:: Positive Technologies

Back to the future

Cross-protocol attacks in the era of 5G

Sergey Puzankov

About the team

Sergey Mashukov
sergey.mashukov@positive-tech.com

The main point of interest is the security of the Diameter protocol. Sergey performs Diameter security audits for international MNOs and conducts research on the protocol weaknesses. Sergey is also the general developer of the Telecom Vulnerability Scanner tool and member of the Telecom Attack Discovery development team.

Alexander Onegov
alexandr.onegov@positive-tech.com

Alexander researched both SS7 and Diameter signaling protocols from security point of view and developed algorithms for an intrusion detection system. He also performs security assessments for mobile operators and conducts research on the network vulnerabilities.

Pavel Novikov
pavel.novikov@positive-tech.com

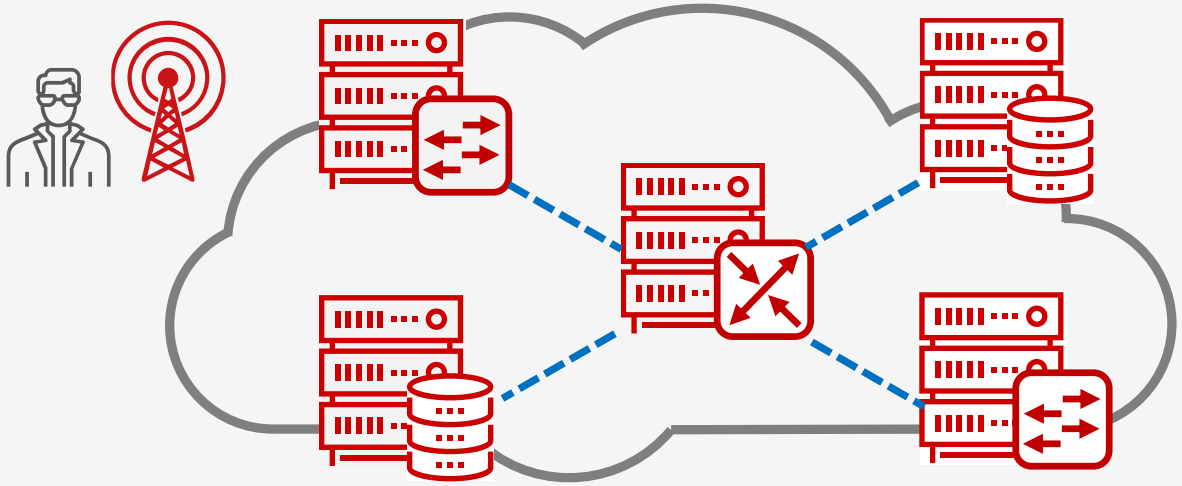
Pavel researches GTP and Diameter protocols, security issues on radio part of mobile networks, and everything that is connected with IoT devices. Pavel is also active contributor to the GSMA Fraud and Security Group.

Sergey Puzankov
sergey.puzankov@positive-tech.com

Sergey conducted research of by-design vulnerabilities in SS7 networks, discovered a number of critical vulnerabilities in mobile network equipment, and showed how an intruder is able to bypass mobile operators' protection means.

Signaling 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.



Diameter is an authentication, authorization, and accounting protocol for computer networks. **RFC 5516** defines a set of IANA Diameter Command Codes to be used in new vendor-specific Diameter applications defined for the **3GPP Evolved Packet System** (EPS).

GTP (GPRS Tunneling Protocol) is a group of IP-based communications protocols used to carry general packet radio service (GPRS) within **GSM, UMTS and LTE** networks.

The basic unit in signaling is a **message**.

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**

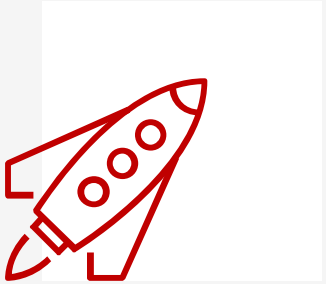
Any mobile operator

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

No special skills needed

Steal **money**

History of signaling security

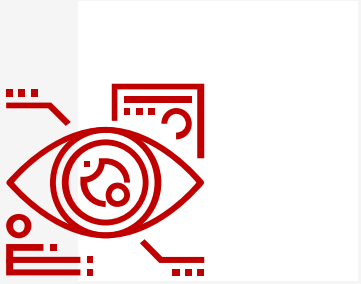


SS7 development

Trusted environment. No security mechanisms in the protocol stack. SIGTRAN (SS7 over IP) introduced. Security is still missing

Scope grows

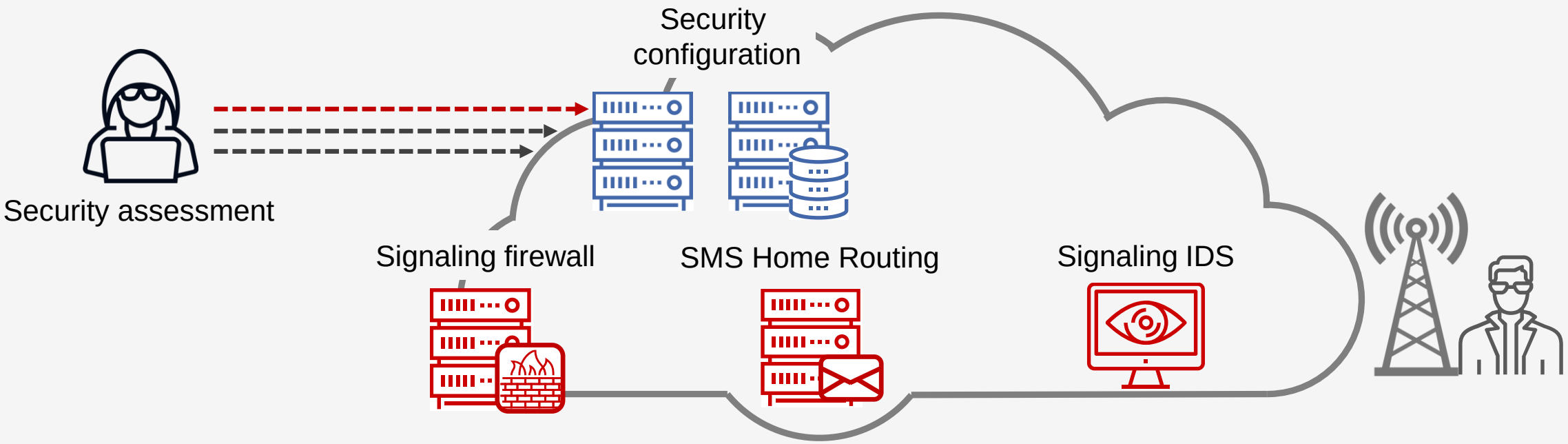
Growing number of SS7 connections, increasing amount of SS7 traffic. No security policies or restrictions



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 signaling security

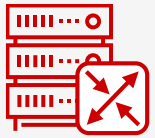


Nodes and identifiers in GSM/UMTS

MSISDN — Mobile Subscriber Integrated Services Digital Number

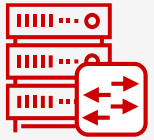
IMSI — International Mobile Subscriber Identity

GT — Global Title, address of a core node element

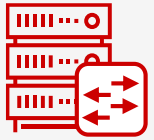


STP — Signaling Transfer Point

HLR — Home Location Register



MSC/VLR — Mobile Switching Center and Visited Location Register



SGSN — Serving GPRS Support Node

SMS-C — SMS Center

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

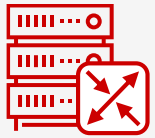
is responsible for **transactions** and **dialogues** processing.

SCCP

Signaling Connection Control Part

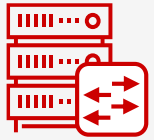
is responsible for the **routing** of a signaling message by **Global Titles**.

Nodes in LTE

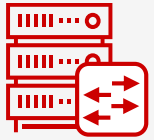


DEA — Diameter Edge Agent

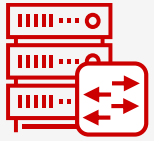
HSS — Home Subscriber Server



MME — Mobile Management Entity



SGW — Serving Gateway



IMS — IP Multimedia System

Diameter protocol stack

Diameter

Diameter
is payload that contains a **command code**, **application ID**, and appropriate **parameters** within Attribute-Value Pairs (**AVP**) blocks.

SCTP

Stream Control Transmission Protocol
is a **transport** protocol that provides some of the features of both UDP and TCP.

IP

Internet Protocol
is responsible for the node Internetworking at the Internet layer.

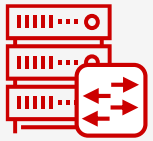
Protocol types and nodes and GTP

GTP-C is control section of the GTP standard (signaling).

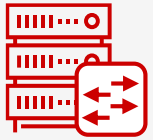
GTP-U is IP-based tunneling protocol which permits many tunnels between each set of end points.

GTP' transfers charging data.

GSM and UMTS

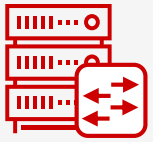


SGSN — Serving GPRS Support Node

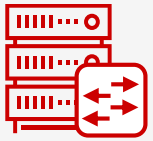


GGSN — Gateway GPRS Support Node

LTE and 5G non-SA



SGW — Serving Gateway



PGW — Public Data Network Gateway

GTP-C protocol stack

GTP-C

GPRS Tunneling Protocol Control Plane

is used within the GPRS core and EPC networks for signaling between gateway and serving packet data nodes.

UDP

User Datagram Protocol

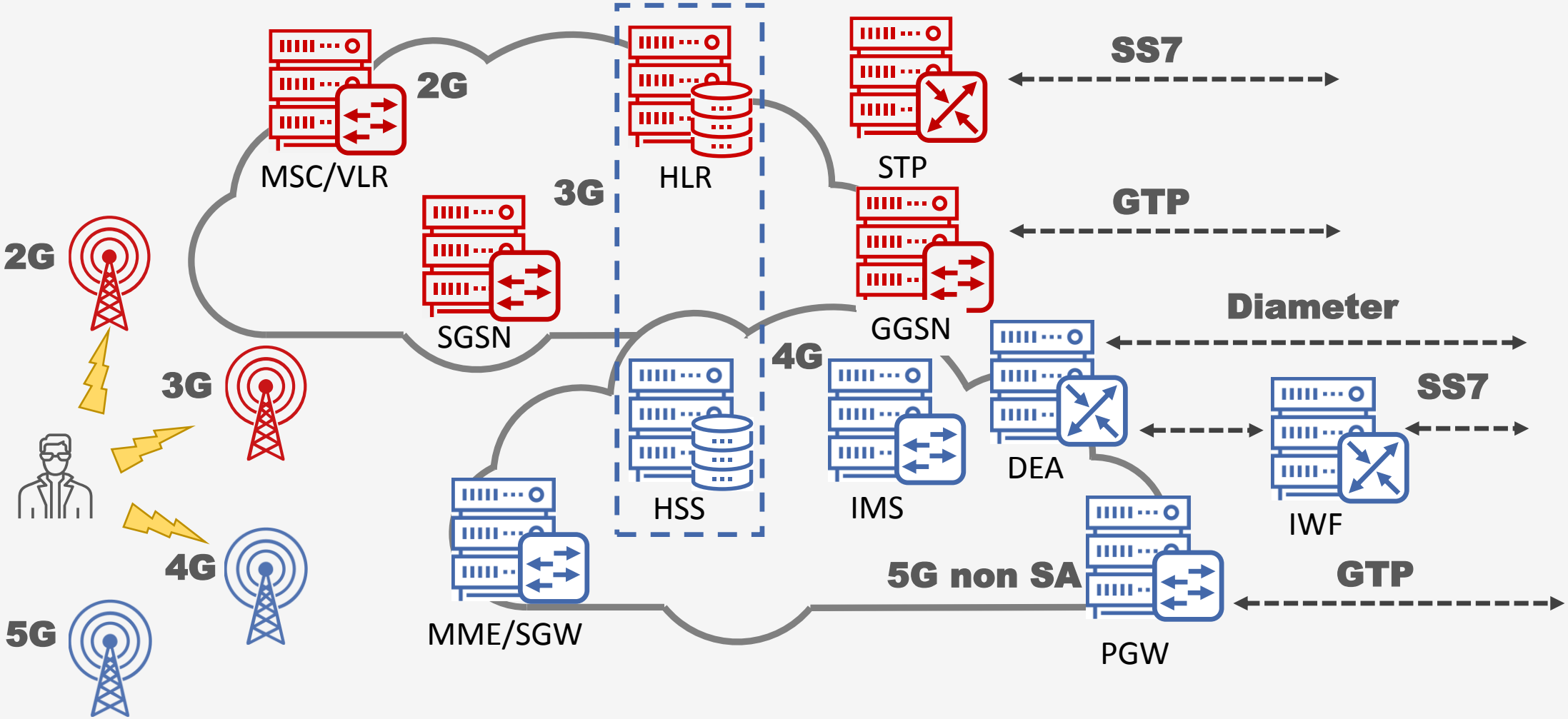
is a transport protocol for establishing **low-latency** and **loss-tolerating** connections between applications on the Internet.

IP

Internet Protocol

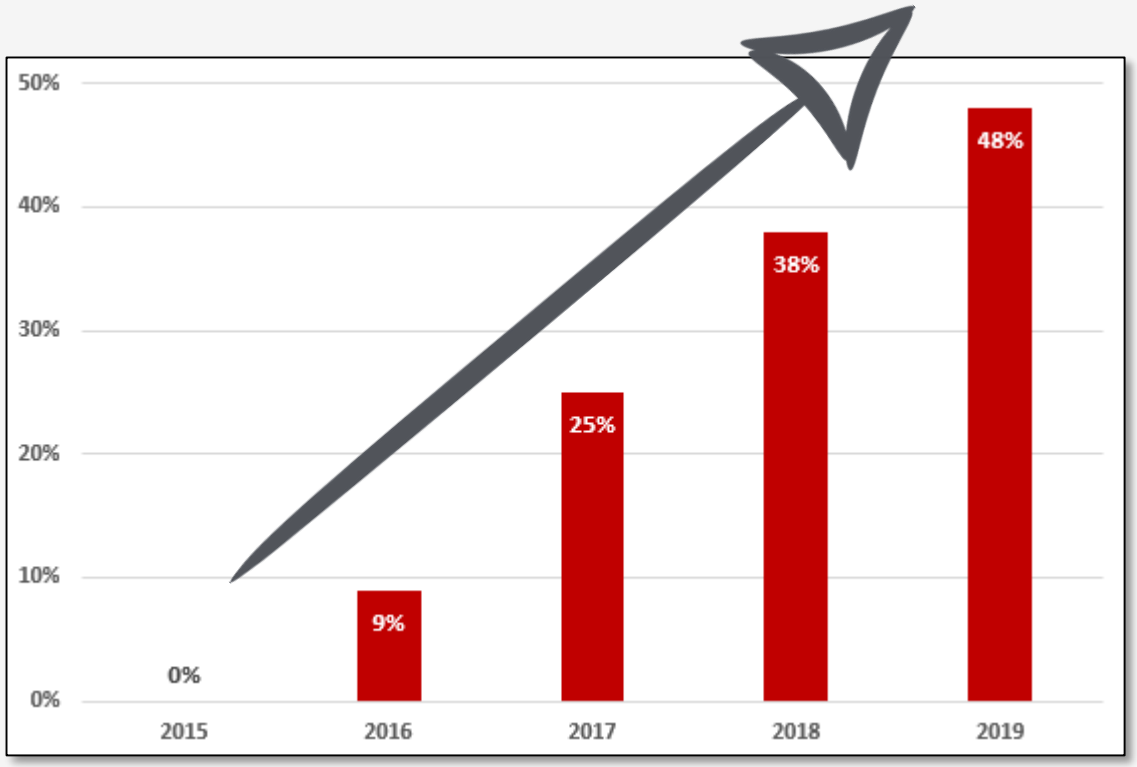
is responsible for the node internetworking at the Internet layer.

Mixed-generation network

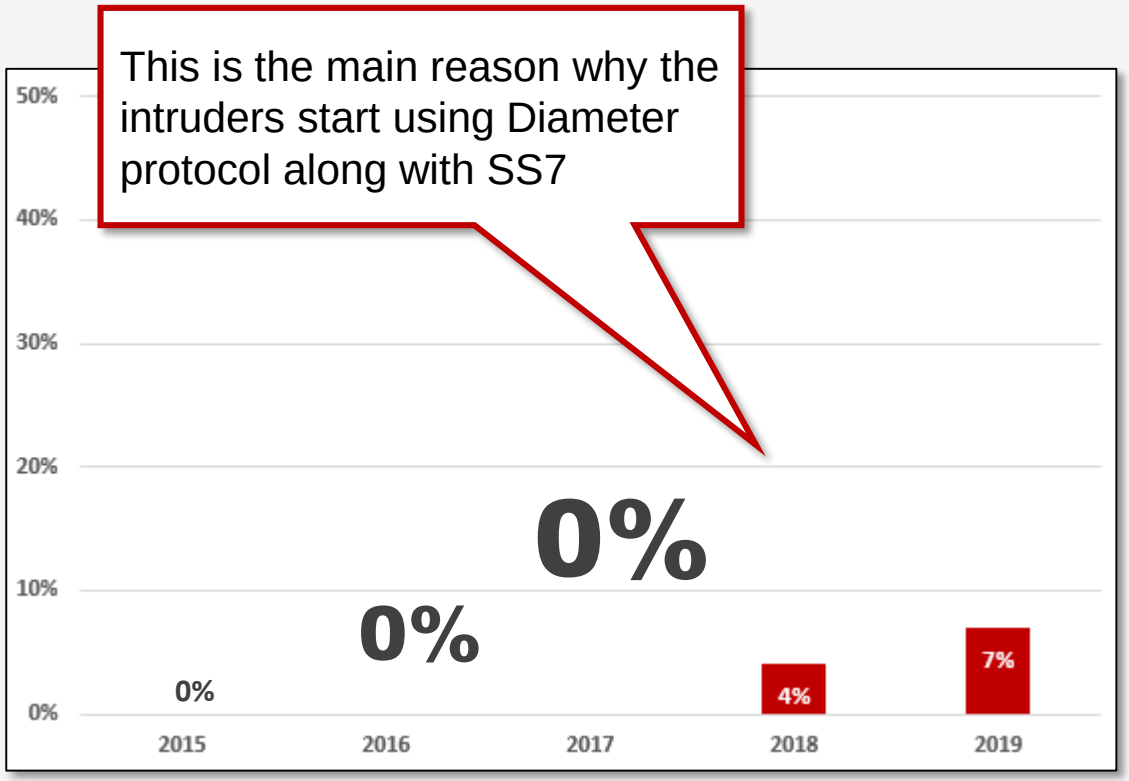


SS7 and Diameter firewall penetration*

SS7 firewall penetration growth

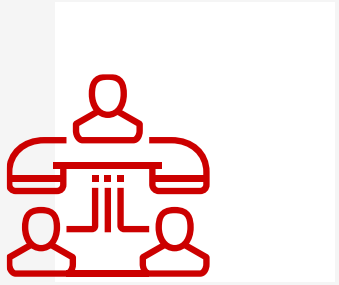


Diameter firewall penetration



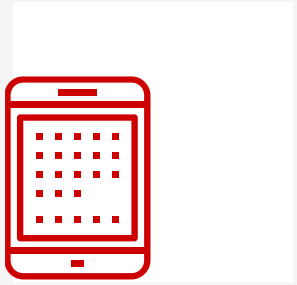
* Statistics based on Positive Technologies' SS7 and Diameter security assessment projects

Cross-protocol attacks



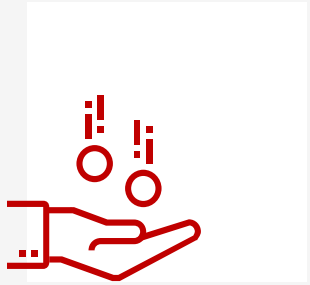
Voice call interception (MITM)

Attack via VoLTE suppression and SS7 firewall bypassing



Voice call interception (MITM)

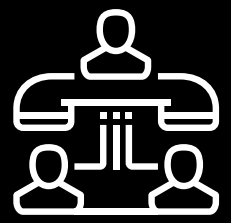
Attack via packet data service disruption



Subscription fraud

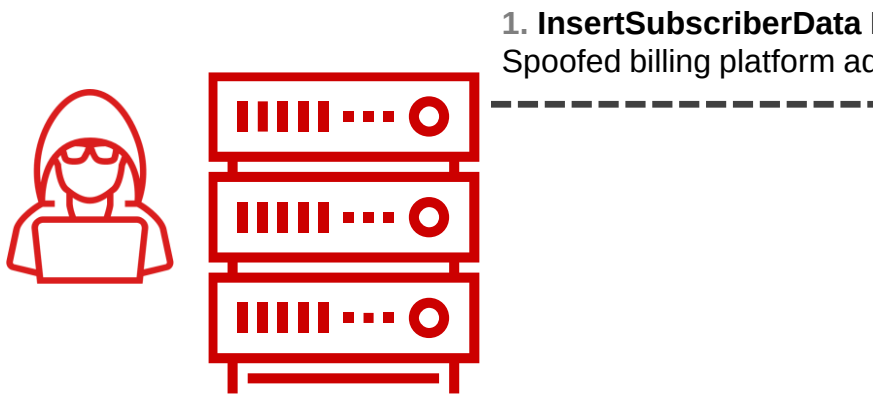
Attack on SS7 and GTP-C protocols

Voice call interception (MITM) on 2G/4G network with VoLTE



Attack via VoLTE suppression and SS7 firewall bypassing

Voice call interception (MITM)



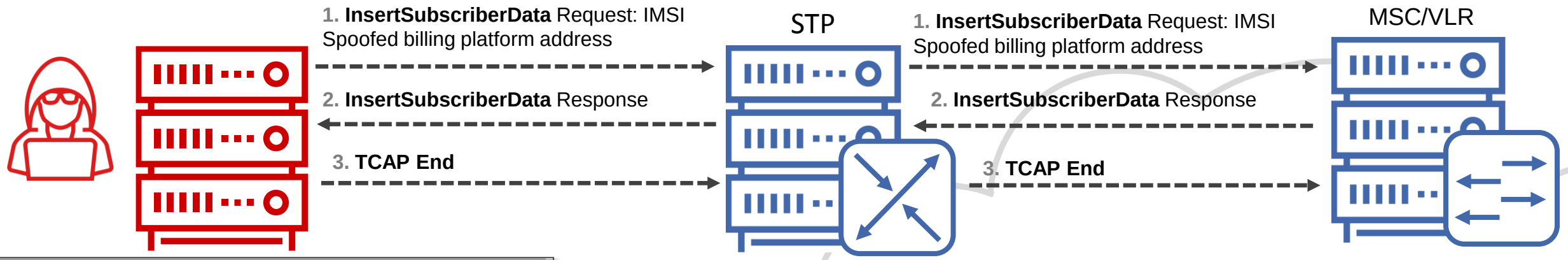
1. **InsertSubscriberData** Request: IMSI
Spoofed billing platform address

STP

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

MSC/VLR

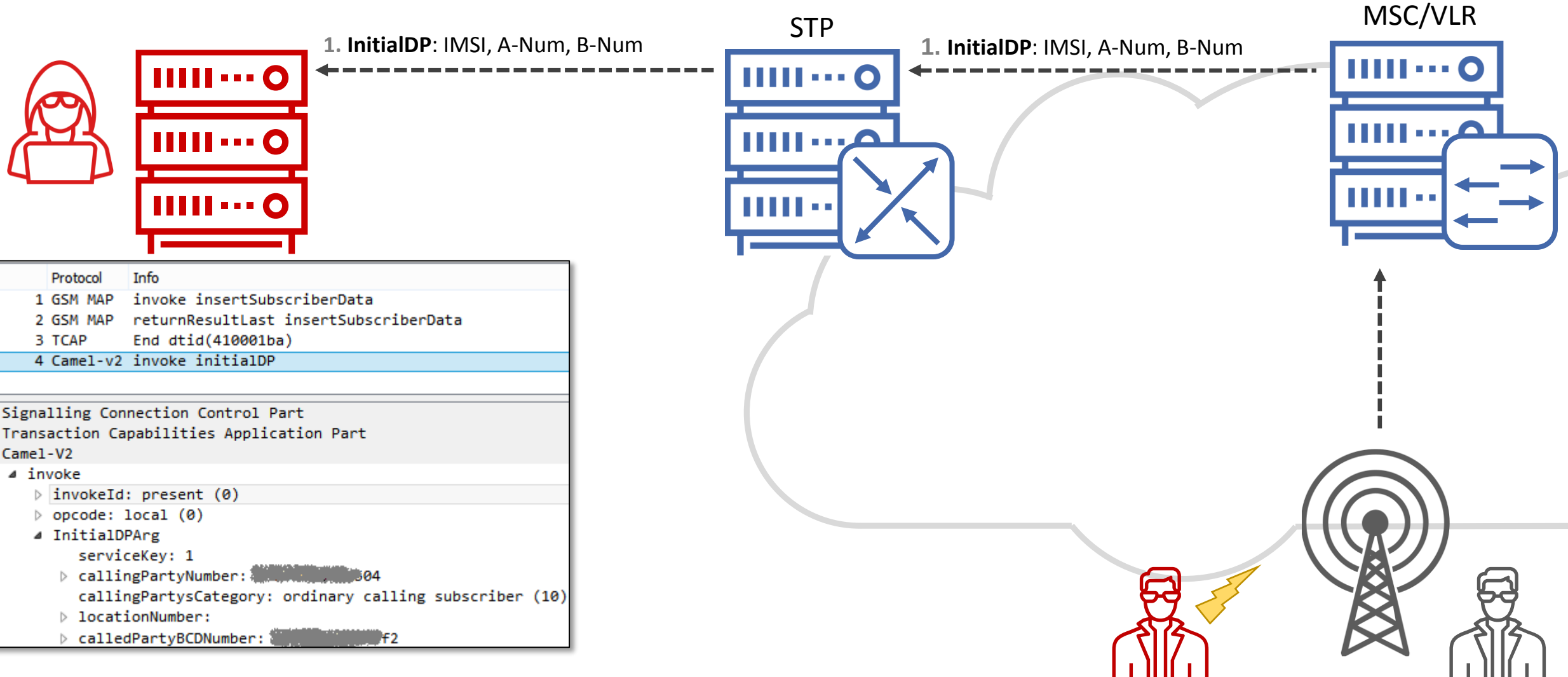
Voice call interception (MITM)



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)
```

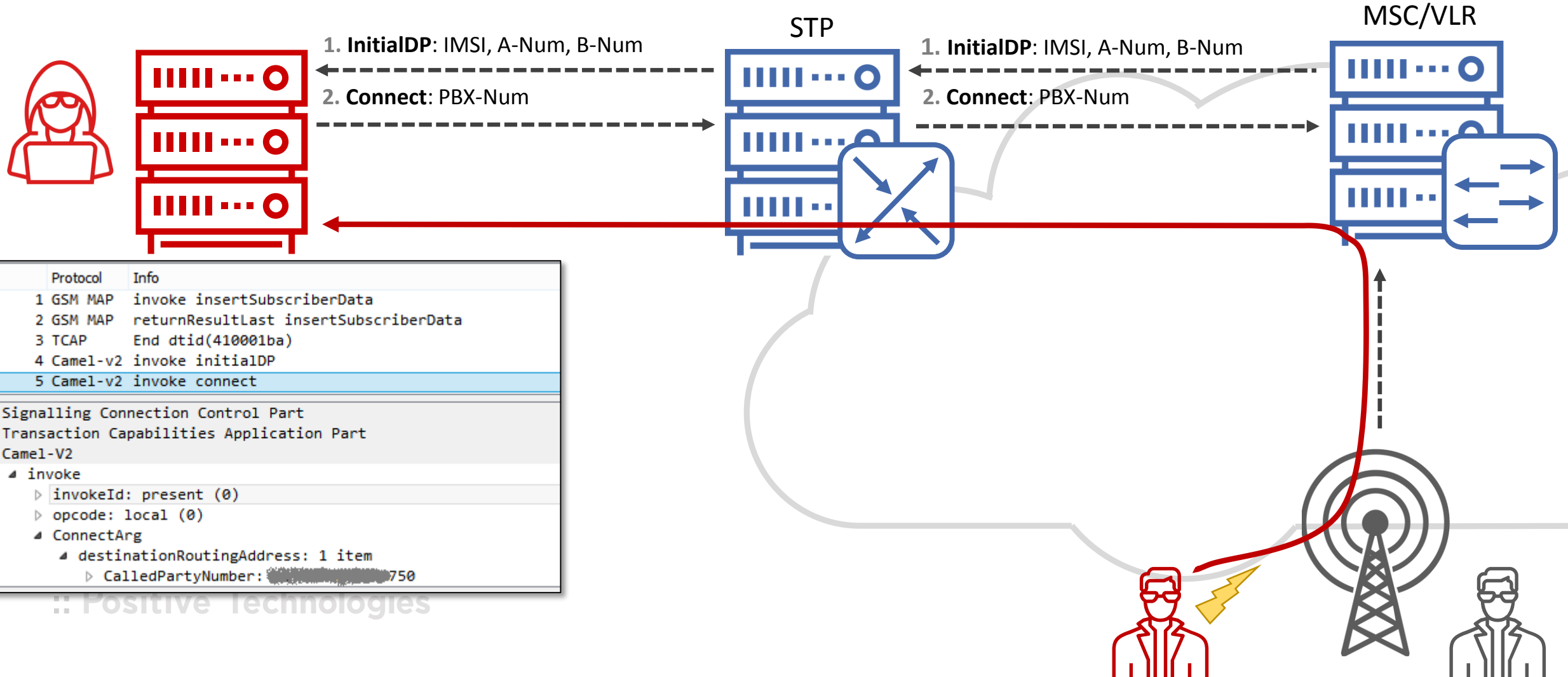
Voice call interception (MITM)



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
```

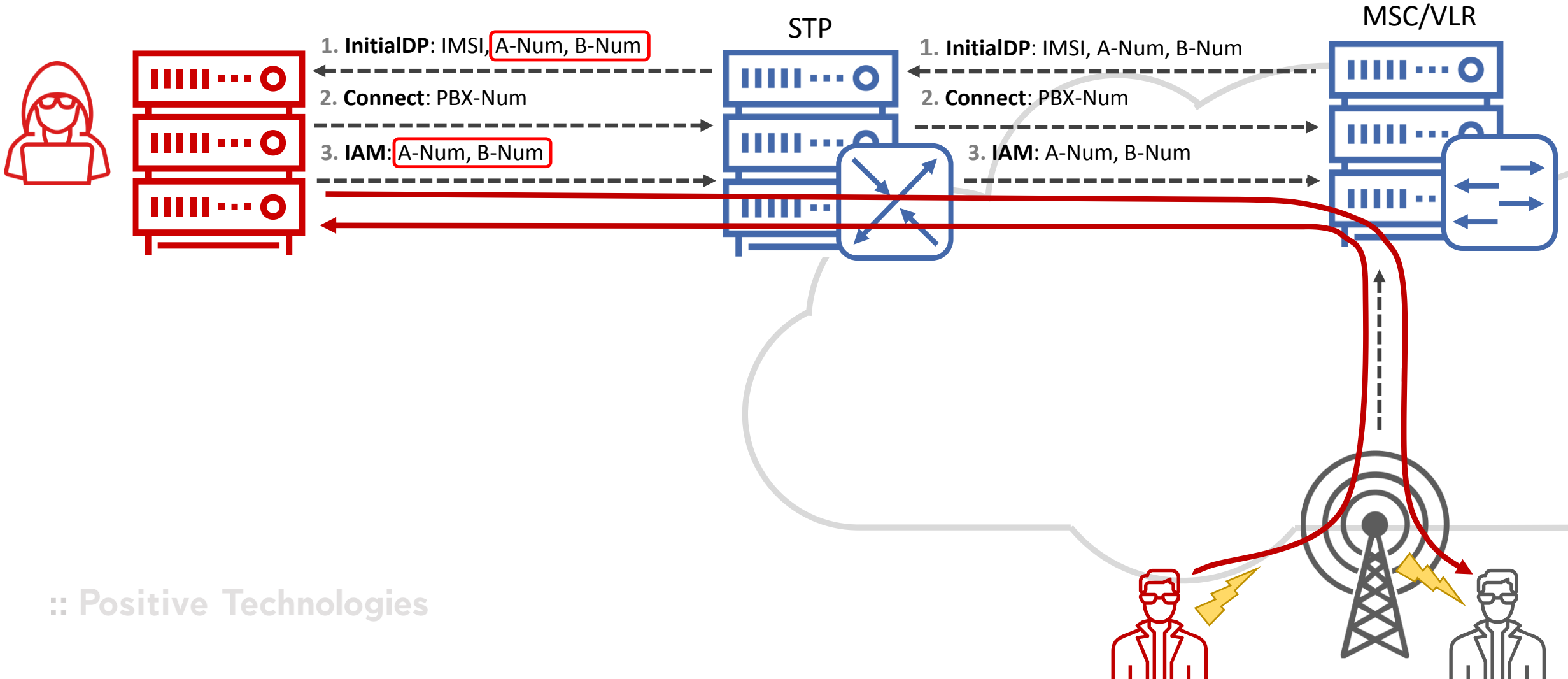
Voice call interception (MITM)



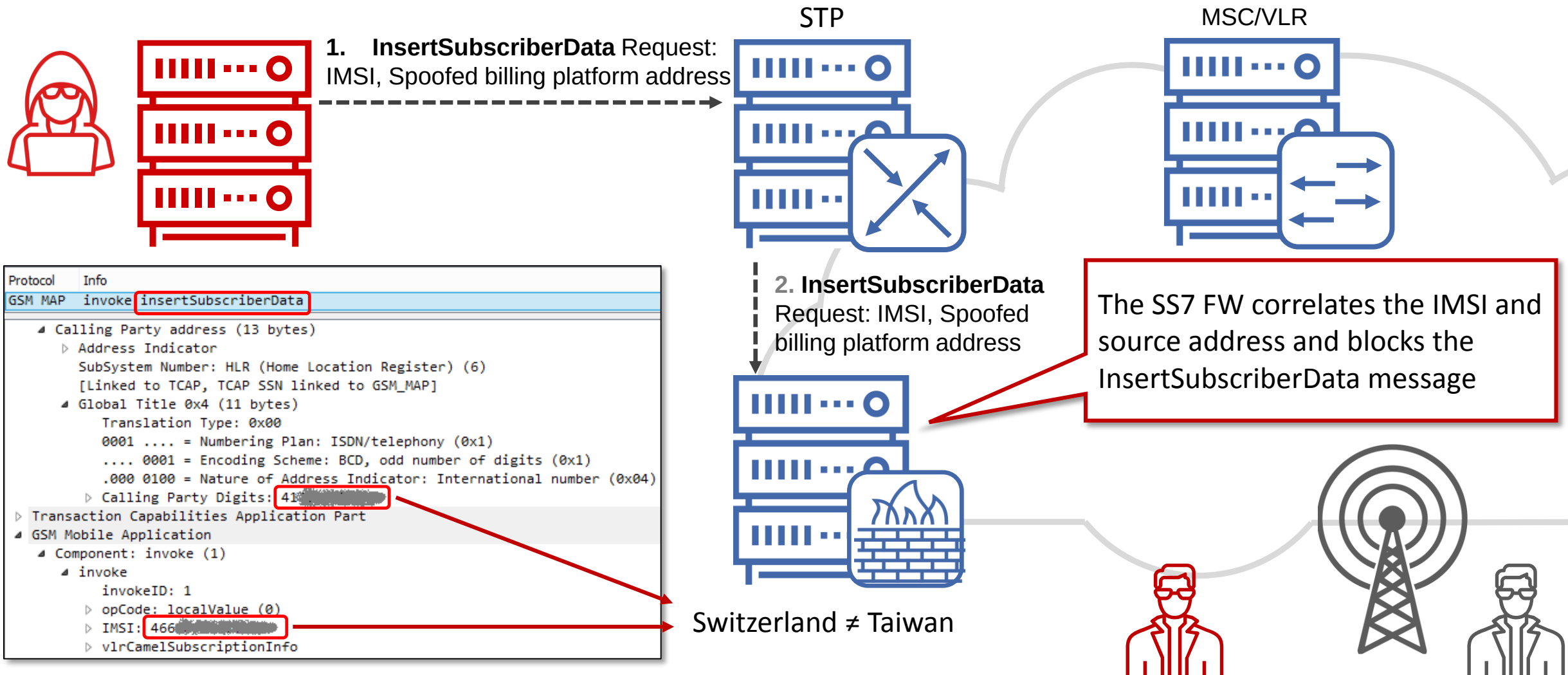
No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData
2	GSM MAP	returnResultLast insertSubscriberData
3	TCAP	End dtid(410001ba)
4	Camel-v2	invoke initialDP
5	Camel-v2	invoke connect

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

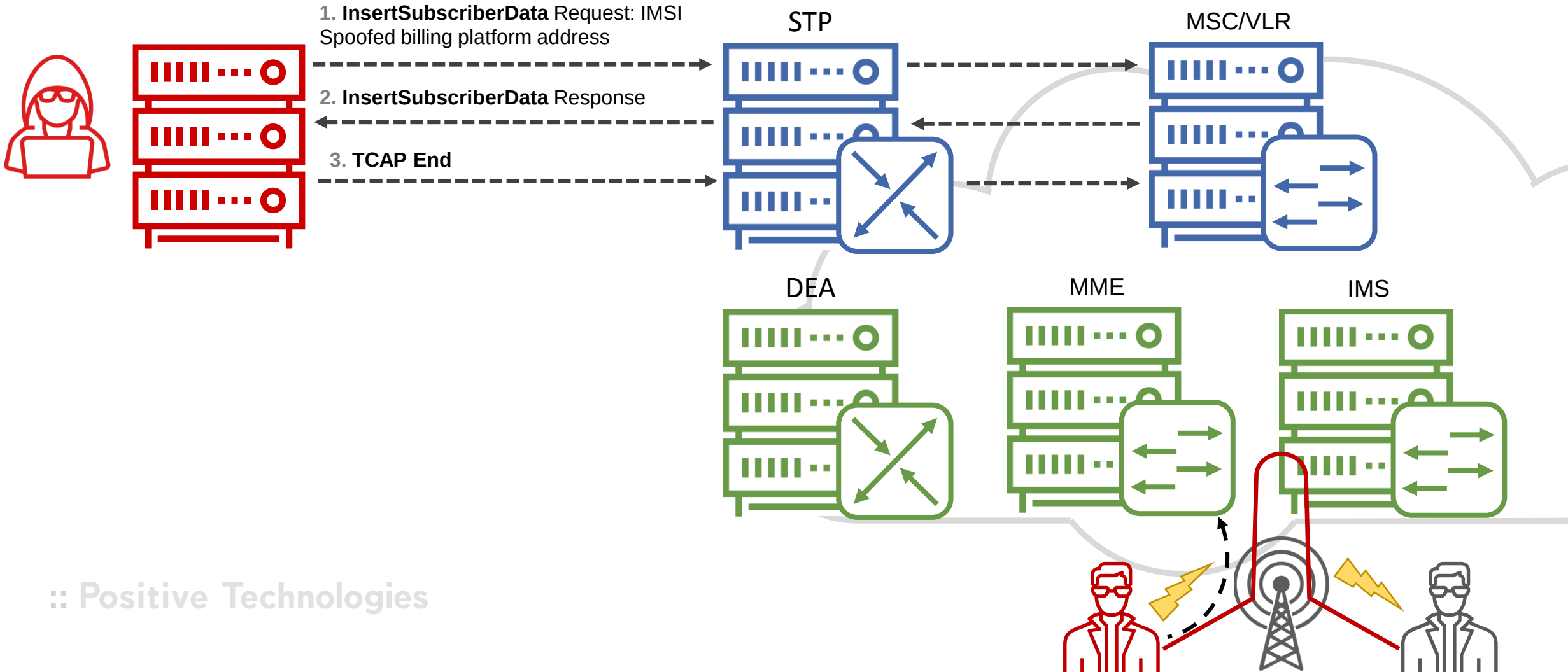
:: Voice call interception (MITM)



SS7 FW against MITM attack

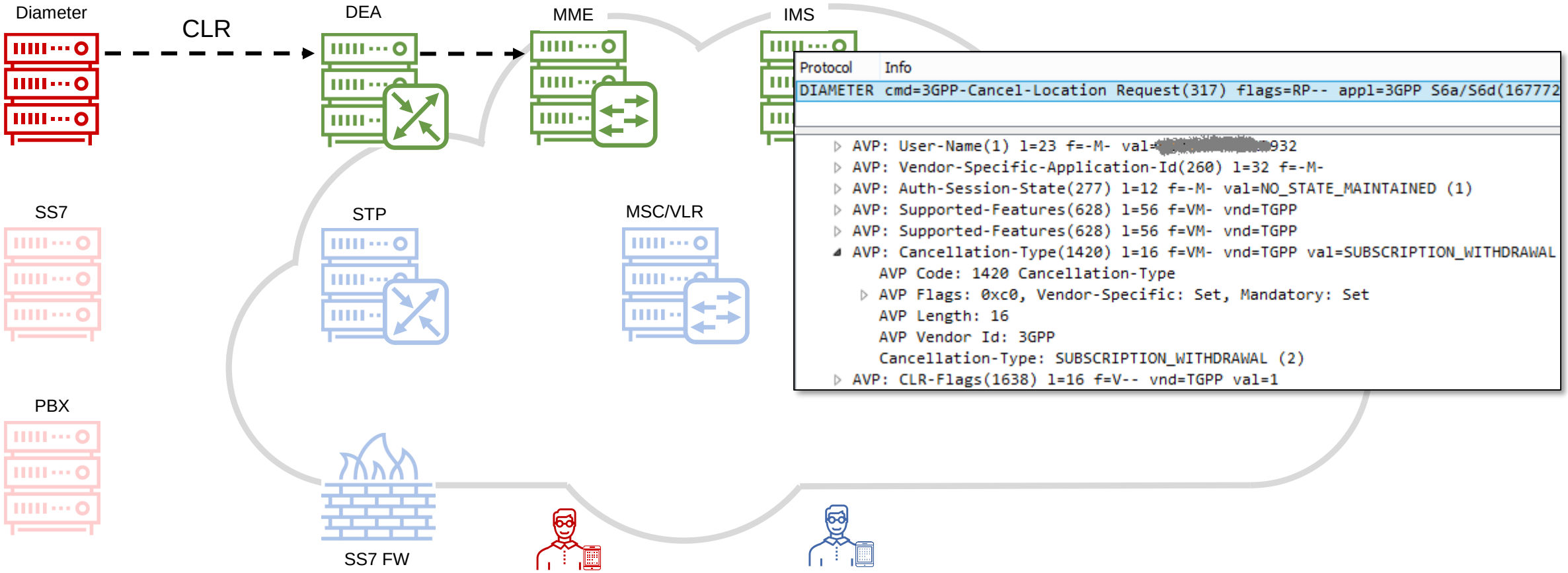


VoLTE against MITM attack



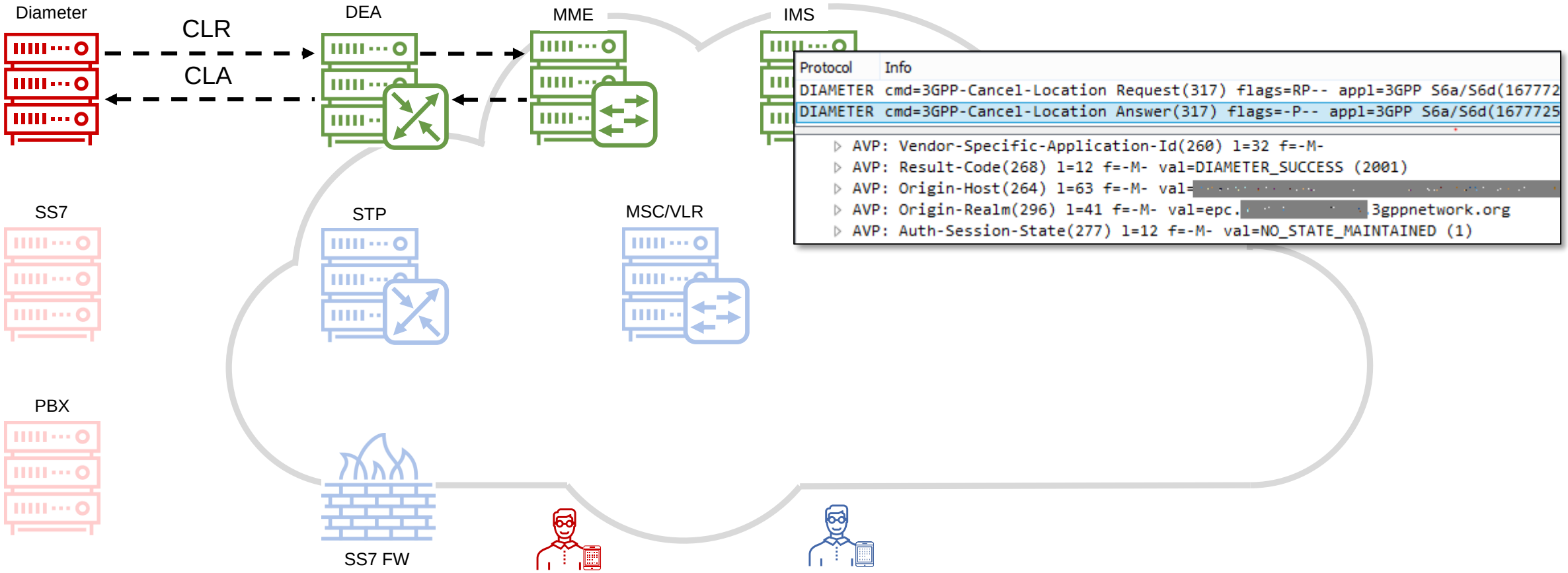
VoLTE service suppression

CLR – Cancel-Location Request



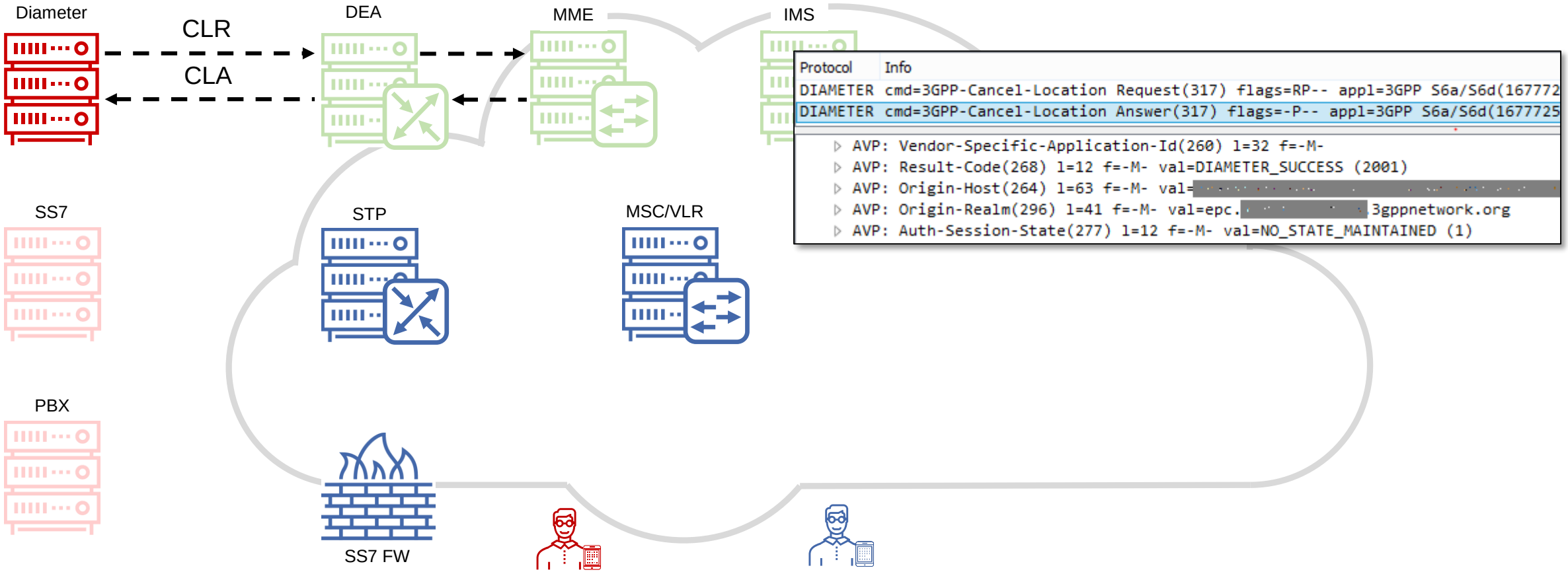
VoLTE service suppression

CLA – Cancel-Location Answer



VoLTE service suppression

CLR – Cancel-Location Answer

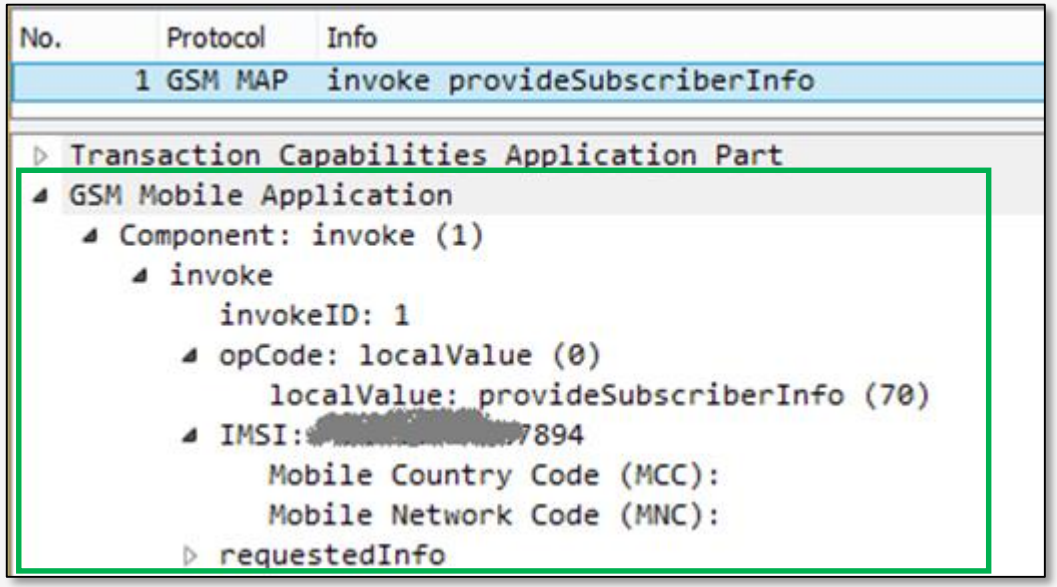


Protocol	Info
DIAMETER	cmd=3GPP-Cancel-Location Request(317) flags=RP-- appl=3GPP S6a/S6d(167772
DIAMETER	cmd=3GPP-Cancel-Location Answer(317) flags=-P-- appl=3GPP S6a/S6d(1677725

```
▷ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
▷ AVP: Result-Code(268) l=12 f=-M- val=DIAMETER_SUCCESS (2001)
▷ AVP: Origin-Host(264) l=63 f=-M- val=
▷ AVP: Origin-Realm(296) l=41 f=-M- val=epc.                3gppnetwork.org
▷ AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
```

TCAP protocol

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



Double MAP component

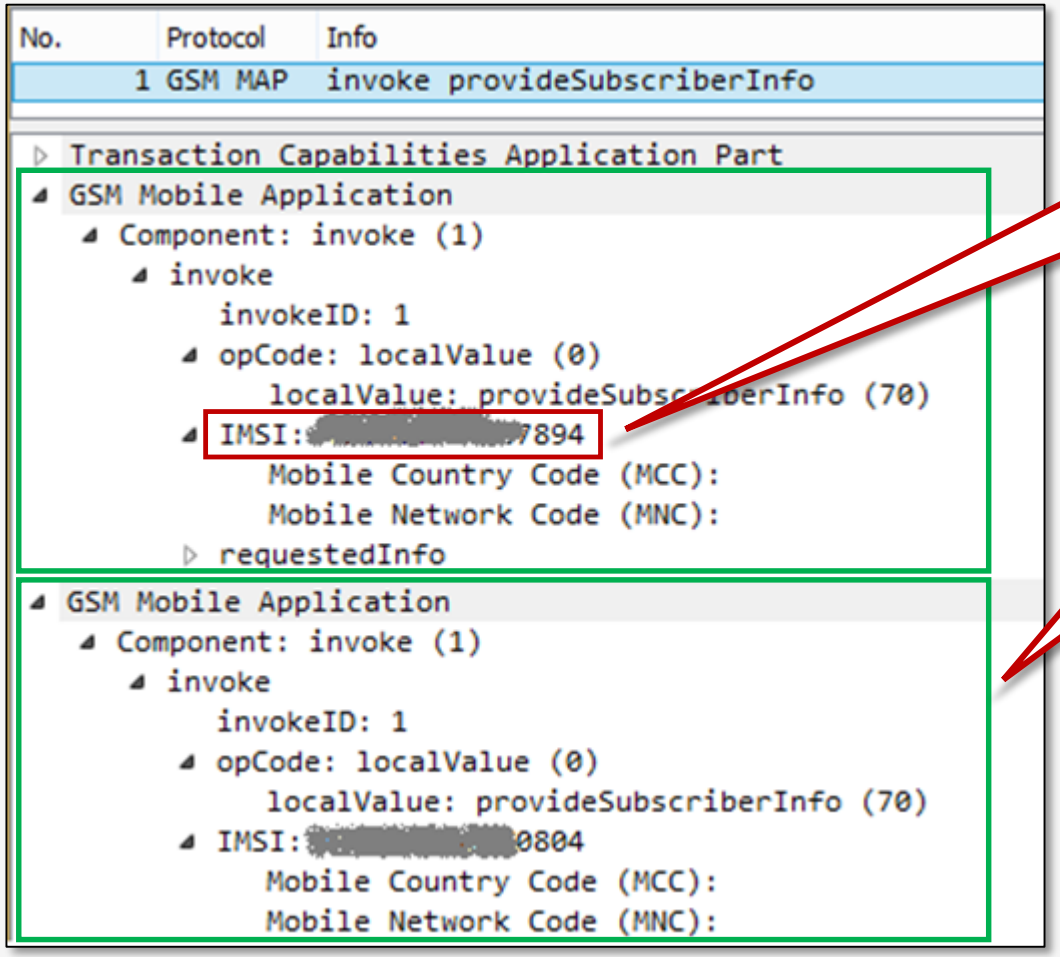
TCAP Message Type — mandatory

Transaction IDs — mandatory

Dialogue Portion — optional

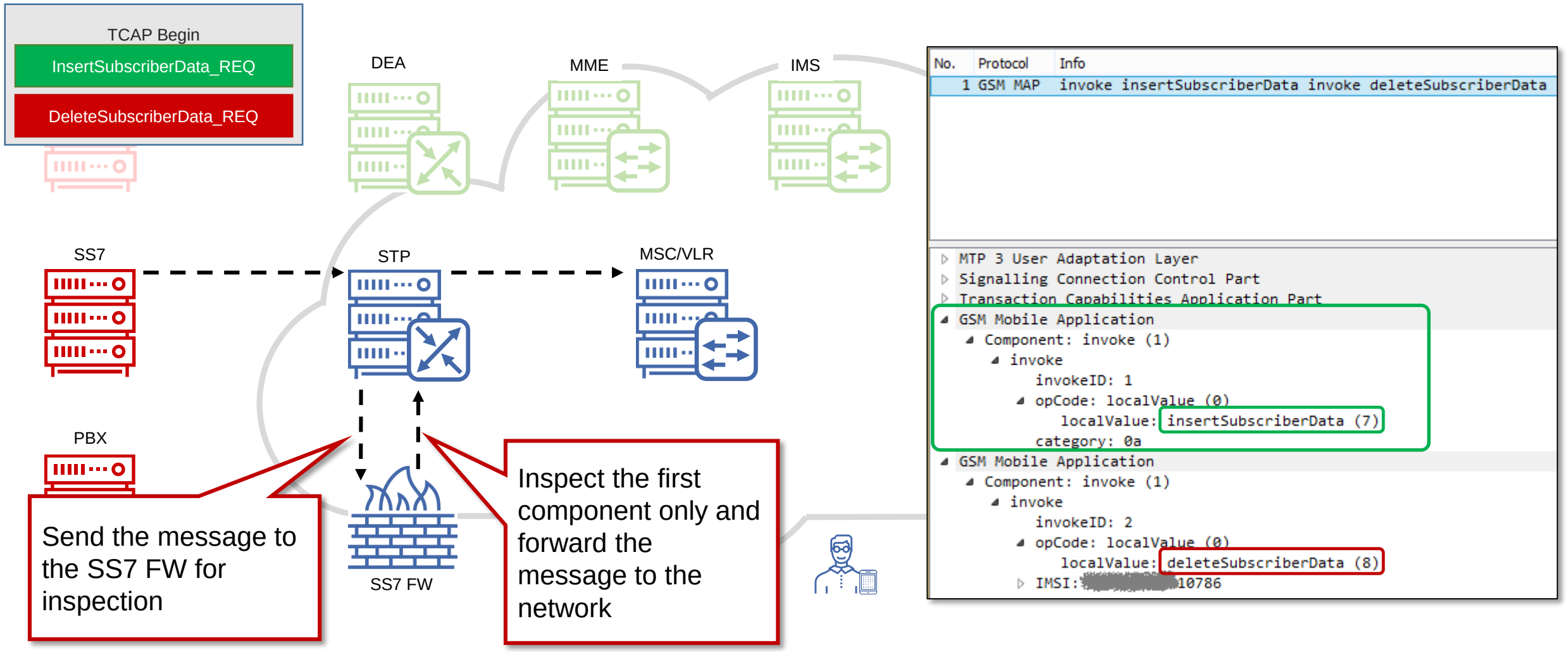
Component Portion — optional

- Component 1
- Component 2

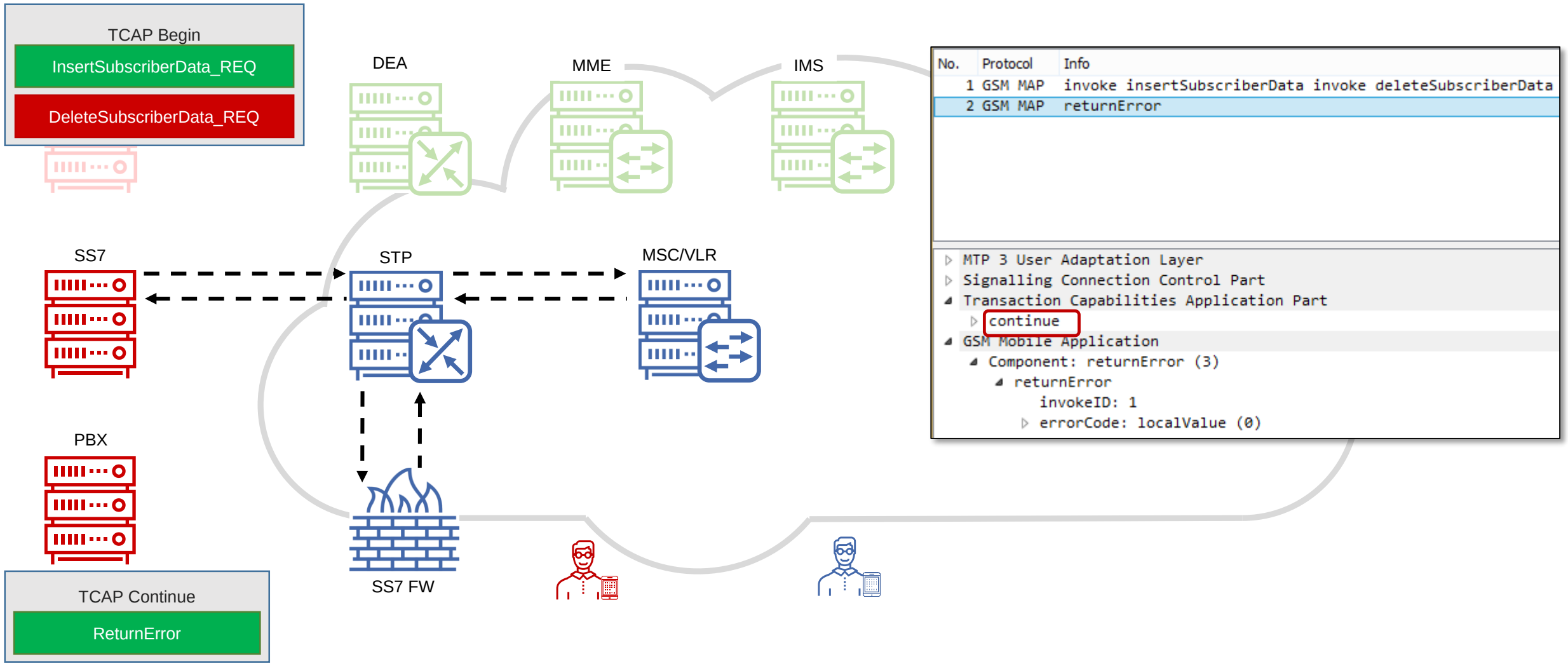


The SS7 FW checks a subscriber's ID in the first component considering the other data as a long payload not meant to be inspected

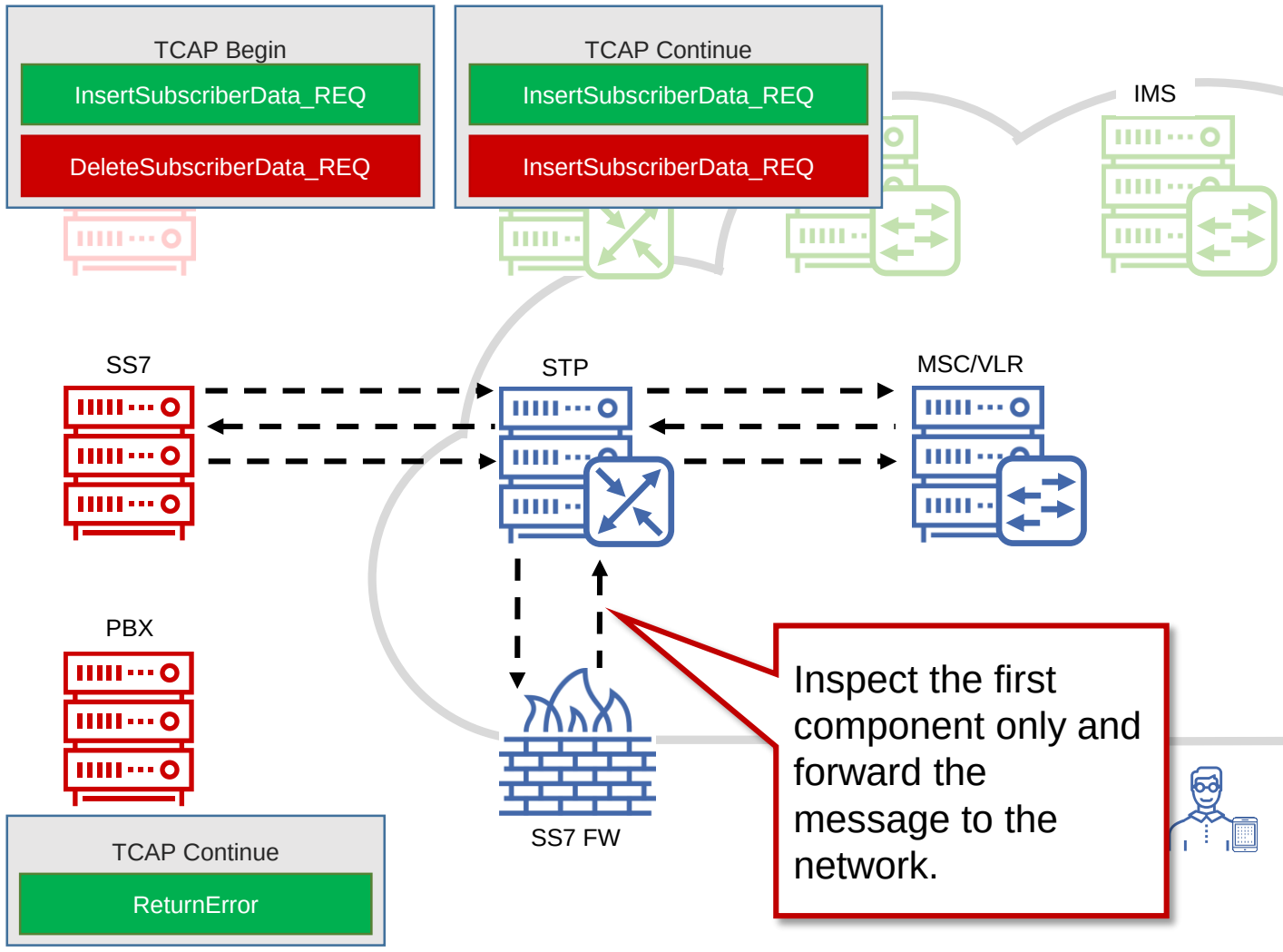
Double MAP in MITM attack

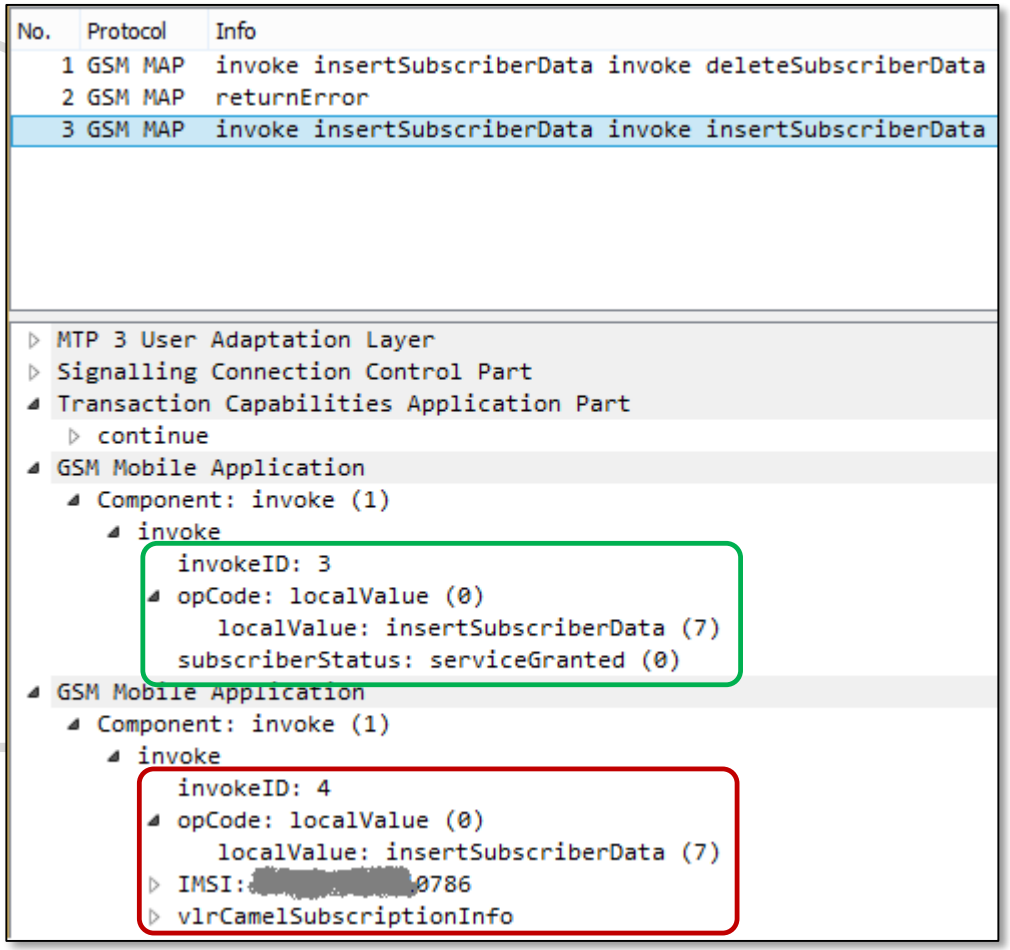


Double MAP in MITM attack

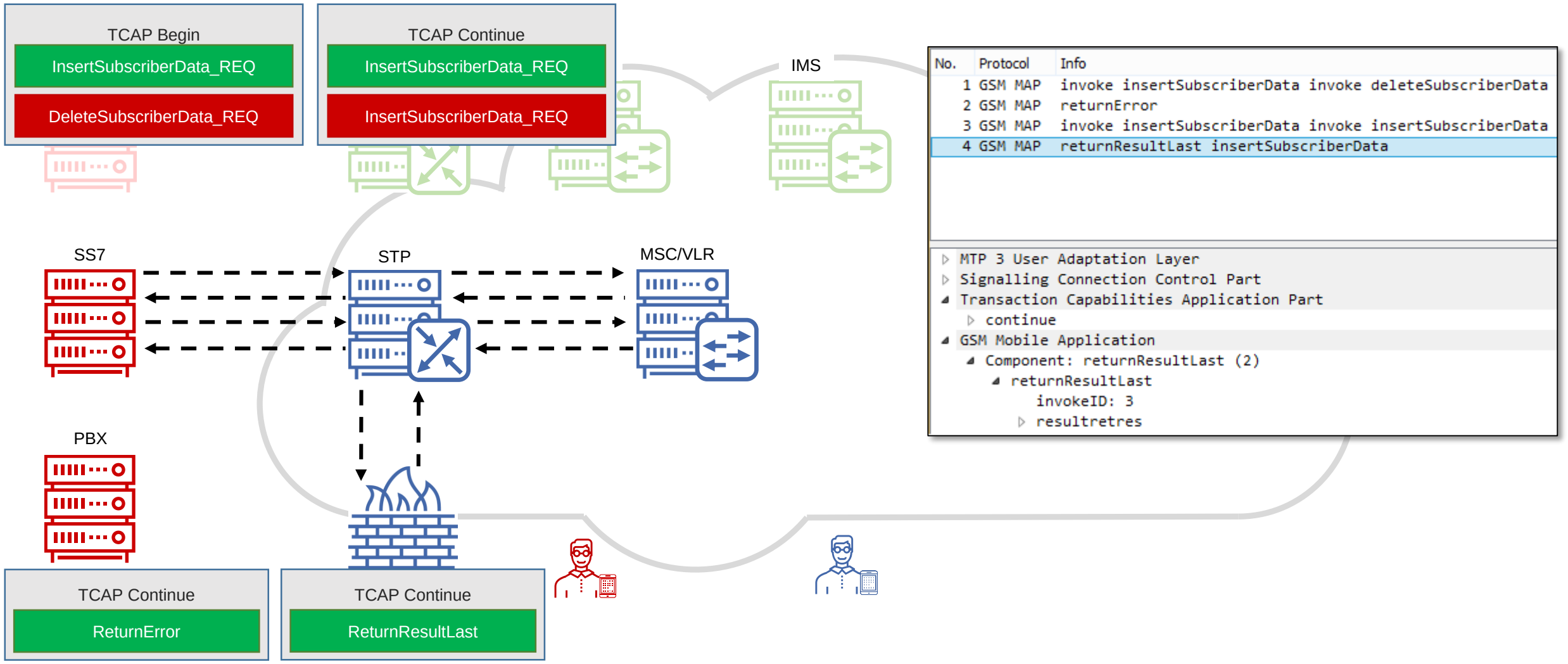


Double MAP in MITM attack

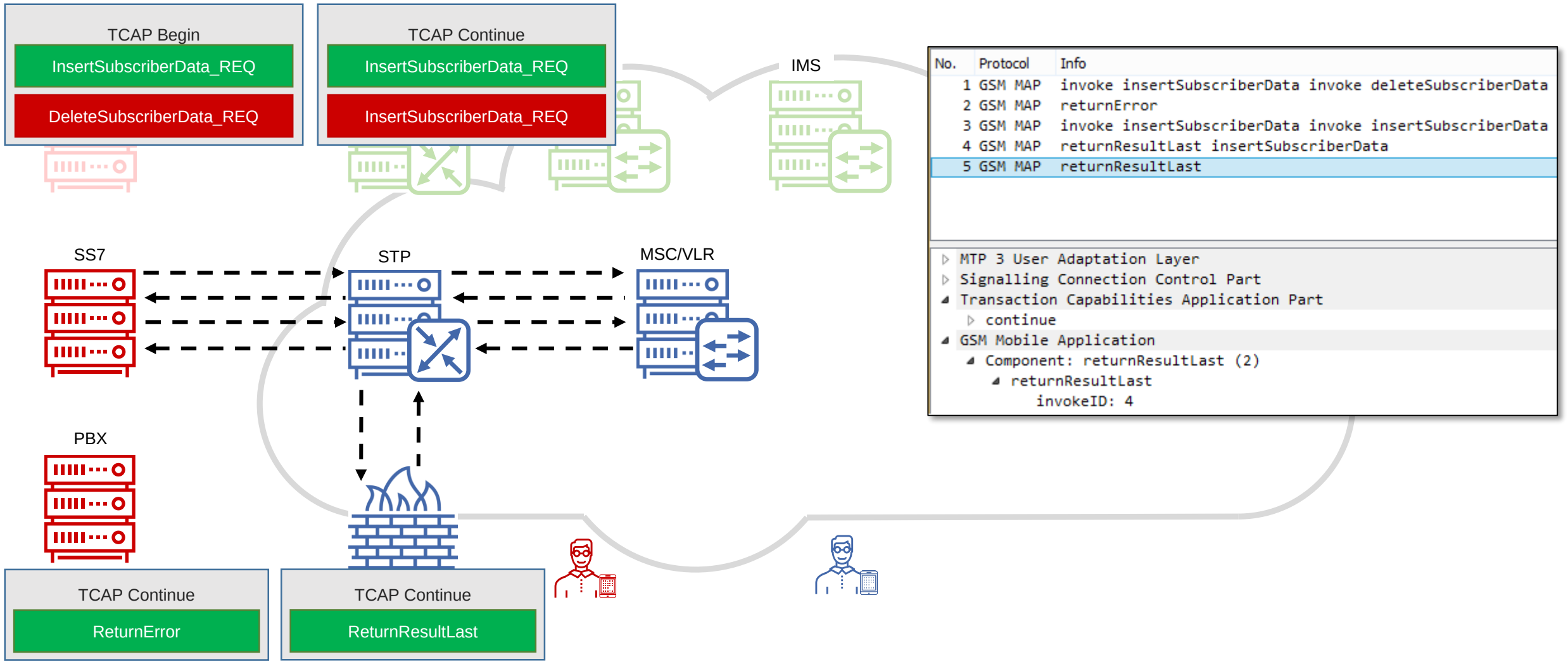




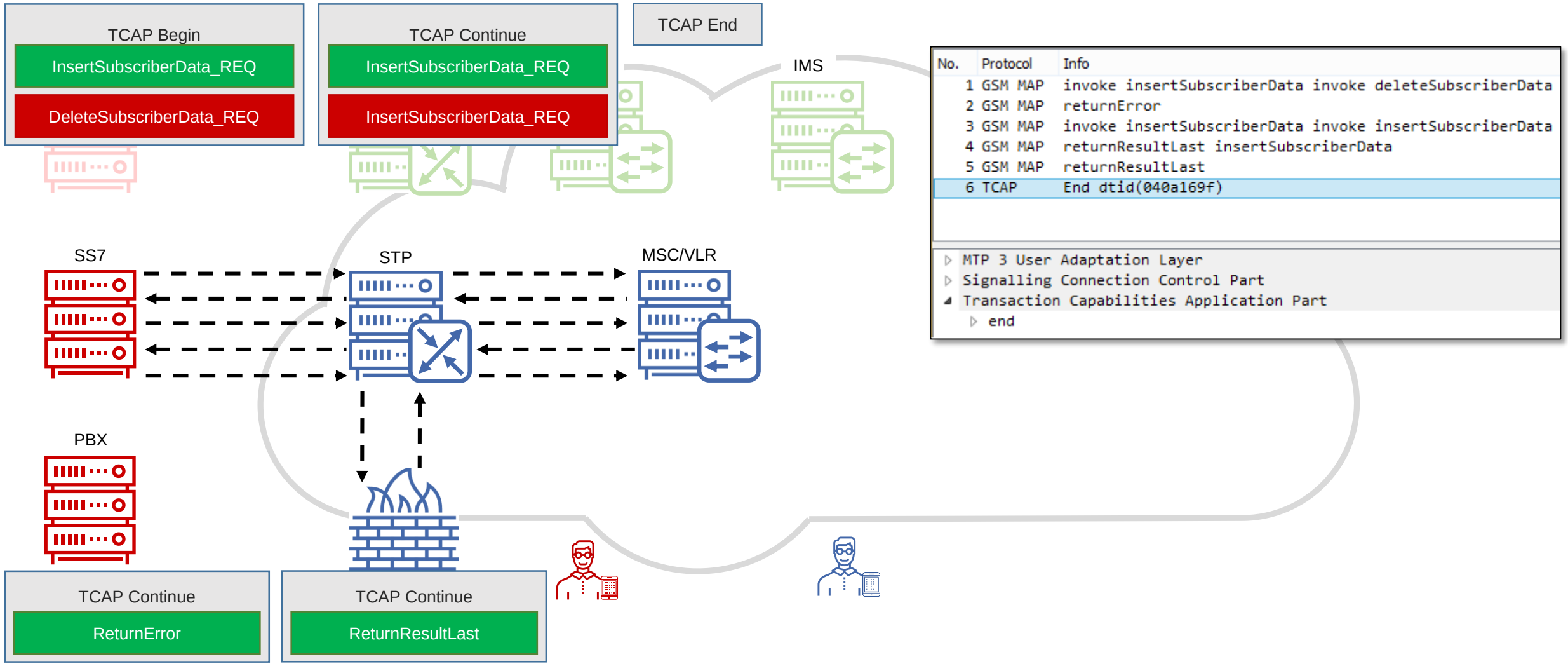
Double MAP in MITM attack



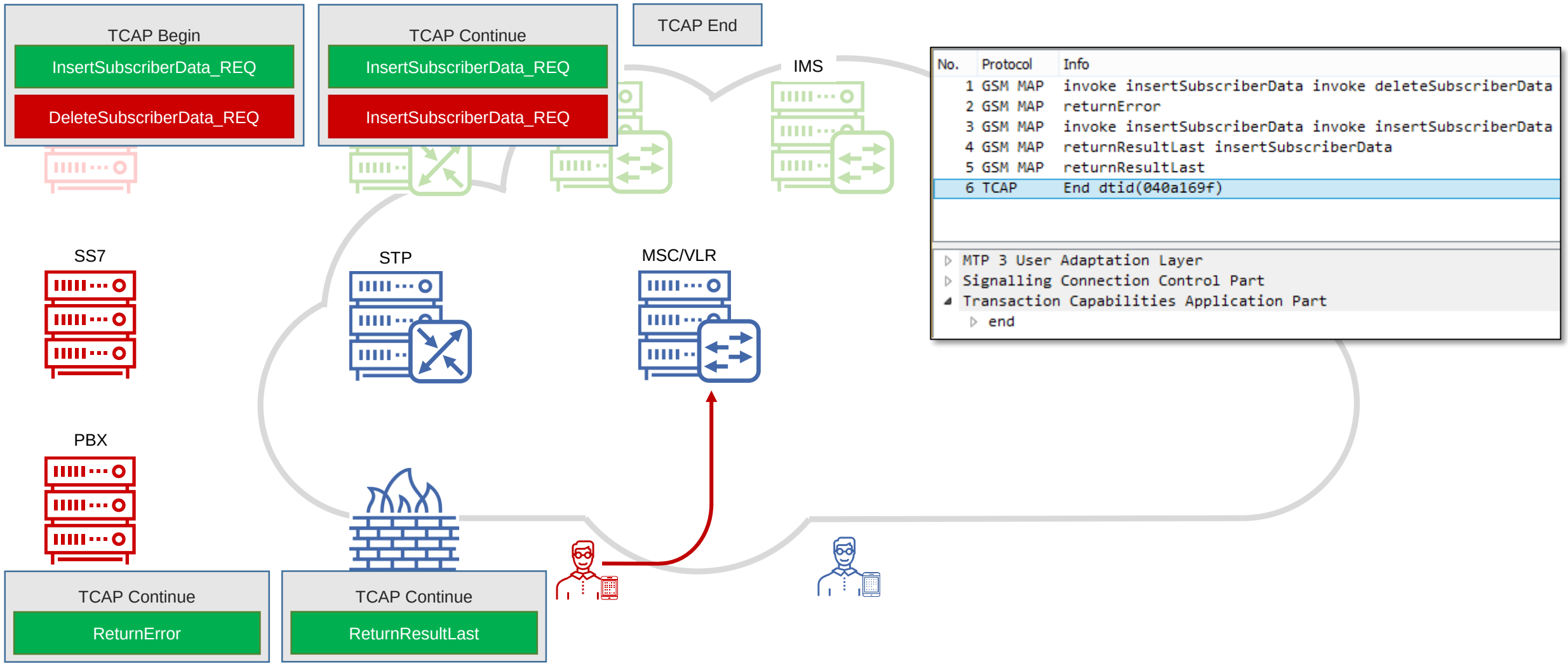
Double MAP in MITM attack



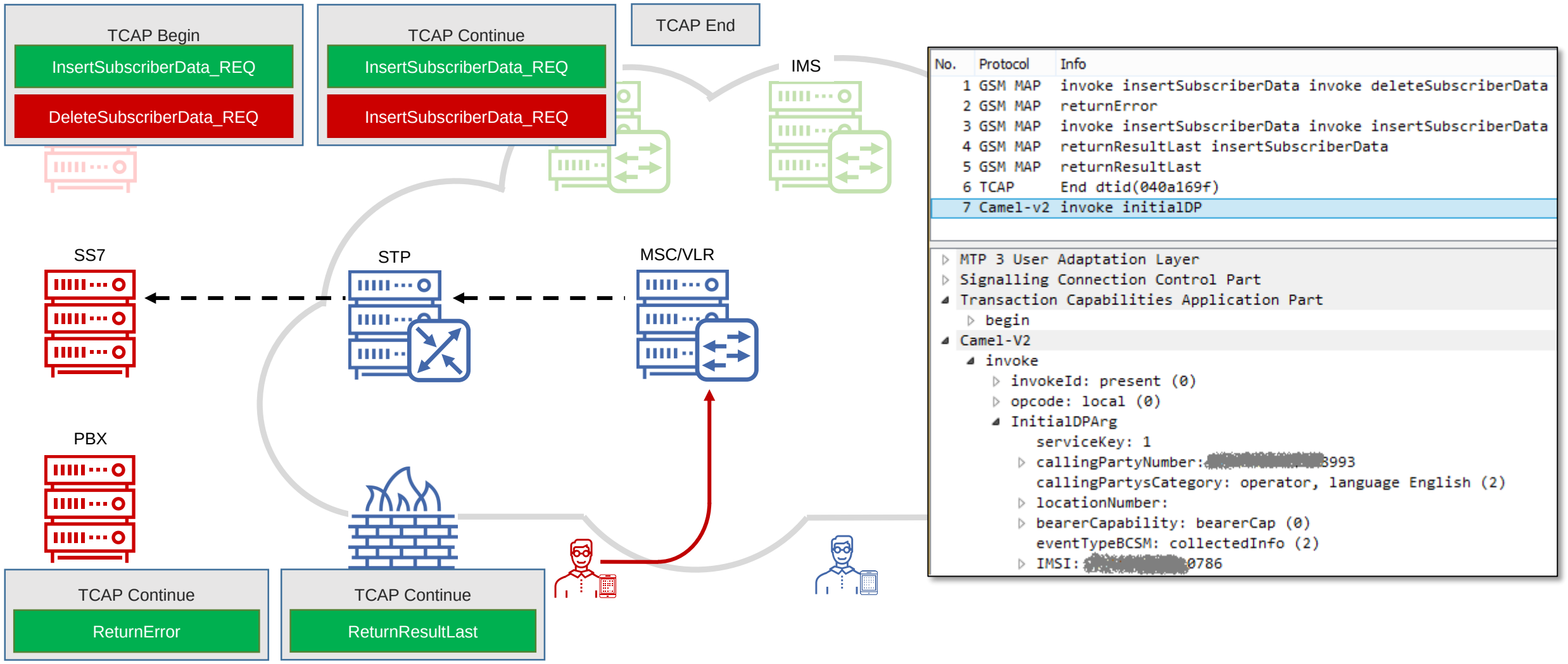
Double MAP in MITM attack



Double MAP in MITM attack



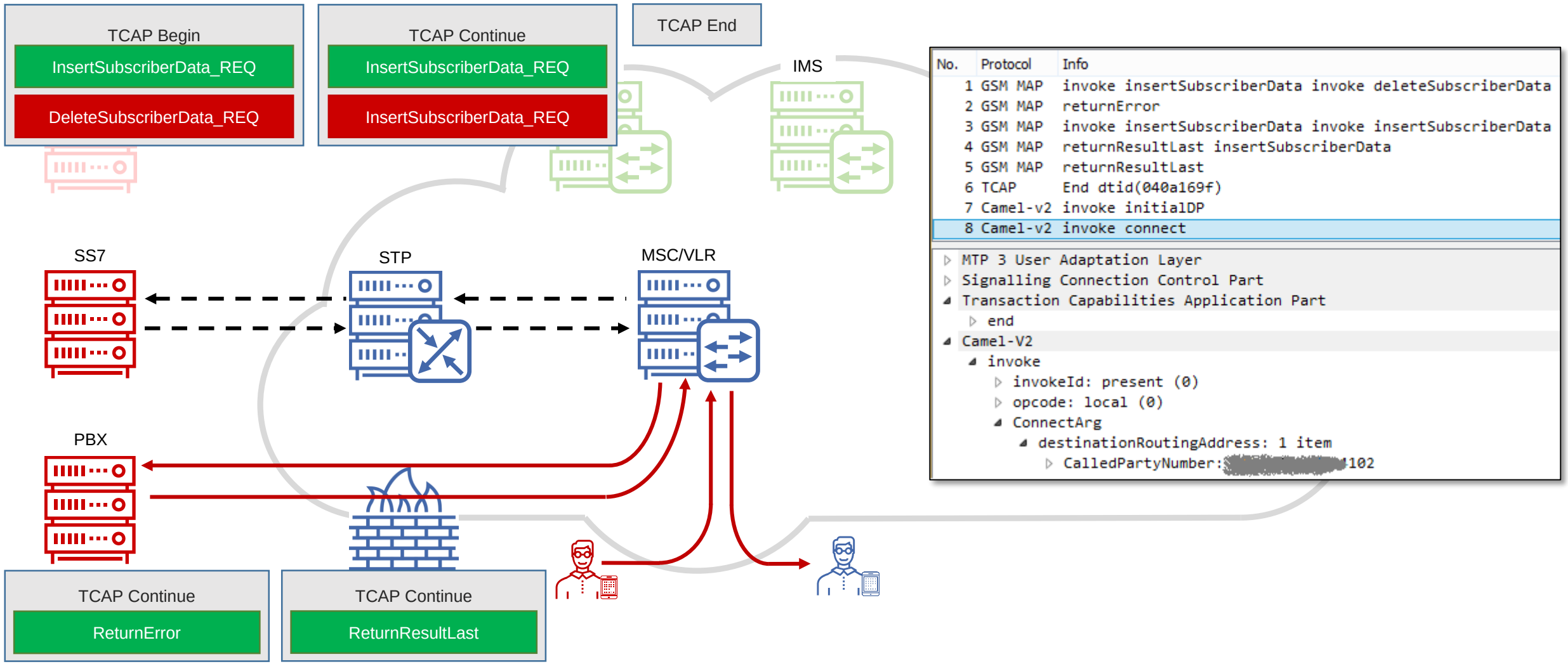
Double MAP in MITM attack



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



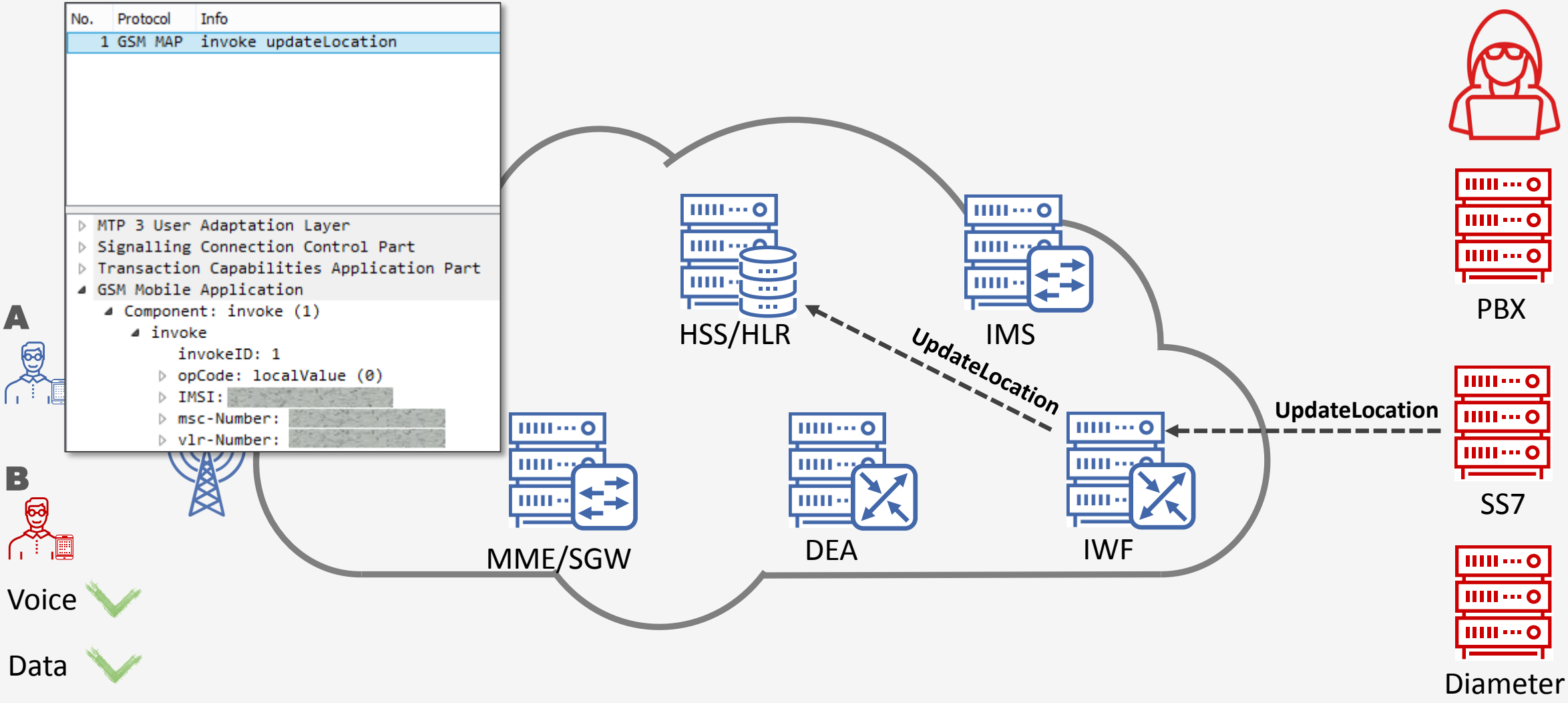
No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData invoke deleteSubscriberData
2	GSM MAP	returnError
3	GSM MAP	invoke insertSubscriberData invoke insertSubscriberData
4	GSM MAP	returnResultLast insertSubscriberData
5	GSM MAP	returnResultLast
6	TCAP	End dtid(040a169f)
7	Camel-v2	invoke initialDP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

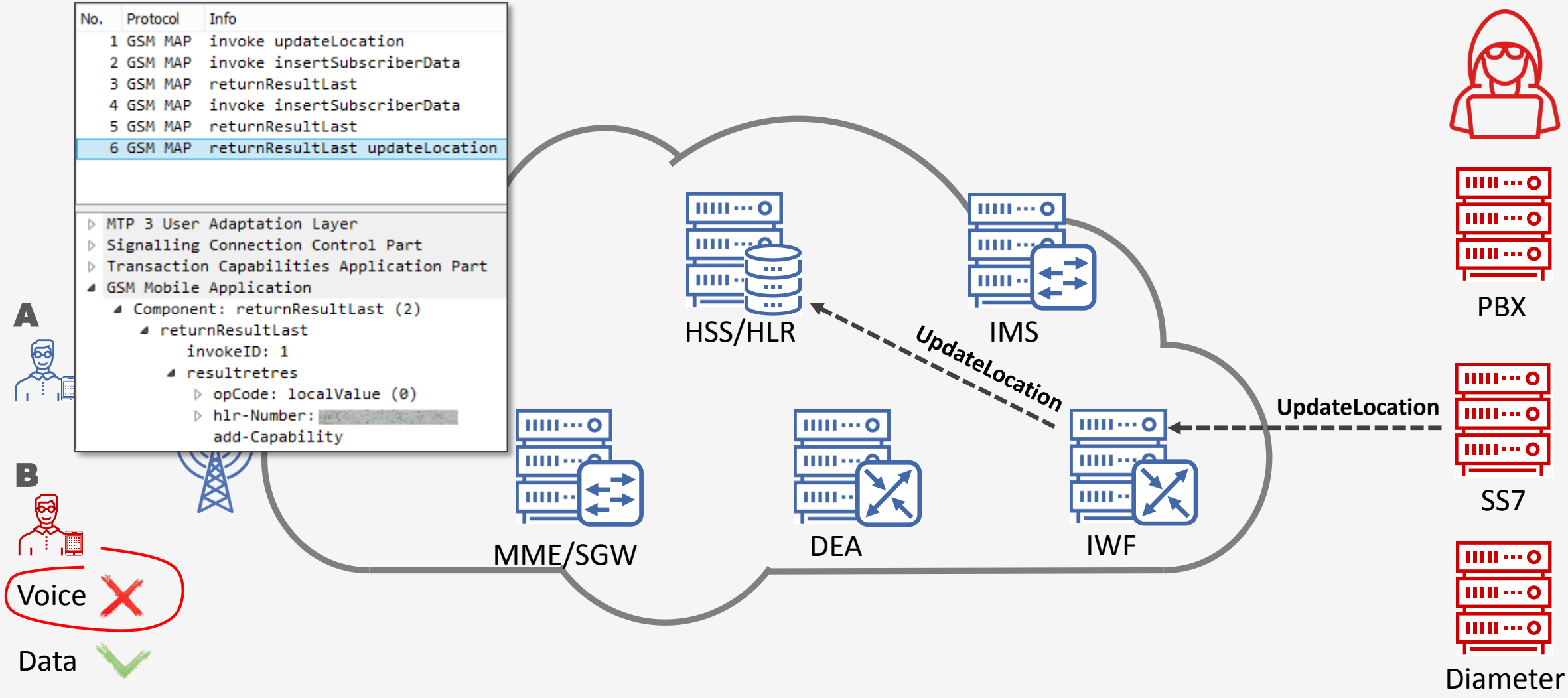
Voice call interception (MITM) on 4G/5G network

Attack via packet data service disruption

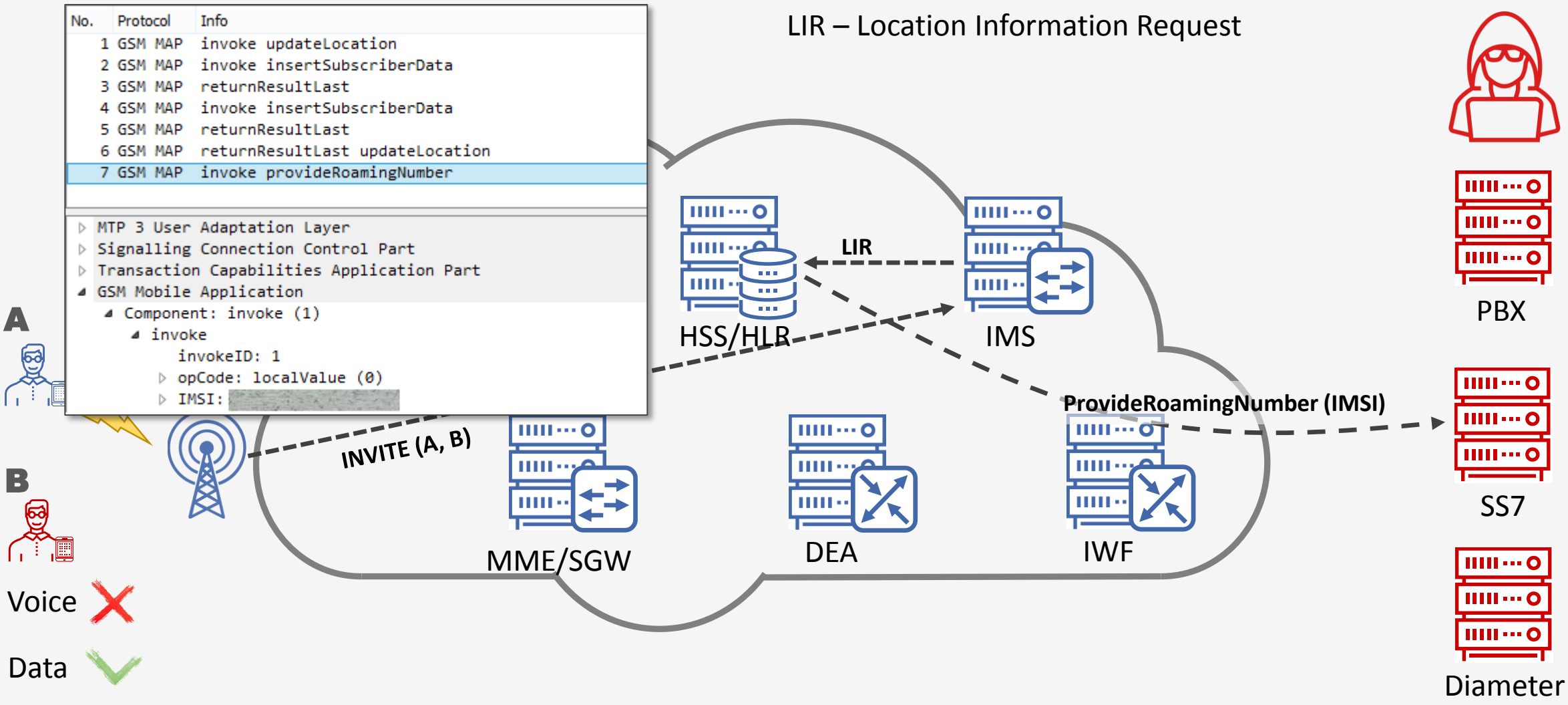
Fake registration on 2G/3G



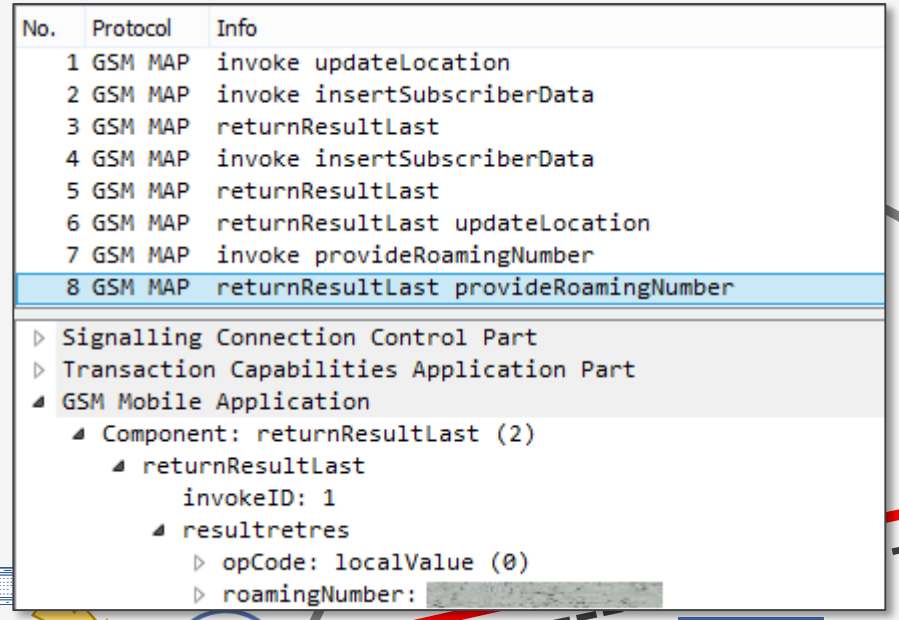
Fake registration on 2G/3G



Originating traffic redirection

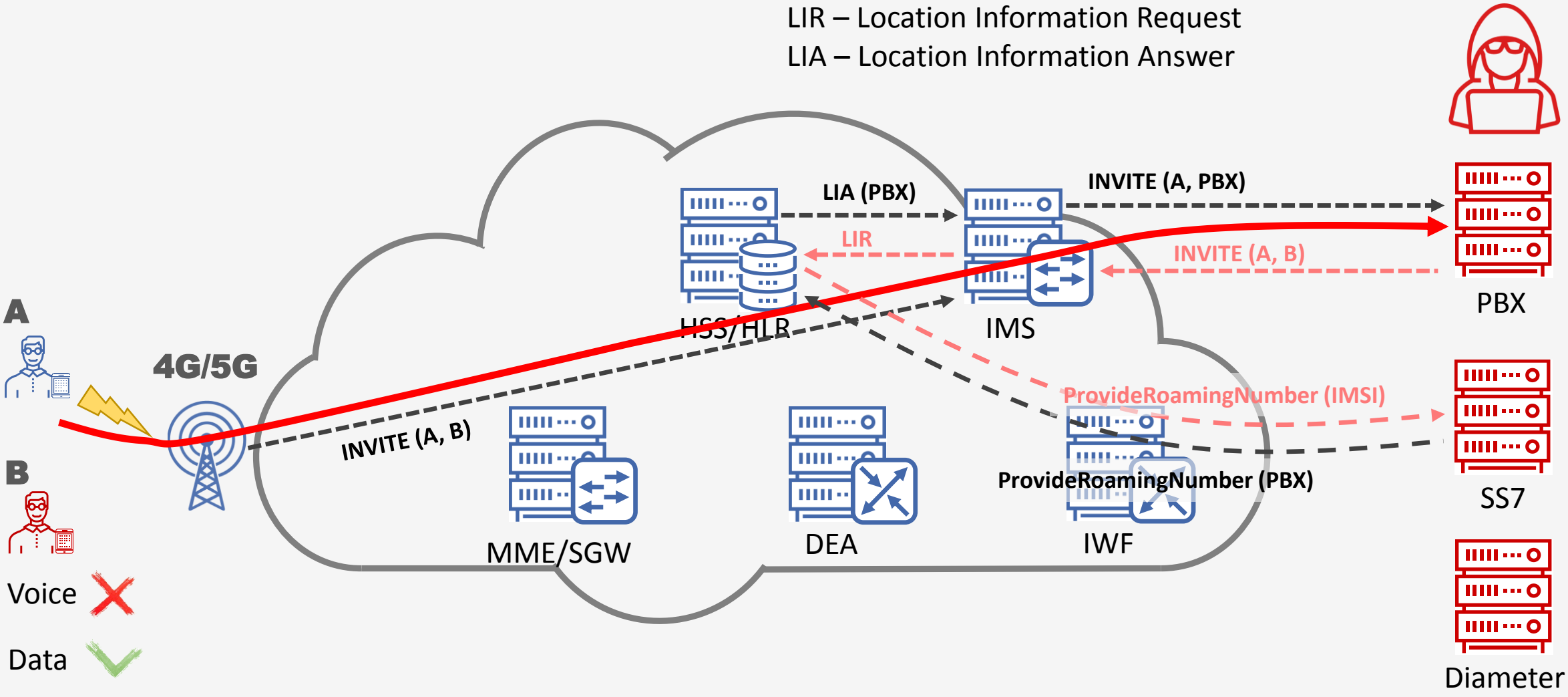


Originating traffic redirection



LIR – Location Information Request
LIA – Location Information Answer

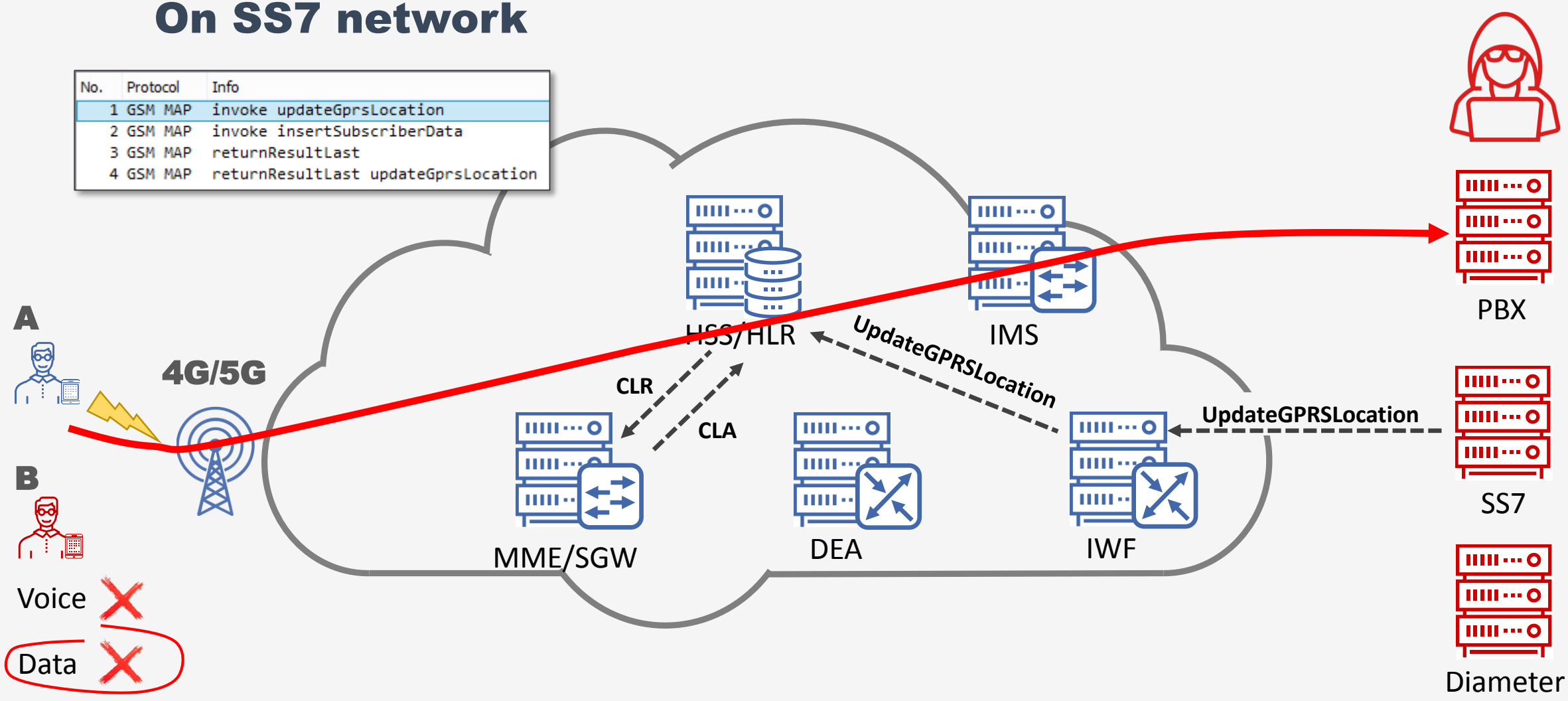
What's the next?



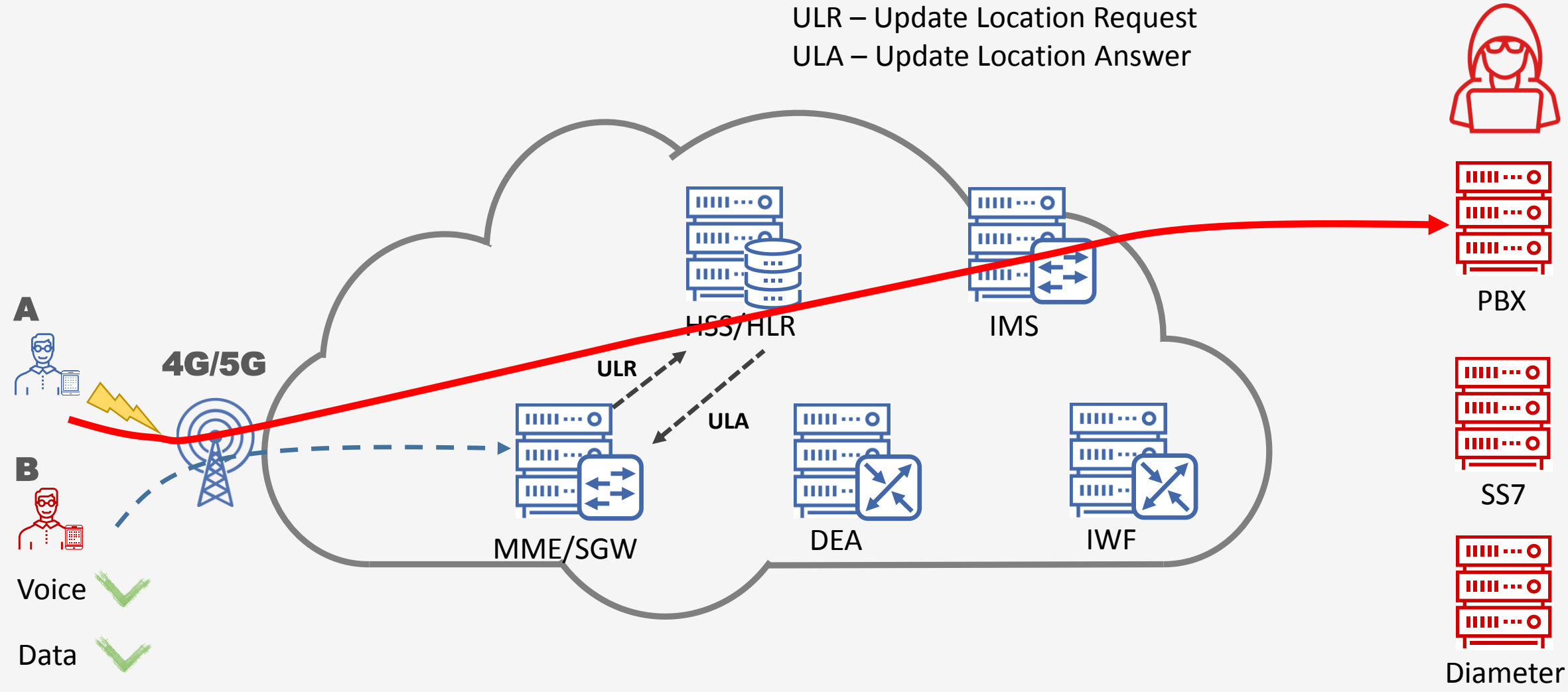
Case 1. Packet data disruption

On SS7 network

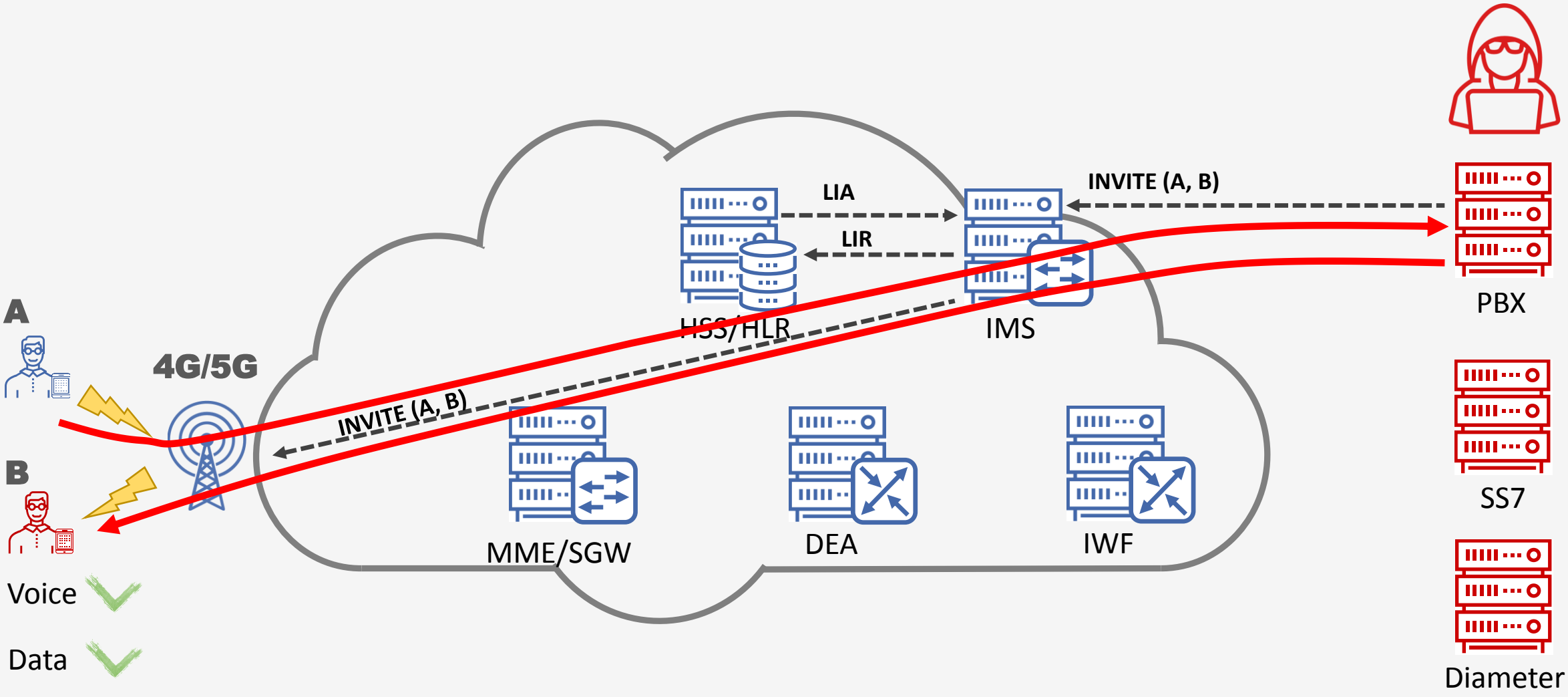
No.	Protocol	Info
1	GSM MAP	invoke updateGprsLocation
2	GSM MAP	invoke insertSubscriberData
3	GSM MAP	returnResultLast
4	GSM MAP	returnResultLast updateGprsLocation



Service restoration



Terminating traffic initiation

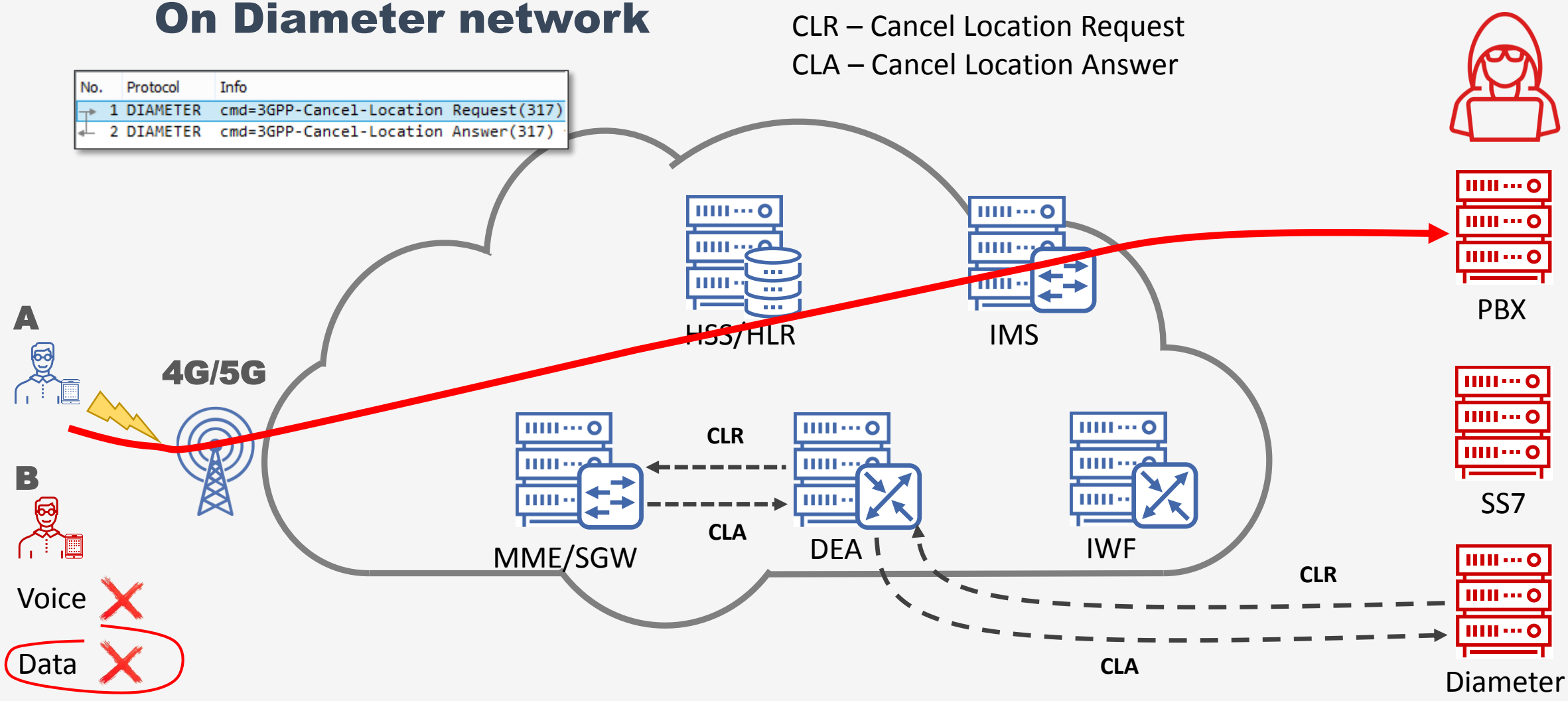


Case 2. Packet data disruption

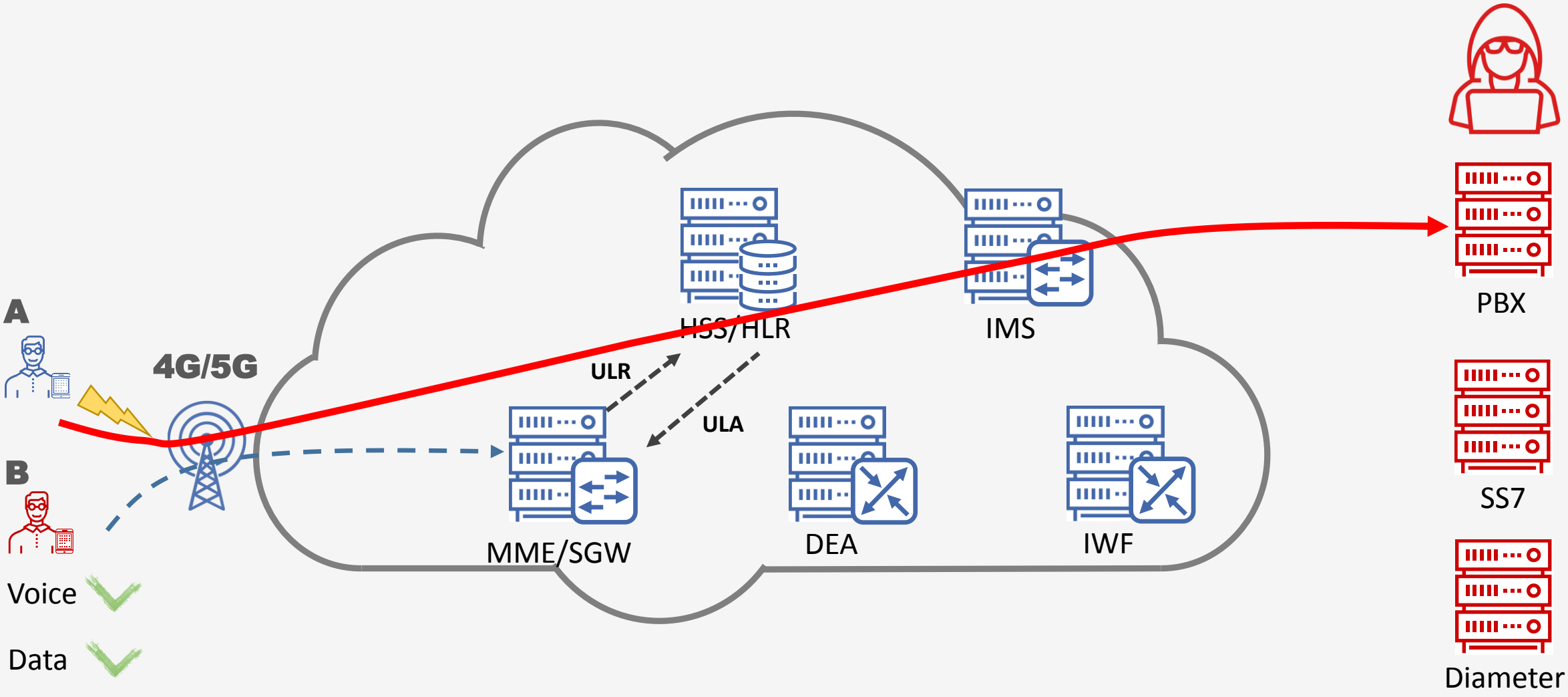
On Diameter network

CLR – Cancel Location Request
CLA – Cancel Location Answer

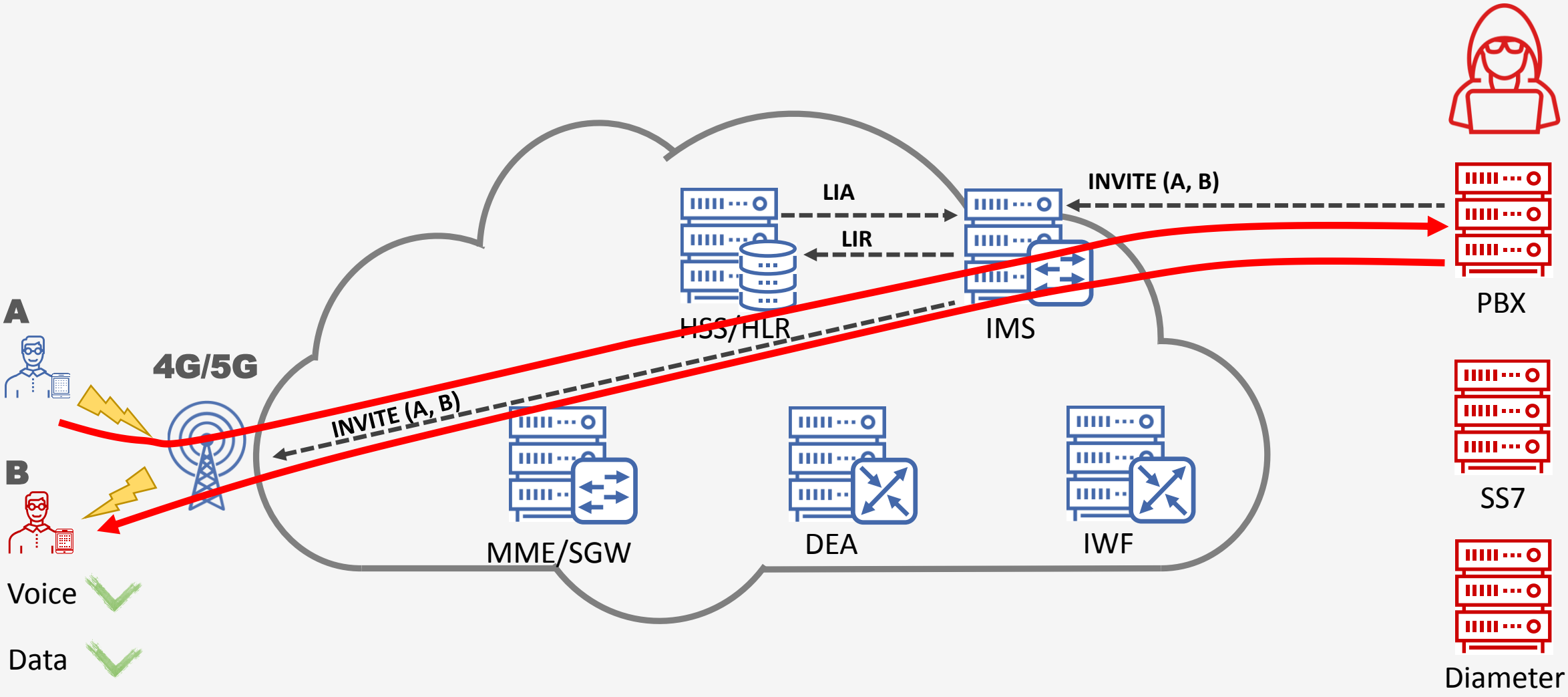
No.	Protocol	Info
1	DIAMETER	cmd=3GPP-Cancel-Location Request(317)
2	DIAMETER	cmd=3GPP-Cancel-Location Answer(317)



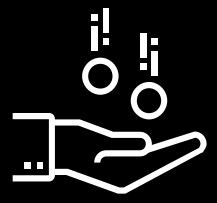
Service restoration



Terminating traffic initiation

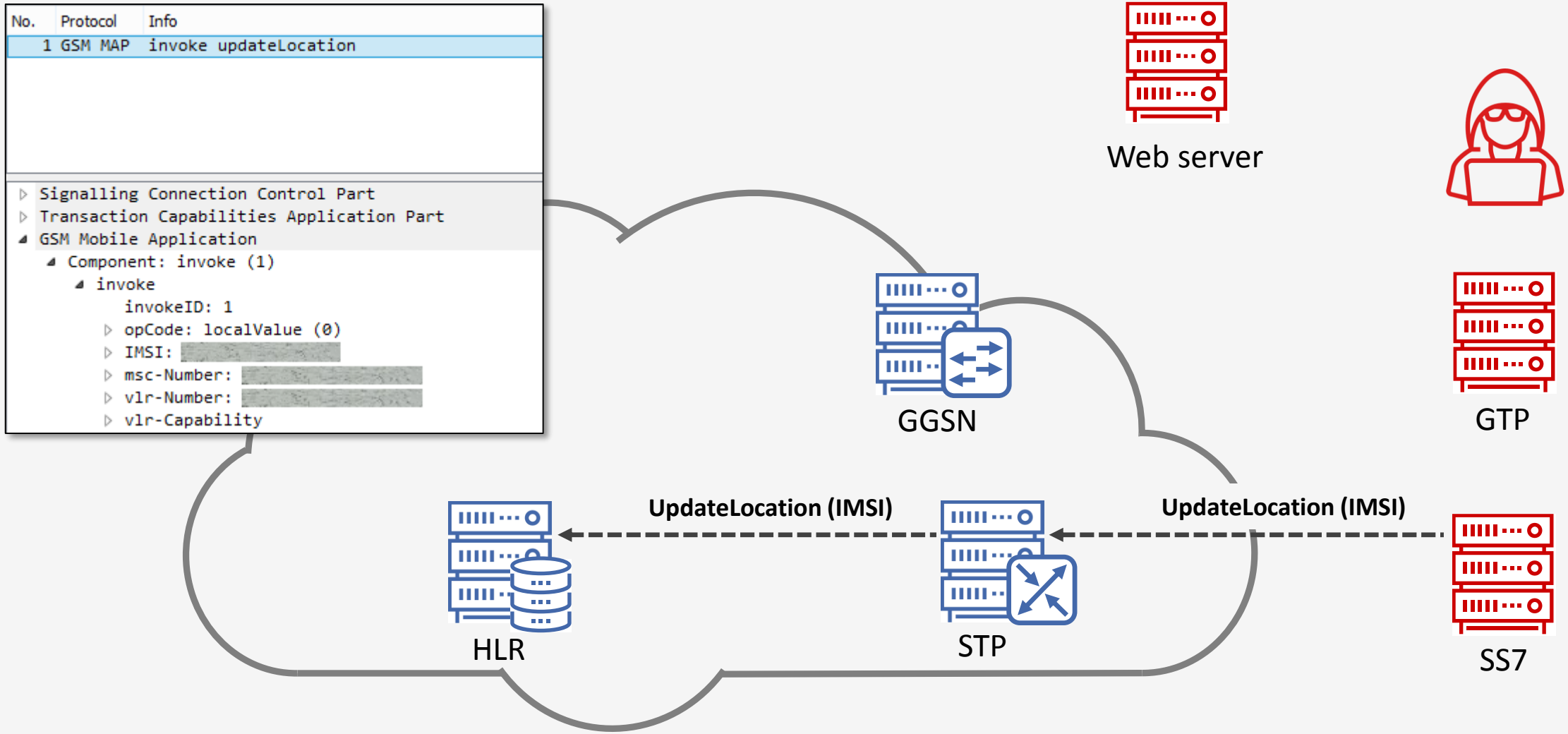


Subscription fraud

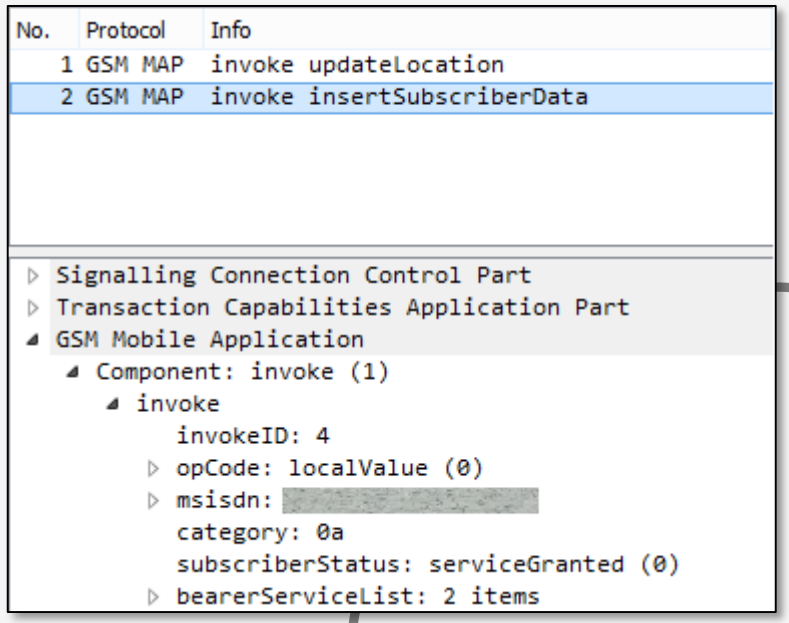


Attack on SS7 and GTP networks

Subscription fraud via SS7/GTP



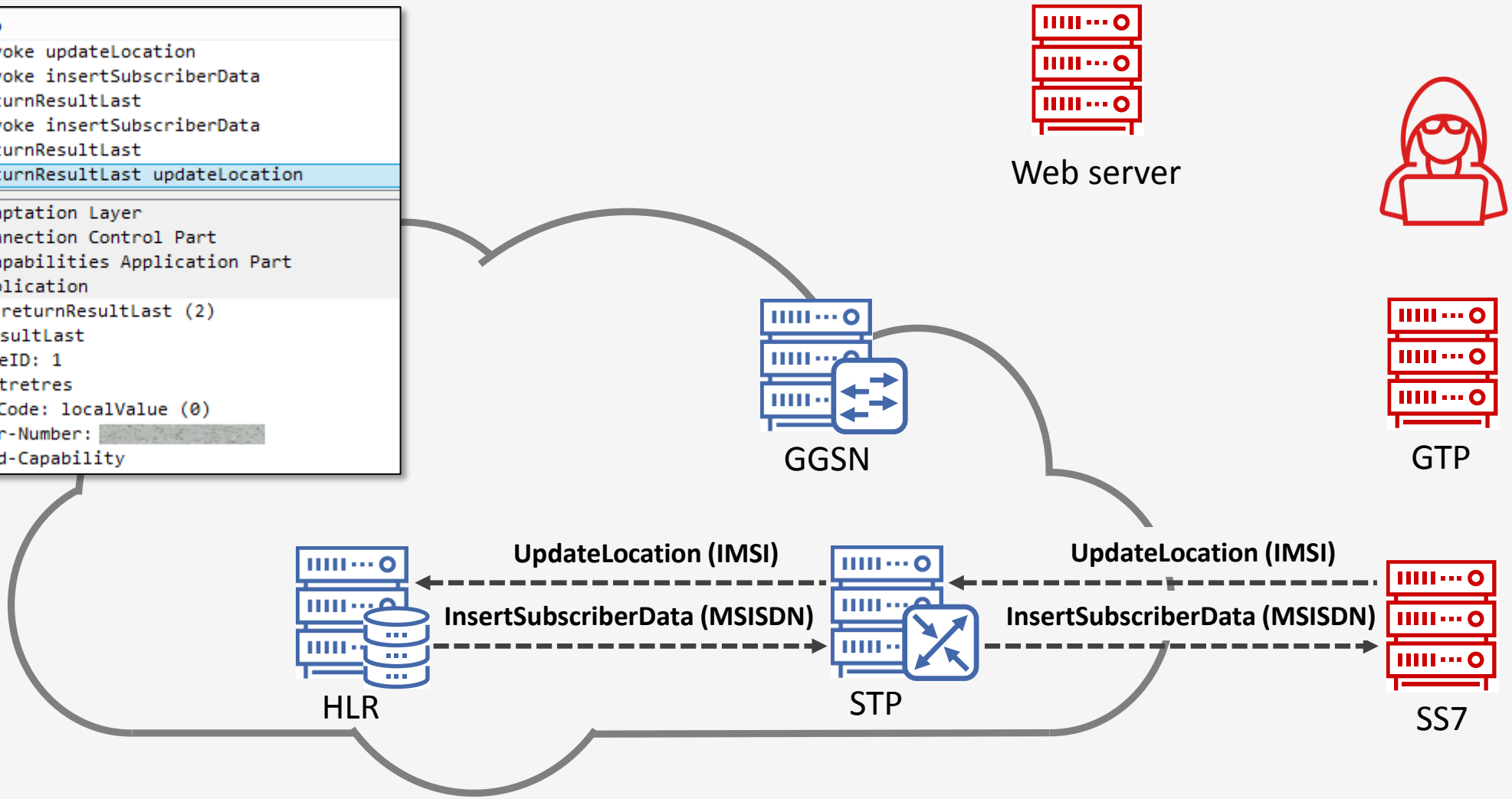
Subscription fraud via SS7/GTP



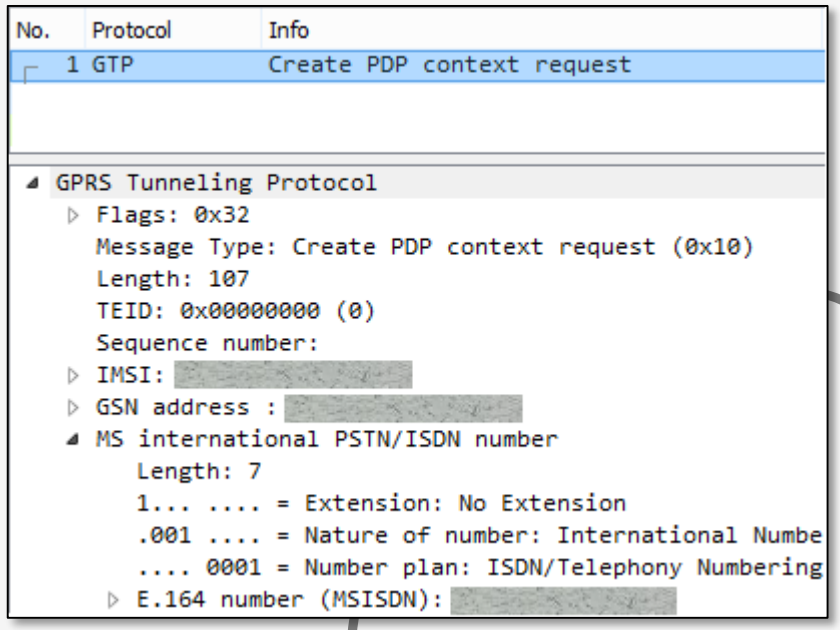
Subscription fraud via SS7/GTP

No.	Protocol	Info
1	GSM MAP	invoke updateLocation
2	GSM MAP	invoke insertSubscriberData
3	GSM MAP	returnResultLast
4	GSM MAP	invoke insertSubscriberData
5	GSM MAP	returnResultLast
6	GSM MAP	returnResultLast updateLocation

```
▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
  ◢ Component: returnResultLast (2)
    ◢ returnResultLast
        invokeID: 1
      ◢ resultretres
        ▷ opCode: localValue (0)
        ▷ hlr-Number: [redacted]
          add-Capability
```



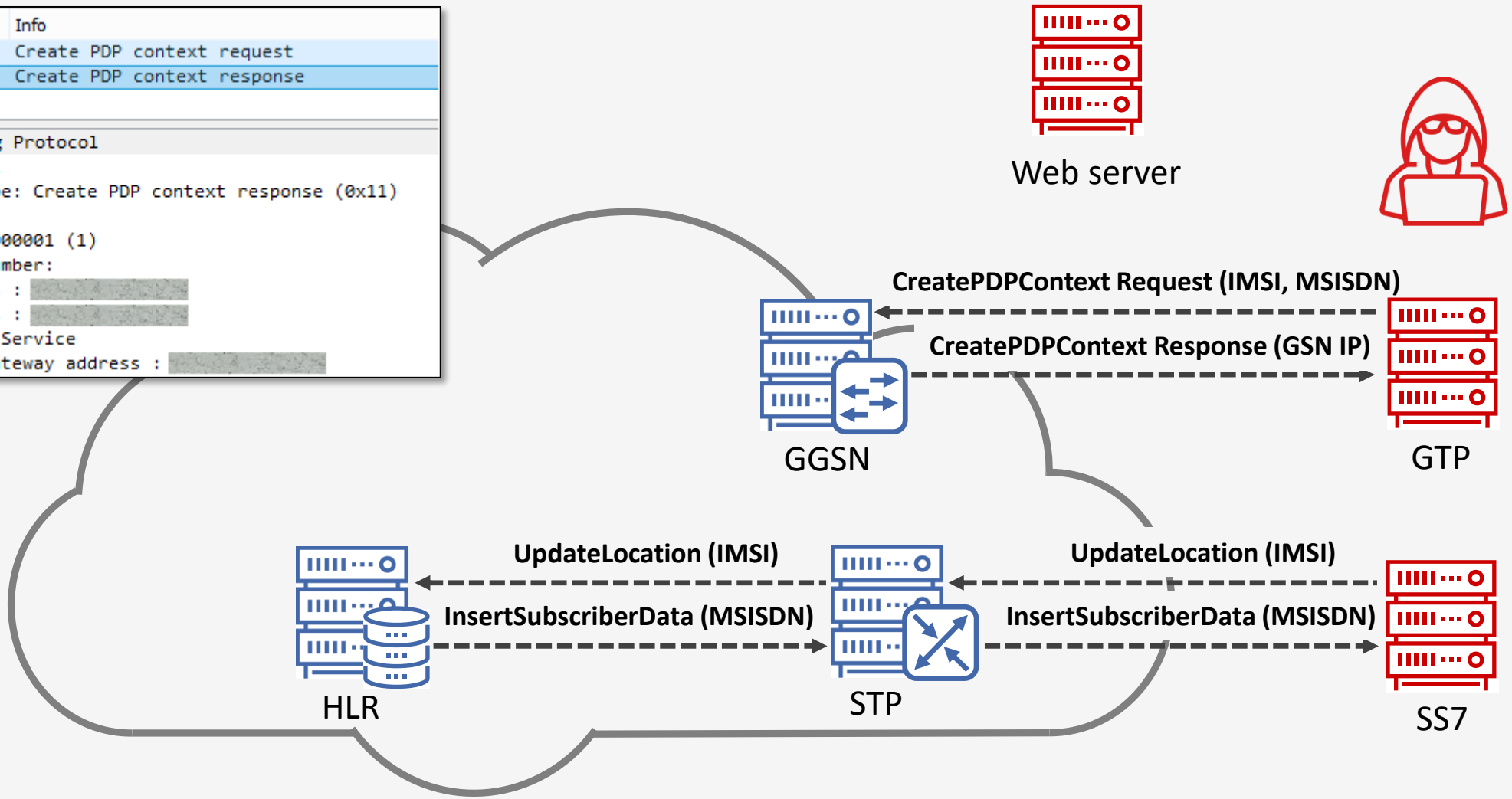
Subscription fraud via SS7/GTP



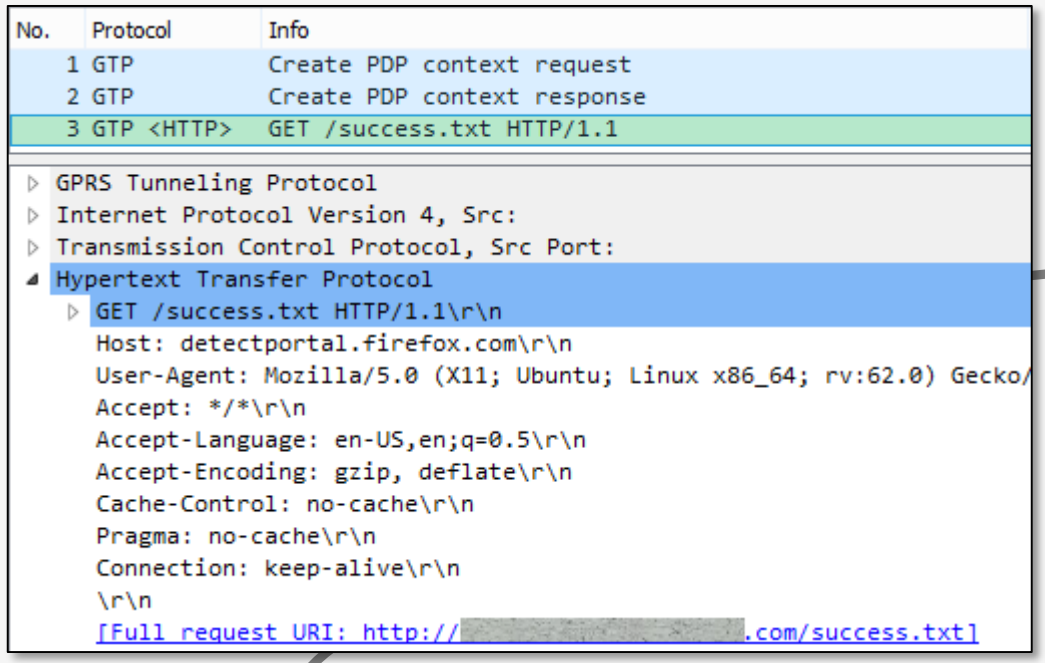
Subscription fraud via SS7/GTP

No.	Protocol	Info
1	GTP	Create PDP context request
2	GTP	Create PDP context response

```
GPRS Tunneling Protocol
  Flags: 0x32
  Message Type: Create PDP context response (0x11)
  Length: 83
  TEID: 0x00000001 (1)
  Sequence number:
  GSN address : [redacted]
  GSN address : [redacted]
  Quality of Service
  Charging Gateway address : [redacted]
```



Subscription fraud via SS7/GTP



Contribution to GSMA

- Information about discovered cross-protocol vulnerabilities has been reported on the **GSMA FASG** meeting in February 2020.
- SS7 firewall bypass techniques were reported to **GSMA FASG*** group in April 2019. This information is **published** in the "SS7 Interconnect Security Monitoring and Firewall Guidelines."
- GSMA Coordinated Vulnerability Programme registered this issue with the number **CVD-2018-0015**.

* FASG is Fraud and Security Group

Main issues in signaling security

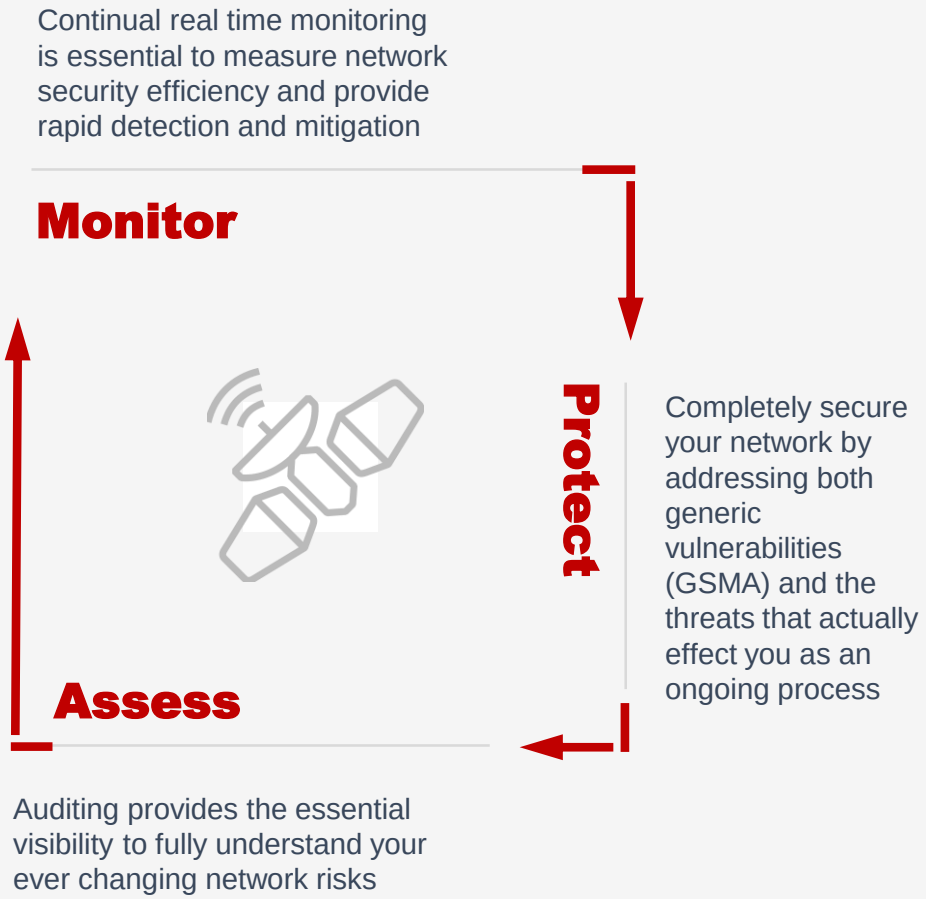
- Architecture flaws
- Configuration errors
- Software bugs

Protection measures

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

2. Use an intrusion detection solution along with an **SS7** and **Diameter** firewalls in order to detect threats promptly and block a hostile source.

3. Configure your STP, DEA, and signaling firewall carefully. Do not forget about reported vulnerabilities such as malformed Application Context Name and double MAP encapsulation.



:: Positive Technologies

Thank you

Sergey Puzankov
sergey.puzankov@positive-tech.com