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.
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?

- Easily
- From anywhere

Easily
- Intercepts private data, calls, and SMS messages
- Take control of your digital identity
- Any mobile operator
- Get access to your email and social media
- No special skills needed
- Steal money

From anywhere
- Track location of VIPs and public figures
- Perform massive denial of service attacks

Intercept private data, calls, and SMS messages
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

Security assessment

Security configuration

Signaling firewall

SMS Home Routing

Signaling IDS
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
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

- MSC/VLR
- SGSN
- HLR
- STP
- GGSN
- HSS
- IMS
- DEA
- IWF
- MME/SGW
- PGW
- 2G
- 3G
- 4G
- 5G non SA
- SS7
- GTP
- Diameter
SS7 and Diameter firewall penetration*

This is the main reason why the intruders start using Diameter protocol along with SS7

* 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. **Insert Subscriber Data** Request: IMSI
   Spoofed billing platform address

---

**Table: Signalling Connection Control Part**
- **Transaction Capabilities Application Part**
  - **GSM Mobile Application**
    - **Component:** invoke (1)
      - **invoke**
        - **invokeID:** 1
        - **opCode:** localValue (0)
        - **IMSI:** 1234567890
        - **vrContainerSubscriptionInfo**
Voice call interception (MITM)

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

2. **InsertSubscriberData** Response

3. TCAP End

---

**Table:**

<table>
<thead>
<tr>
<th>No.</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GSM MAP</td>
<td>invoke insertSubscriberData</td>
</tr>
<tr>
<td>2</td>
<td>GSM MAP</td>
<td>returnResultLast insertSubscriberData</td>
</tr>
<tr>
<td>3</td>
<td>TCAP</td>
<td>End dtid(410001bs)</td>
</tr>
</tbody>
</table>

---

**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 (phased1, phased2)
Voice call interception (MITM)

1. InitialDP: IMSI, A-Num, B-Num

<table>
<thead>
<tr>
<th>No.</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GSM MAP</td>
<td>invoke insertSubscriberData</td>
</tr>
<tr>
<td>2</td>
<td>GSM MAP</td>
<td>returnResultLast insertSubscriberData</td>
</tr>
<tr>
<td>3</td>
<td>TCAP</td>
<td>End dtid(4100810a)</td>
</tr>
<tr>
<td>4</td>
<td>Camel-v2</td>
<td>invoke InitialDP</td>
</tr>
</tbody>
</table>

- Signalling Connection Control Part
- Transaction Capabilities Application Part
- Camel-V2
  - Invoke
    - InvokeId: present (0)
    - opcode: local (0)
    - InitialDPArg
      - serviceKey: 1
        - callingPartyNumber: 86800000000804
        - callingPartyCategory: ordinary calling subscriber (10)
      - locationNumber: 1
      - calledPartyBCDNumber: 8680000000804

MSC/VLR
Voice call interception (MITM)
Voice call interception (MITM)

1. InitialDP: IMSI, A-Num, B-Num
2. Connect: PBX-Num
3. IAM: A-Num, B-Num

STP

MSC/VLR

:: Positive Technologies
SS7 FW against MITM attack

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

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

Switzerland ≠ Taiwan
VoLTE against MITM attack

1. InsertSubscriberData Request: IMSI Spoofed billing platform address

2. InsertSubscriberData Response

3. TCAP End
VoLTE service suppression

CLR – Cancel-Location Request

- Diameter
- CLR
- DEA
- MME
- IMS
- SS7
- STP
- MSC/VLR
- PBX
- SS7 FW
- DEA
- MME
- IMS

Diameter cmd=3GPP.Cancel-Location Request(317) flags=RP-- appl=3GPP S6a/S6d(167772)

- AVP: User-Name(1) l=23 f=M- val=***@******.***
- AVP: Vendor-Specific-Application-Id(260) l=32 f=M-
- AVP: Auth-Session-State(277) l=12 f=M- val=NO_STATE_MAINTAINED (1)
- AVP: Supported-Features(628) l=56 f=VM- vnd=3GPP
- AVP: Cancellation-Type(1420) l=16 f=VM- vnd=3GPP val=SUBSCRIPTION_WITHDRAWAL
  - AVP Code: 1420 Cancellation-Type
  - AVP Flags: 0xc0, Vendor-Specific: Set, Mandatory: Set
  - AVP Length: 16
  - AVP Vendor Id: 3GPP
  - Cancellation-Type: SUBSCRIPTION_WITHDRAWAL (2)
- AVP: CLR-Flags(1638) l=16 f=V- vnd=3GPP val=1
VoLTE service suppression

CLR – Cancel-Location Answer

Diameter

CLA

SS7

STP

MSC/VLR

SS7 FW

PBX

DEA

MME

IMS

Diameter cmd=3GPP-Cancel-Location Request(317) flags=-- appl=3GPP S6a/S6d(167772)

Diameter cmd=3GPP-Cancel-Location Answer(317) flags=-- appl=3GPP S6a/S6d(167772)

Protocol Info

AVP: Vendor-Specific-Application-Id(260) 1=32 f--M-

AVP: Result-Code(268) 1-12 f--M- val=DIAMETER_SUCCESS (2001)

AVP: Origin-Host(254) 1-63 f--M- val=3gonetwork.org

AVP: Origin-Realm(296) 1-41 f--M- val=epc.3gonetwork.org

AVP: Auth-Session-State(277) 1=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

Send the message to the SS7 FW for inspection

Inspect the first component only and forward the message to the network
Double MAP in MITM attack

Inspect the first component only and forward the message to the network.
Double MAP in MITM attack

TCAP Begin
- InsertSubscriberData_REQ
- DeleteSubscriberData_REQ

TCAP Continue
- InsertSubscriberData_REQ
- InsertSubscriberData_REQ

IMS

<table>
<thead>
<tr>
<th>No.</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GSM MAP</td>
<td>invoke insertSubscriberData invoke deleteSubscriberData</td>
</tr>
<tr>
<td>2</td>
<td>GSM MAP</td>
<td>returnError</td>
</tr>
<tr>
<td>3</td>
<td>GSM MAP</td>
<td>Invoke insertSubscriberData Invoke insertSubscriberData</td>
</tr>
<tr>
<td>4</td>
<td>GSM MAP</td>
<td>returnResultLast insertSubscriberData</td>
</tr>
</tbody>
</table>

MTP 3 User Adaptation Layer
- Signalling Connection Control Part
- Transaction Capabilities Application Part
  - continue
- GSM Mobile Application
  - Component: returnResultLast (2)
    - returnResultLast
      - invokeId: 3
      - resultRetries
Double MAP in MITM attack
Double MAP in MITM attack

TCAP Begin
InsertSubscriberData_REQ
DeleteSubscriberData_REQ

TCAP Continue
InsertSubscriberData_REQ

TCAP End

IMS

SS7

STP

MSC/VLR

PBX

TCAP Continue
ReturnError

TCAP Continue
ReturnResultLast

TCAP End dtid(046a169f)

- MTP 3 User Adaptation Layer
- Signalling Connection Control Part
- Transaction Capabilities Application Part
- end
Double MAP in MITM attack

- TCAP Begin
  - InsertSubscriberData_REQ
  - DeleteSubscriberData_REQ

- TCAP Continue
  - InsertSubscriberData_REQ
  - InsertSubscriberData_REQ

- IMS
  - 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)

- PBX

- SS7

- STP

- MSC/VLR

- ReturnError
- ReturnResultLast
Double MAP in MITM attack

TCAP Begin
InsertSubscriberData_REQ
DeleteSubscriberData_REQ

TCAP Continue
InsertSubscriberData_REQ
InsertSubscriberData_REQ

TCAP End

IMS

No. | Protocol | Info
---|---------|---
1  | GSM MAP | invoke insertSubscriberData
2  | GSM MAP | invoke deleteSubscriberData
3  | GSM MAP | Invoke returnError
4  | GSM MAP | Invoke invoke insertSubscriberData
5  | GSM MAP | returnResultLast
6  | TCAP    | End dtdid(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: 8993
      - callingPartyCategory: operator, language English (2)
      - locationNumber:
      - bearerCapability: bearerCao (0)
      - eventTypeBCSM: collectedInfo (2)
      - IMSI: 8993 0786
Double MAP in MITM attack

TCAP Begin
- InsertSubscriberData_REQ
- DeleteSubscriberData_REQ

TCAP Continue
- InsertSubscriberData_REQ
- InsertSubscriberData_REQ

TCAP End

IMS

SS7

STP

MSC/VLR

PBX

TCAP Continue
- ReturnError
- 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)
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: 0000000000102
Voice call interception (MITM) on 4G/5G network

Attack via packet data service disruption
Fake registration on 2G/3G
Fake registration on 2G/3G

<table>
<thead>
<tr>
<th>No.</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GSM MAP</td>
<td>invoke updateLocation</td>
</tr>
<tr>
<td>2</td>
<td>GSM MAP</td>
<td>invoke insertSubscriberData</td>
</tr>
<tr>
<td>3</td>
<td>GSM MAP</td>
<td>returnResultLast</td>
</tr>
<tr>
<td>4</td>
<td>GSM MAP</td>
<td>invoke insertSubscriberData</td>
</tr>
<tr>
<td>5</td>
<td>GSM MAP</td>
<td>returnResultLast</td>
</tr>
<tr>
<td>6</td>
<td>GSM MAP</td>
<td>returnResultLast updateLocation</td>
</tr>
</tbody>
</table>

- **MTP 3 User Adaptation Layer**
- **Signalling Connection Control Part**
- **Transaction Capabilities Application Part**
  - **GSM Mobile Application**
    - Component: returnResultLast (2)
      - InvokeID: 1
      - resultRetres
        - opCode: localValue (0)
        - hlr-Number: \[\text{Redacted}\]
          - add-Capability

- **HSS/HLR**
- **IMS**
- **MME/SGW**
- **DEA**
- **IWF**

- **PBX**
- **SS7**
- **Diameter**

Voice ✗
Data ✓
Originating traffic redirection

<table>
<thead>
<tr>
<th>No.</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GSM MAP</td>
<td>invoke updateLocation</td>
</tr>
<tr>
<td>2</td>
<td>GSM MAP</td>
<td>invoke insertSubscriberData</td>
</tr>
<tr>
<td>3</td>
<td>GSM MAP</td>
<td>returnResultLast</td>
</tr>
<tr>
<td>4</td>
<td>GSM MAP</td>
<td>invoke insertSubscriberData</td>
</tr>
<tr>
<td>5</td>
<td>GSM MAP</td>
<td>returnResultLast</td>
</tr>
<tr>
<td>6</td>
<td>GSM MAP</td>
<td>returnResultLast updateLocation</td>
</tr>
<tr>
<td>7</td>
<td>GSM MAP</td>
<td>invoke provideRoamingNumber</td>
</tr>
</tbody>
</table>

LIR – Location Information Request

- MME/SGW
- DEA
- IMS
- HSS/HLR
- IWF

INVITE (A, B)

ProvideRoamingNumber (IMSI)

PBX

SS7

Diameter
Originating traffic redirection

<table>
<thead>
<tr>
<th>No.</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GSM MAP</td>
<td>invoke updateLocation</td>
</tr>
<tr>
<td>2</td>
<td>GSM MAP</td>
<td>invoke insertSubscriberData</td>
</tr>
<tr>
<td>3</td>
<td>GSM MAP</td>
<td>returnResultLast</td>
</tr>
<tr>
<td>4</td>
<td>GSM MAP</td>
<td>invokeInsertSubscriberData</td>
</tr>
<tr>
<td>5</td>
<td>GSM MAP</td>
<td>returnResultLast</td>
</tr>
<tr>
<td>6</td>
<td>GSM MAP</td>
<td>returnResultLast updateLocation</td>
</tr>
<tr>
<td>7</td>
<td>GSM MAP</td>
<td>invoke provideRoamingNumber</td>
</tr>
<tr>
<td>8</td>
<td>GSM MAP</td>
<td>returnResultLast_provideRoamingNumber</td>
</tr>
</tbody>
</table>

- LIR – Location Information Request
- LIA – Location Information Answer

Key Components:
- MME/SGW
- DEA
- IWF
- DE4/5G
- PBX
- SS7
- Diameter

Processes:
- INVITE (A, PBX)
- ProvideRoamingNumber (IMSI)
- ProvideRoamingNumber (PBX)
- LIR
- LIA

Voice: ✗
Data: ✓
What's the next?

LIR – Location Information Request
LIA – Location Information Answer

INVITE (A, B)

MME/SGW

DEA

HSS/HLR

IMS

LIR

ProvideRoamingNumber (IMSI)

ProvideRoamingNumber (PBX)

LIA (PBX)

INVITE (A, PBX)

IWF

PBX

SS7

4G/5G

Voice

Data

Diameter
Case 1. Packet data disruption

On SS7 network

<table>
<thead>
<tr>
<th>No.</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GSM MAP</td>
<td>invoke updateGPRSLocation</td>
</tr>
<tr>
<td>2</td>
<td>GSM MAP</td>
<td>invoke insertSubscriberData</td>
</tr>
<tr>
<td>3</td>
<td>GSM MAP</td>
<td>returnResult last</td>
</tr>
<tr>
<td>4</td>
<td>GSM MAP</td>
<td>returnResult last updateGPRSLocation</td>
</tr>
</tbody>
</table>

- **4G/5G**
- **MME/SGW**
- **HSS/HLR**
- **IMS**
- **PBX**
- **SS7**
- **Diameter**

Voice Data
Service restoration

ULR – Update Location Request
ULA – Update Location Answer

MME/SGW
HSS/HLR
IMS
DEA
IWF
PBX
SS7
Diameter

4G/5G

Voice
Data
Terminating traffic initiation
Case 2. Packet data disruption

On Diameter network

<table>
<thead>
<tr>
<th>No.</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DIAMETER</td>
<td>cmd=3GPP-Cancel-Location Request(317)</td>
</tr>
<tr>
<td>2</td>
<td>DIAMETER</td>
<td>cmd=3GPP-Cancel-Location Answer(317)</td>
</tr>
</tbody>
</table>

CLR – Cancel Location Request
CLA – Cancel Location Answer

Voice
Data

4G/5G

PBX

SS7

Diameter
Service restoration
Terminating traffic initiation
Subscription fraud

Attack on SS7 and GTP networks
Subscription fraud via SS7/GTP

<table>
<thead>
<tr>
<th>No.</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GSM MAP</td>
<td>invoke updateLocation</td>
</tr>
</tbody>
</table>

- **Signalling Connection Control Part**
- **Transaction Capabilities Application Part**
- **GSM Mobile Application**
  - Component: invoke (1)
    - Invoke
      - InvokeID: 1
      - opCode: localValue (0)
      - IMSI: 
      - nsc-Number: 
      - vlr-Number: 
      - vlr-Capability

Diagram:
- HLR
- GGSN
- STP
- SS7
- Web server
- GTP
- Positive Technologies
Subscription fraud via SS7/GTP

<table>
<thead>
<tr>
<th>No.</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GSM MAP</td>
<td>invoke updateLocation</td>
</tr>
<tr>
<td>2</td>
<td>GSM MAP</td>
<td>invoke InsertSubscriberData</td>
</tr>
</tbody>
</table>

- **SS7**
- **Web server**
- **GTP**
- **HLR**
- **GGSN**
- **STP**

*Signalling Connection Control Part*  
*Transaction Capabilities Application Part*  
*GSM Mobile Application*  
*Component: invoke (1)*

- **Invoke**
  - **invokeID**: 4
  - **opCode**: localValue (0)
  - **msisdn**: [redacted]
  - **category**: 0
  - **subscriberStatus**: serviceGranted (0)
  - **bearerServiceList**: 2 items

*InsertSubscriberData (MSISDN)*  
*UpdateLocation (IMSI)*
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

GSM MAP

STP

InsertSubscriberData (MSISDN)

UpdateLocation (IMSI)

HLR

GGSN

GTP

Web server

SS7

Positive Technologies
Subscription fraud via SS7/GTP

- GPRS Tunneling Protocol
  - Flags: 0x32
  - Message Type: Create PDP context request (0x10)
  - Length: 107
  - TEID: 0x00000000 (0)
  - Sequence number:
  - INST: 
  - GSN address: 
  - MS International PSTN/ISDN number
    - Length: 7
      - ... = Extension: No Extension
      - .001 = Nature of number: International Number
      - ... .001 = Number plan: ISDN/Telephony Numbering
      - E.164 number (MSISDN):

- HLR
- GGSN
- UpdateLocation (IMSI)
- InsertSubscriberData (MSISDN)
- STP
- CreatePDPContext Request (IMSI, MSISDN)
- GTP
- SS7
- Web server
Subscription fraud via SS7/GTP

<table>
<thead>
<tr>
<th>No.</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GTP</td>
<td>Create PDP context request</td>
</tr>
<tr>
<td>2</td>
<td>GTP</td>
<td>Create PDP context response</td>
</tr>
</tbody>
</table>

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

Web server

CreatePDPContext Request (IMSI, MSISDN)
CreatePDPContext Response (GSN IP)

GGSN

UpdateLocation (IMSI)
InsertSubscriberData (MSISDN)

HLR

UpdateLocation (IMSI)
InsertSubscriberData (MSISDN)

STP

SS7
Subscription fraud via SS7/GTP

<table>
<thead>
<tr>
<th>No.</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GTP</td>
<td>Create POP context request</td>
</tr>
<tr>
<td>2</td>
<td>GTP</td>
<td>Create POP context response</td>
</tr>
<tr>
<td>3</td>
<td>GTP &lt;HTTP&gt;</td>
<td>GET /success.txt HTTP/1.1</td>
</tr>
</tbody>
</table>


HLR

GGSN

STP

CreatePDPContext Request (IMSI, MSISDN)

CreatePDPContext Response (GSN IP)

HTTP request

InsertSubscriberData (MSISDN)

UpdateLocation (IMSI)

UpdateLocation (IMSI)

InsertSubscriberData (MSISDN)

SS7

Web server

HTTP request
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.

Continual real time monitoring is essential to measure network security efficiency and provide rapid detection and mitigation.

Monitor

Protect

Assess

Auditing provides the essential visibility to fully understand your ever changing network risks.

Completely secure your network by addressing both generic vulnerabilities (GSMA) and the threats that actually affect you as an ongoing process.
Thank you

Sergey Puzankov
sergey.puzankov@positive-tech.com