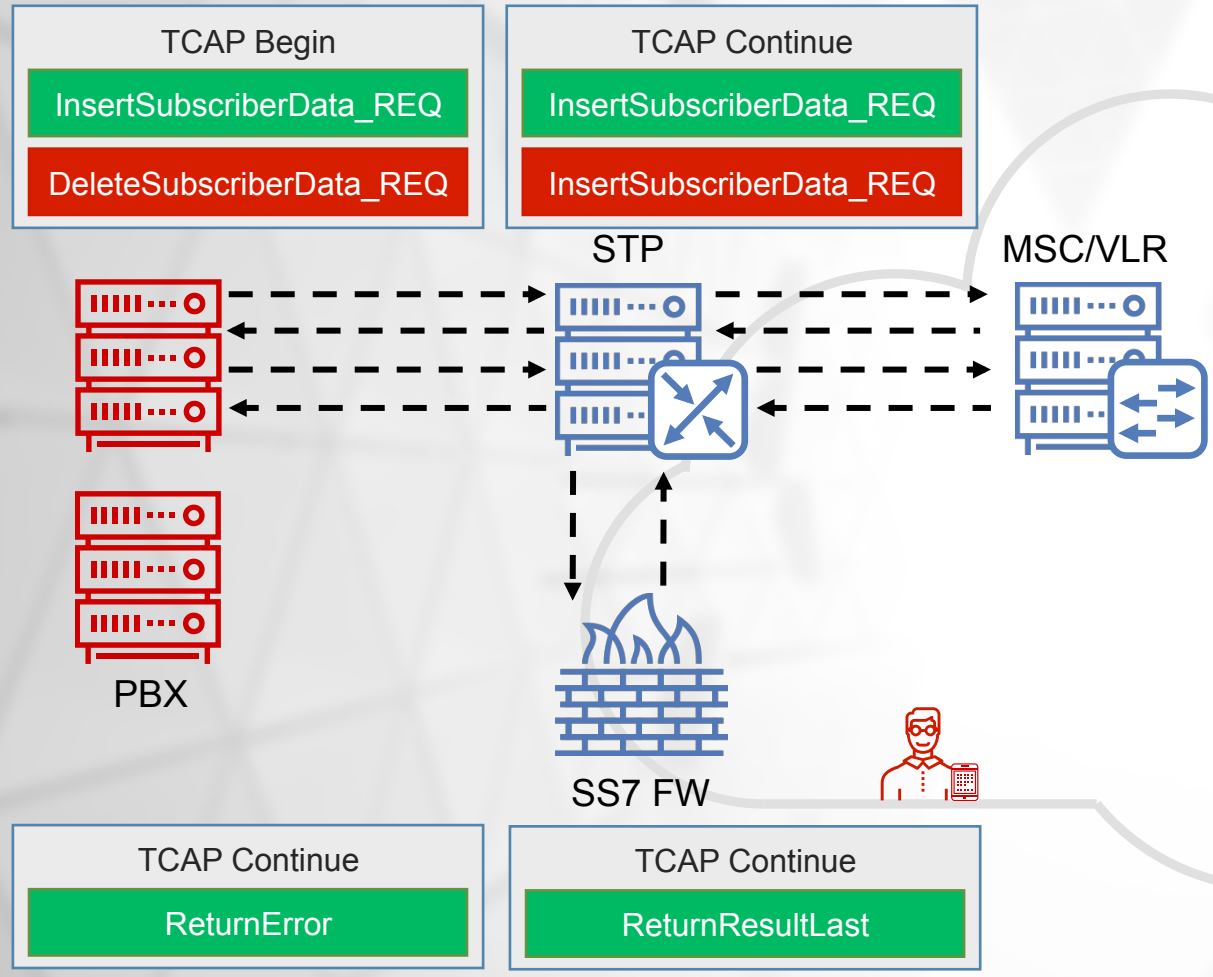
```
▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ▷ continue
◢ GSM Mobile Application
   ◢ Component: returnError (3)
      ◢ returnError
           invokeID: 1
         ▷ errorCode: localValue (0)
```

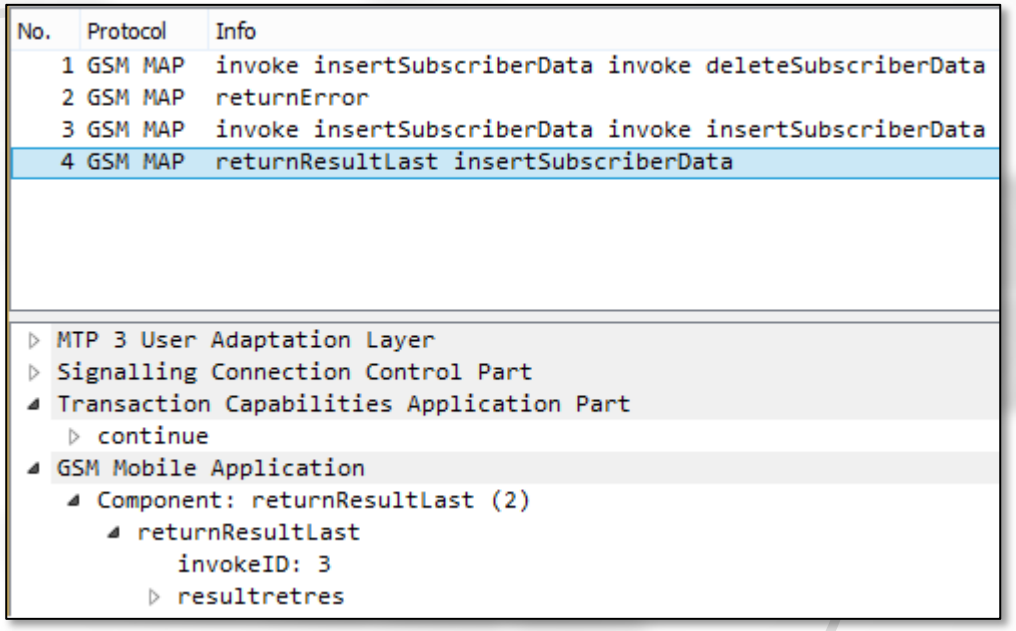
Double MAP in MiTM attack



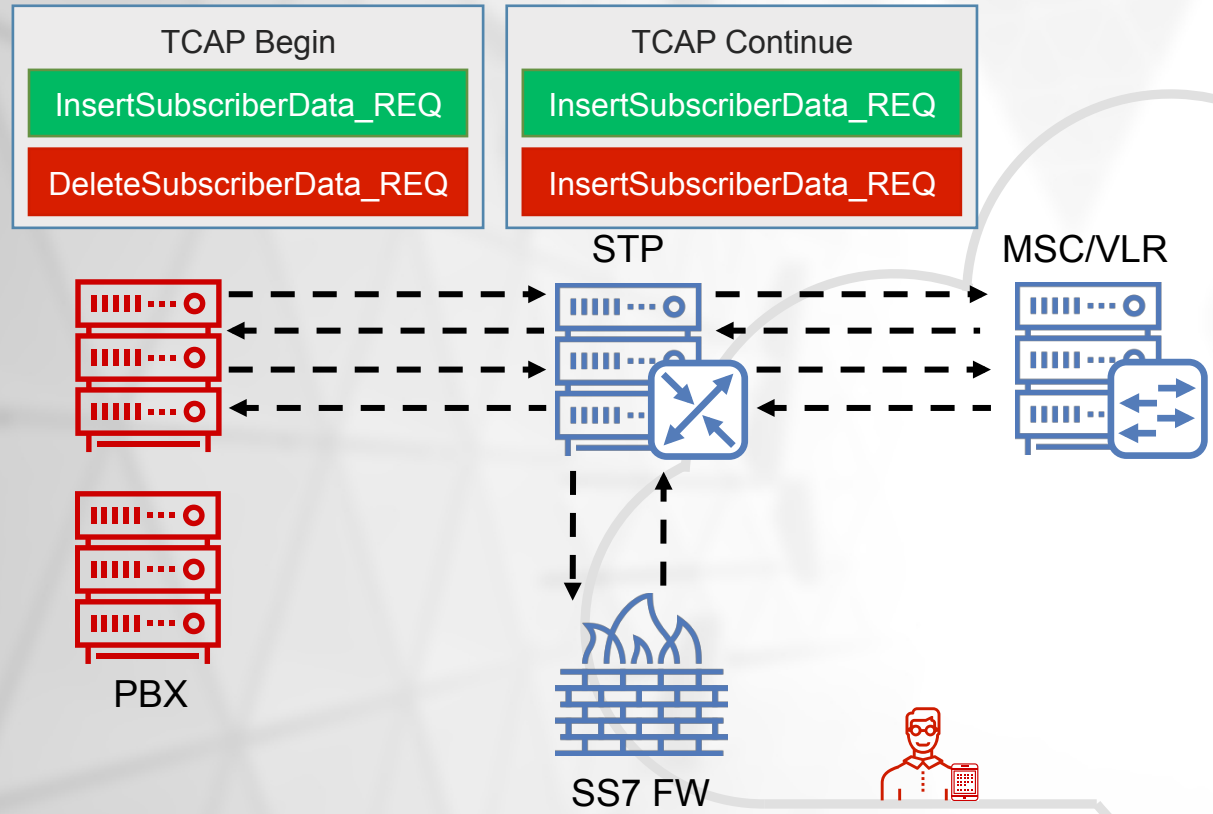


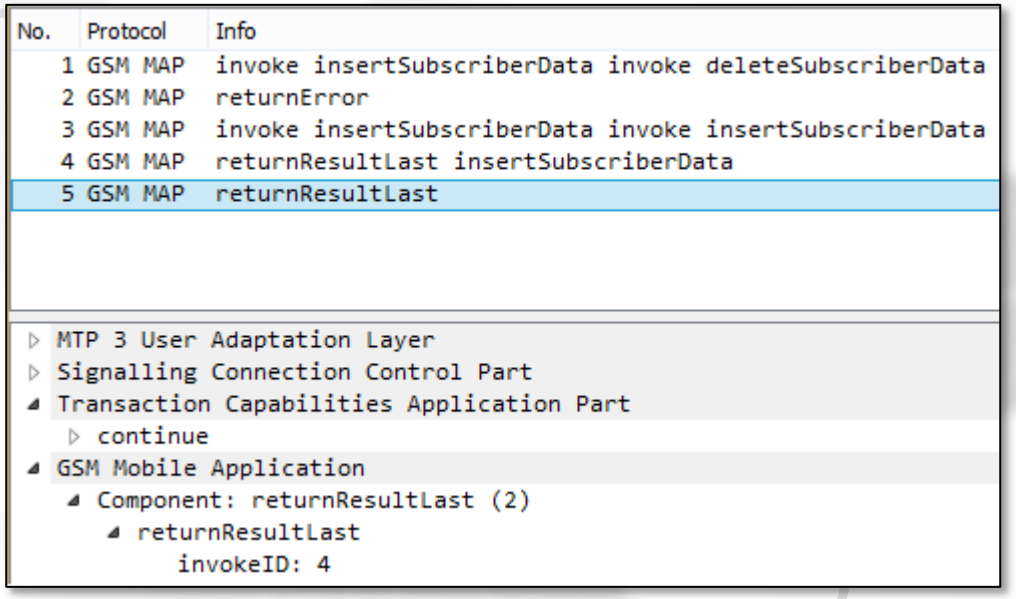
Double MAP in MiTM attack



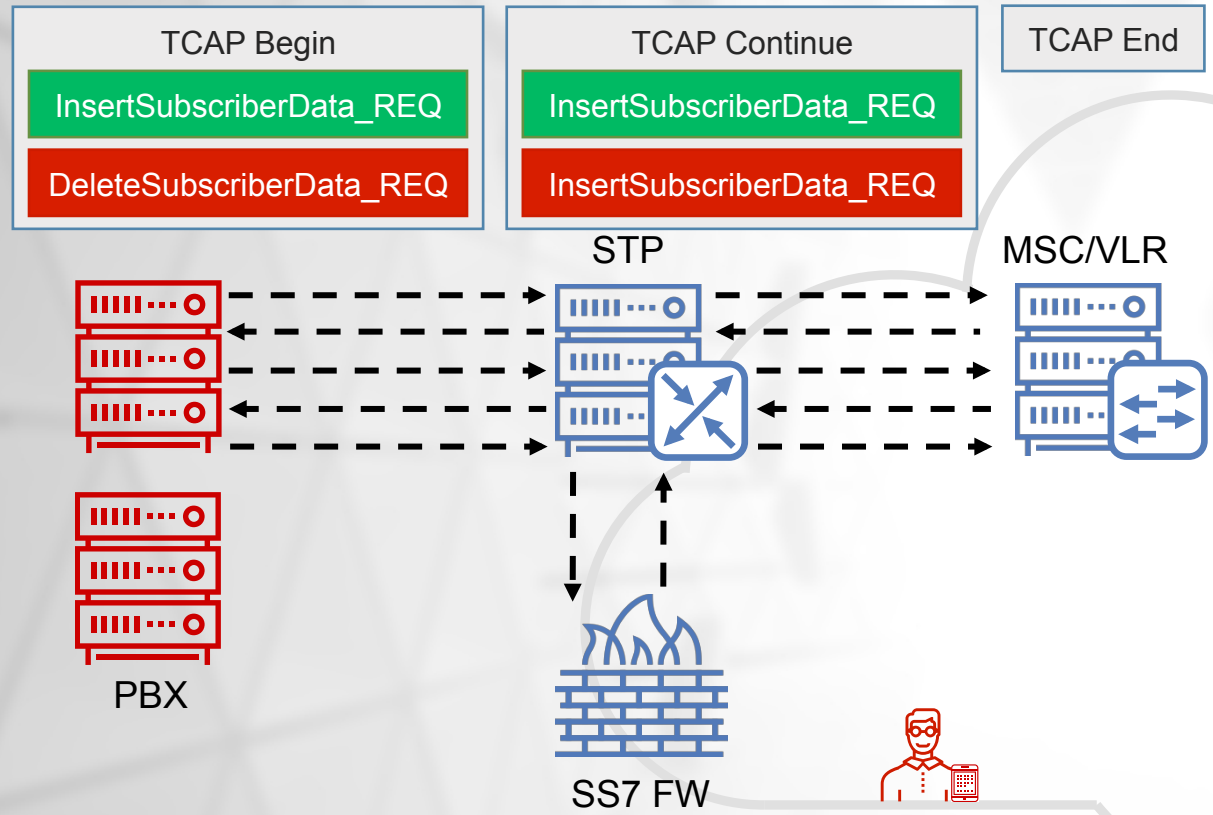


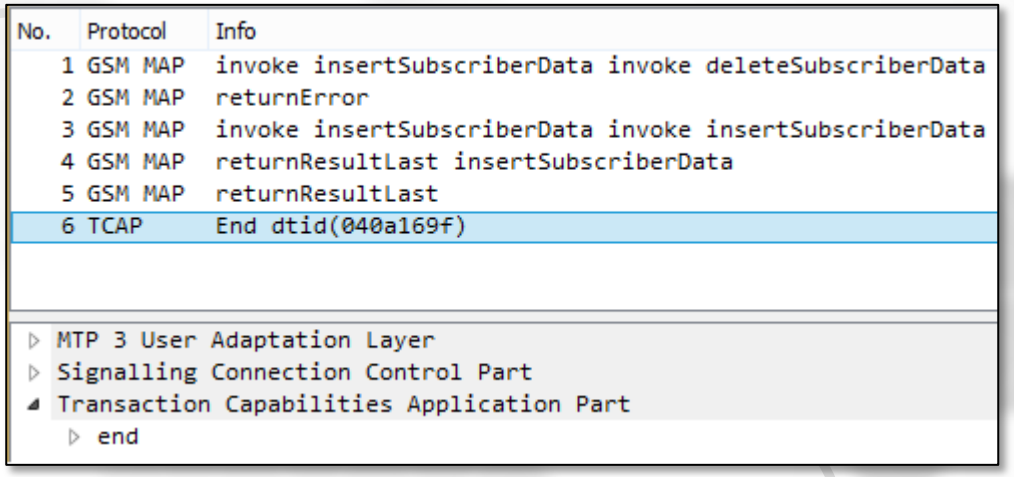
Double MAP in MiTM attack





Double MAP in MiTM attack





Double MAP in MiTM attack

TCAP Begin

InsertSubscriberData_REQ

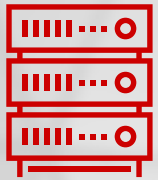
DeleteSubscriberData_REQ

TCAP Continue

InsertSubscriberData_REQ

InsertSubscriberData_REQ

TCAP End

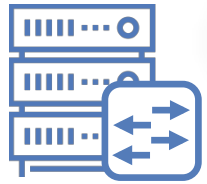


PBX

STP



MSC/VLR





SS7 FW





TCAP Continue

ReturnError

TCAP Continue

ReturnResultLast

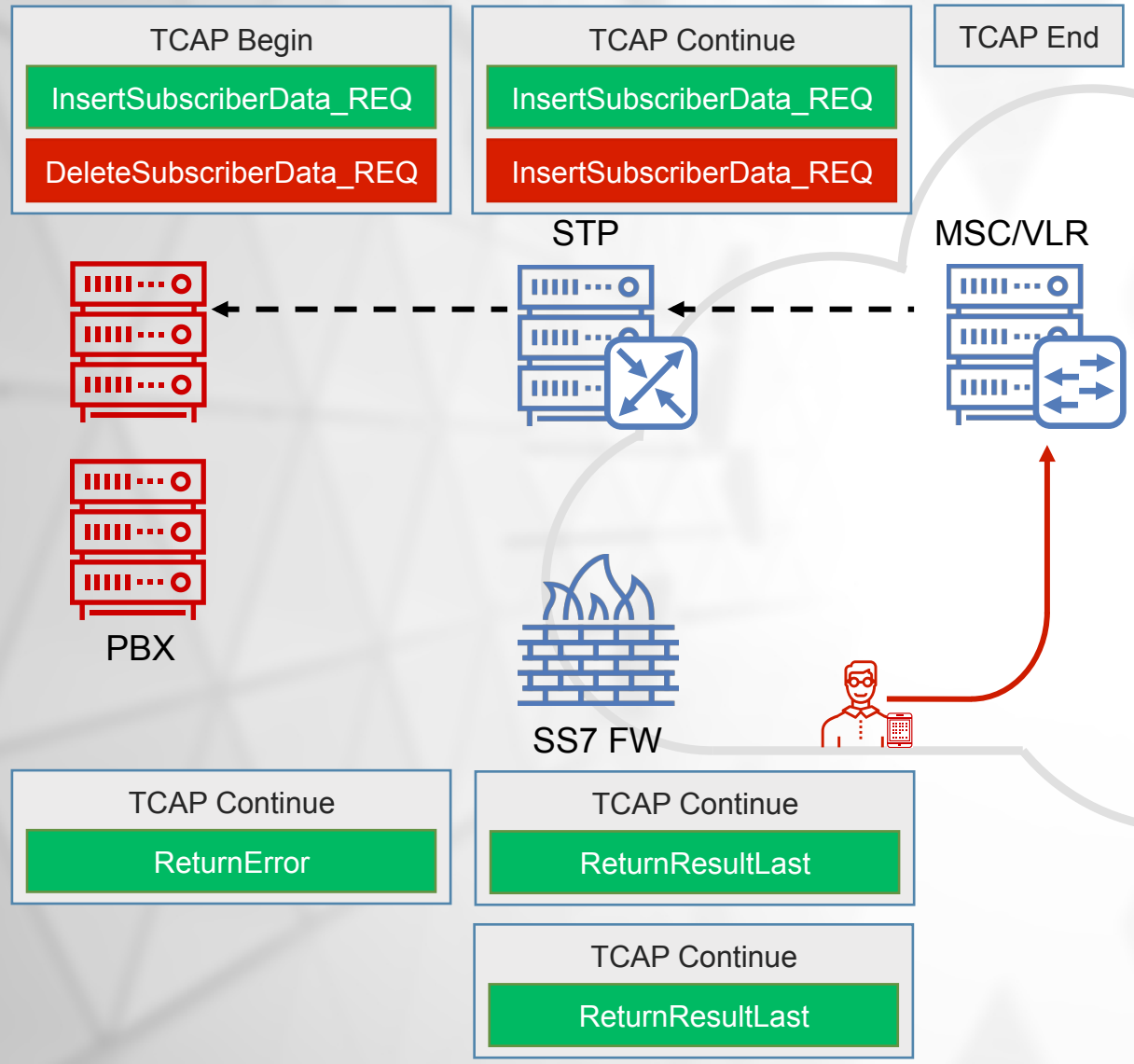
TCAP Continue

ReturnResultLast

No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData invoke deleteSubscriberData
2	GSM MAP	returnError
3	GSM MAP	invoke insertSubscriberData invoke insertSubscriberData
4	GSM MAP	returnResultLast insertSubscriberData
5	GSM MAP	returnResultLast
6	TCAP	End dtid(040a169f)

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
▷ end

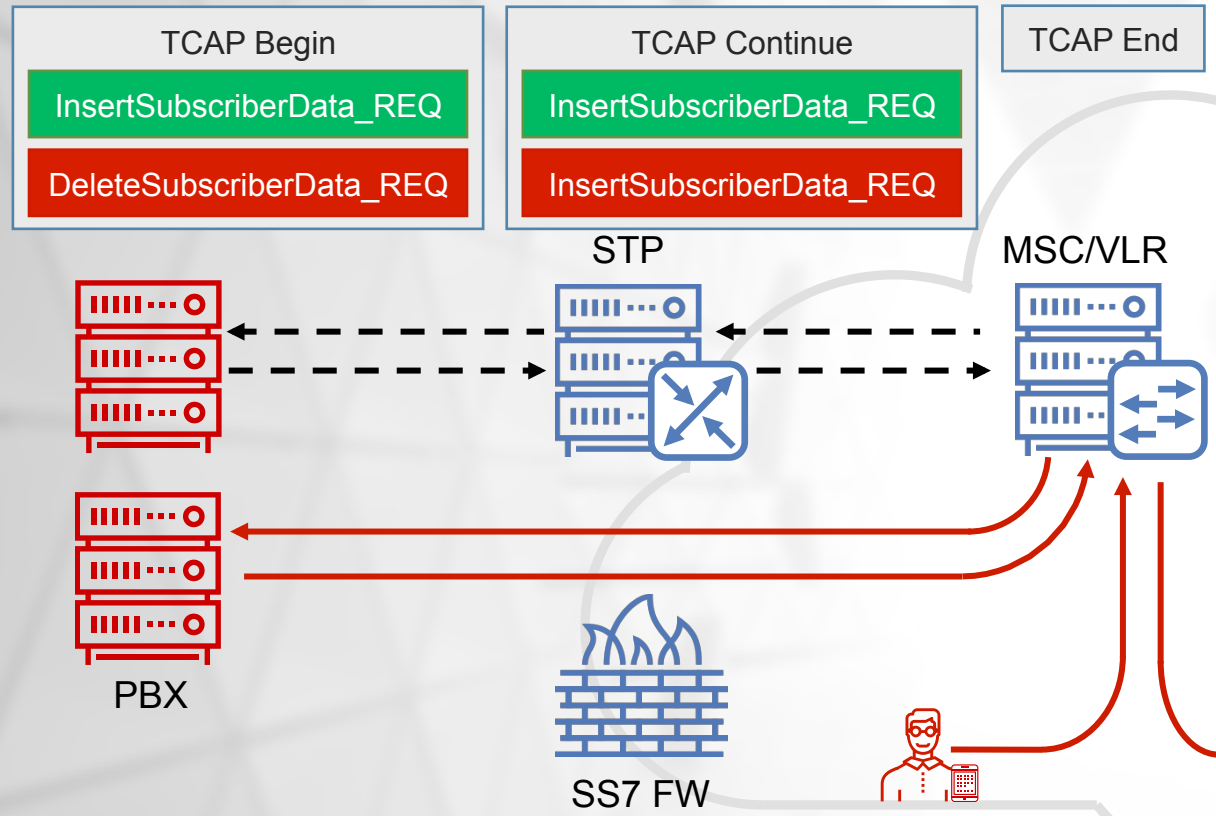
Double MAP in MiTM attack




```
No.  Protocol  Info
    1 GSM MAP  invoke insertSubscriberData invoke deleteSubscriberData
    2 GSM MAP  returnError
    3 GSM MAP  invoke insertSubscriberData invoke insertSubscriberData
    4 GSM MAP  returnResultLast insertSubscriberData
    5 GSM MAP  returnResultLast
    6 TCAP     End dtid(040a169f)
    7 Camel-v2 invoke initialDP

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ▷ begin
◢ Camel-V2
  ◢ invoke
    ▷ invokeId: present (0)
    ▷ opcode: local (0)
    ◢ InitialDPArg
        serviceKey: 1
      ▷ callingPartyNumber:[redacted]8993
        callingPartysCategory: operator, language English (2)
      ▷ locationNumber:
      ▷ bearerCapability: bearerCap (0)
        eventTypeBCSM: collectedInfo (2)
      ▷ IMSI:[redacted]0786
```

Double MAP in MiTM attack



No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData invoke deleteSubscriberData
2	GSM MAP	returnError
3	GSM MAP	invoke insertSubscriberData invoke insertSubscriberData
4	GSM MAP	returnResultLast insertSubscriberData
5	GSM MAP	returnResultLast
6	TCAP	End dtid(040a169f)
7	Camel-v2	invoke initialDP
8	Camel-v2	invoke connect

```
▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ▷ end
◢ Camel-V2
  ◢ invoke
    ▷ invokeId: present (0)
    ▷ opcode: local (0)
    ◢ ConnectArg
      ◢ destinationRoutingAddress: 1 item
        ▷ CalledPartyNumber: [redacted]102
```

Main issues in SS7 security

SS7 architecture flaws

Configuration mistakes

Software bugs

Conclusion

1. Check if your security tools are effective against new vulnerabilities.

2. Use an intrusion detection solution alone with an SS7 firewall in order to detect threats promptly and block a hostile source.

3. Block TCAP Begin messages with double MAP components.
   We observed only one legal pair:
   BeginSubscriberActivity + ProcessUnstructuredSS-Data.

4. Configure your STP and SS7 firewall carefully. Do not forget about malformed Application Context Name and Global OpCodes.

Thank you!

Sergey Puzankov for 

spuzankov@ptsecurity.com

POSITIVE TECHNOLOGIES