



GPRS Tunnelling Protocol (GTP) Security

Version 6.1

21 April 2023

Security Classification: Confidential - Operator, Rapporteur, Industry and Sector Members

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2025 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contained herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1	Introduction	4
1.1	Overview	4
1.2	Scope	4
1.3	Definitions	5
1.4	Abbreviations	5
1.5	References	7
2	Affected Mobile Network Operators and Technical Background	9
2.1	All Mobile Network Operators are Affected	9
2.2	GTP Brief Technical Background	9
3	Attacks, Exploitation and Risks	14
3.1	Network Topology and Reachability of Network Elements	14
3.2	GTP-Related Attacks	16
3.2.1	Information Gathering	16
3.2.2	Subscriber Denial of Service (DoS) Attack	19
3.2.3	Fraud	20
3.2.4	Location Tracking	24
3.3	Missing Binding of Network Interfaces to 3GPP Interfaces	25
3.4	Malicious Peers and Faulty Behaviour Experienced as Attack	25
3.5	Vulnerabilities on Network Elements	26
4	Countermeasures	27
4.1	Secure Network Architecture	28
4.1.1	Basic Network Security	29
4.1.2	Network (IP) Layer and Transport Layer Security	30
4.1.3	Further Reading on Fundamental Network Security	31
4.2	Network Element Security	32
4.3	GTP Security	32
4.3.1	GTP Message Filtering Categories	32
4.3.2	GTP Category 1 – Interface-Unauthorised Packet	33
4.3.3	GTP Category 2 – Home-Network Packet	34
4.3.4	GTP Category 3 – Plausible-Network Packet	35
4.3.5	Plausibility of GTP Messages and GTP message validation	35
4.3.6	Protection against Manipulated and Fake GTP Messages	39
4.3.7	Protection Against Location Data Leakage	39
4.4	Effectiveness and Coverage of Countermeasures	39
5	Summary of attacks	41
6	Resources and Complexity	46
Annex A	List of GTP Messages	47
A.1	GTP Messages of the S8 Interface (GTPv2)	47
A.2	GTP Messages of the Gp Interface (GTPv1)	48
A.3	GTP Messages of the Gp Interface (GTPv0)	49
Annex B	GTP Risk Classification	51
Annex C	GTP Firewall Recommendations	52

C.1	Introduction	52
C.2	Definitions	52
C.3	GTP Firewall Rules	54
C.3.1	General	54
C.3.2	Low-Layer Format Filtering	57
C.3.3	Category 1 Filtering	57
C.3.4	Category 2 Filtering	58
C.3.5	Category 3 Filtering	59
C.4	Firewall Node Hardening	59
C.5	Firewall Data Sharing	59
C.5.1	General	59
C.5.2	GTP Firewall Data Sharing	60
C.5.3	Data Sharing for GTP Analytics	60
C.5.4	Data Sharing for GTP Monitoring	61
C.6	Implementation of a GTP firewall in the network	62
C.6.1	Combined Firewall (IP + APP)	62
C.6.2	Dedicated GTP Firewall for GTP-C and GTP-U	63
C.6.3	Dedicated GTP Firewall for GTP-C	63
Annex D	Document Management	65
D.1	Document History	65
D.2	Other Information	66

1 Introduction

1.1 Overview

This document describes attacks on the mobile core network performed through the General Packet Radio Service (GPRS) Exchange (GRX) or Internet Protocol Exchange (IPX) network or the internet. The GPRS Tunnelling Protocol (GTP) that is used between roaming partners on the GRX/IPX network is the target of the attackers. They either abuse the GTP interface exposed to the network, or they send their own messages to the network element (NE) in order to receive messages back that reveal information the attackers are interested in.

This document briefly explains the issues and presents the types of attacks a mobile network is exposed to, before it addresses mitigation strategies and countermeasures. This document is intended to be read by staff of mobile network operators (MNOs) to determine what additional security measures should be implemented on their networks to prevent the attacks described here. IPX providers are affected if they process GTP messages on behalf of their customer MNOs (see section 2.1).

The topic of signalling security has received extra attention since SS7 research in 2014 highlighted security vulnerabilities associated with that protocol suite. Security researchers publicly explained and demonstrated what can be done to mobile networks and mobile subscribers when an attacker has access to the SS7 network. Additional publicised research on GTP and Diameter followed in 2015. To protect their businesses and customers, MNOs are recommended to familiarise themselves with GTP security and to apply the countermeasures that are described in this document.

1.2 Scope

This document provides a technical background on how GTP is used, introduces attacks and exploitation possibilities, and derives associated risk. It then presents countermeasures for MNOs to protect their networks against attacks that involve GTP.

GTP is used in 2G (GPRS), 3G (Universal Mobile Telecommunications System / UMTS), and 4G (Long Term Evolution / LTE) networks. As a consequence, the attacks, exploitation possibilities, and countermeasures described here are applicable to all radio technologies and thus they are relevant for all MNOs.

The focus of this document is on protection of a mobile network against attacks from the outside. As a consequence, only NEs that are connected to the outside and that exchange GTP messages with other networks are relevant. They are used for international roaming and for connecting user equipment (UE) to other networks, e.g. the internet or virtual private networks (VPNs) of corporate customers. Use of GTP in international roaming is defined in GSMA PRD IR.88 [17] for the evolved packet core (EPC) and in GSMA PRD IR.33 [14] for earlier core network technologies.

In addition, the GTP Risk Classification can be found in Annex B and the recommendations for GTP firewall in Annex C. For GTP firewall, please refer to section C.3.1.1 for a detailed scope description of the GTP firewall rules, which is a simple set of filtering rules in the current version of the document as explained in sections C.1 and C.3.1.4, as well as section C.6 for the implementation of a GTP firewall in the network.

The following protocols are out of scope of this document:

- GTP prime (GTP');
- General GRX/IPX security (captured in PRD IR.77 [15]);
- SS7 and Signalling Transport (SIGTRAN) network security (covered in PRD FS.07 [10] and FS.11 [11]); and
- Diameter security (covered in GSMA PRD FS.19 [12]).

This document addresses GTP based signalling and specifically focuses on the security of GTP as Control Plane protocol (GTP-C).

1.3 Definitions

Term	Description
Network element	Any active component on the network that implements certain functionality that is involved in sending, receiving, processing, storing, or creating data packets. Network elements are connected to networks. In the mobile network, components like the Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), Mobility Management Entity (MME), Serving Gateway (SGW), Packet Data Network Gateway (PGW), Home Location Register (HLR), Home Subscriber Server (HSS), and GTP firewall, as well as routers and gateways, are network elements.

1.4 Abbreviations

Term	Description
3GPP	3 rd Generation Partnership Project
APN	Access Point Name
BSC	Base Station Controller
CGF	Charging Gateway Function
CHAP	Challenge Handshake Authentication Protocol
DoS	Denial of Service
DPI	Deep Packet Inspection
EPC	Evolved Packet Core
FIB	Forwarding Information Base
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSMA	GSM Association
GRX	GPRS Exchange
GTP	GPRS Tunnelling Protocol
GTP-C	GPRS Tunnelling Protocol Control Plane
GTP-U	GPRS Tunnelling Protocol User Plane
GTP'	GTP Prime
GUTI	Globally Unique Temporary Identifier
HPLMN	Home Public Land Mobile Network
HLR	Home Location Register

Term	Description
HSS	Home Subscriber Server
IANA	Internet Assigned Numbers Authority
IDS	Intrusion Detection System
IE	Information Element
IMSI	International Mobile Subscriber Identity
IPX	Internet Protocol Exchange
LAG	Link Aggregation Group
LTE	Long Term Evolution
MAC	Media Access Control
MCC	Mobile Country Code
MITM	Man In The Middle
MME	Mobility Management Entity
MNC	Mobile Network Code
MNO	Mobile Network Operator
MPLS	Multiprotocol Layer Switching
MS	Mobile Station
NE	Network Element
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PGW	Packet Data Network (PDN) Gateway
PLMN	Public Land Mobile Network
PPP	Point to Point Protocol
PRD	Permanent Reference Document
RAEX	Roaming Exchange
RAN	Radio Access Network
RAT	Radio Access Technology
RNC	Radio Network Controller
SCTP	Stream Control Transmission Protocol
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SIGTRAN	Signalling Transport
SSH	Secure Shell
TEID	GTP Tunnel Endpoint Identifier
TCP	Transport Control Protocol
TFT	Traffic Flow Template
TLV	Type-Length-Value
TMSI	Temporary Mobile Subscriber Identity
UDP	User Datagram Protocol

Term	Description
UE	User Equipment
ULI	User Location Information
UMTS	Universal Mobile Telecommunications System
VLAN	Virtual Local Area Network
VPLMN	Visited Public Land Mobile Network
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding

1.5 References

Ref	Doc Number	Title
[1]	3GPP TS 09.60	"General Packet Radio Service (GPRS); GPRS Tunnelling Protocol GPT) across the Gn and Gp Interface".
[2]	3GPP TS 29.060	"General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".
[3]	3GPP TS 29.274	"3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".
[4]	3GPP TS 29.281	"General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)".
[5]	3GPP TS 32.295	"Telecommunication management; Charging management; Charging Data Record (CDR) transfer".
[6]	3GPP TS 33.117	"Catalogue of General Security Assurance Requirements".
[7]	Creutzburg	Reiner Creutzburg et al., Wikipedia Handbook of Computer Security and Digital Forensics 2016 – Part I – Computer Security, ebook, ResearchGate, January 2016; https://www.researchgate.net/publication/296669124
[8]	Maiwald	Eric Maiwald: Network Security A Beginner's Guide, 3 rd ed., McGraw-Hill Education, 2013.
[9]	Nohl	Karsten Nohl, Luca Melette: Advanced interconnect attacks – Chasing GRX and SS7 vulns; Chaos Communication Camp 2015, 13 August 2015, Mildenberg, Germany; video on CCC Web site .
[10]	GSMA PRD FS.07	"SS7 and SIGTRAN Network Security".
[11]	GSMA PRD FS.11	"SS7 Interconnect Security Monitoring and Firewall Guidelines".
[12]	GSMA PRD FS.19	"Diameter Roaming Security".
[13]	GSMA PRD IR.21	"GSM Association Roaming Database, Structure and Updating Procedures".
[14]	GSMA PRD IR.33	"GPRS Roaming Guidelines".
[15]	GSMA PRD IR.77	"InterOperator IP Backbone Security Req. For Service and Inter-operator IP backbone Providers".

Ref	Doc Number	Title
[16]	GSMA PRD IR.85	“Roaming Hubbing Provider Data, Structure and Updating Procedures”.
[17]	GSMA PRD IR.88	“LTE and EPC Roaming Guidelines”.
[18]	Security Configuration Guidance	National Security Agency, Information Assurance, Security Configuration Guidance,, https://www.iad.gov/iad/library/ia-guidance/security-configuration/index.cfm .
[19]	Kacer	Martin Kacer: SS7, Diameter, GTP Security. GTP screening recommendations, 2016, https://www.h21lab.com/telecom-security/presentations .
[20]	Kacer, Langlois	Martin Kacer, Philippe Langlois: SS7 Attacker Heaven turns into Riot: How to make Nation-State and Intelligence Attackers life much harder on mobile networks. Black Hat USA, 2017.
[21]	Positive Technologies	Threats to Packet Core Security of 4G, 2017 https://www.ptsecurity.com/upload/iblock/772/EPC_research.pdf .
[22]	GSMA PRD FS.21	“Interconnect Signalling Security Recommendations”
[23]	GSMA RIFS#103 Doc 005	“New Variants for Data Interception & Location Tracking”, Fabrício Ferraz (MEO/Altice Portugal), Silke Holtmanns (AdaptiveMobile Security)
[24]	GSMA RIFS#109 Doc 006	“TEID Analysis and new GTP attack full MITM”, Fabrício Ferraz (Meo/Altice Portugal)

2 Affected Mobile Network Operators and Technical Background

2.1 All Mobile Network Operators are Affected

Signalling security vulnerabilities affect all MNOs worldwide. Attackers can reconfigure Nes in the mobile core network, obtain session keys of subscribers to decrypt air interface communications, and obtain information about subscribers such as location, called numbers, and more.

In the interest of keeping full control over their networks and in protecting customer data, it is essential for all MNOs to determine what countermeasures are needed to prevent successful attacks, and to deploy these countermeasures.

All MNOs are recommended to assess the risk they are exposed to and to decide what mitigation steps to take. This document intends to help, as it provides the necessary technical background, and explains risk exposure and possible countermeasures.

If MNOs outsource some of their activities, e.g. name resolution, routing, filtering, to their GRX/IPX providers, they should note that the GRX/IPX providers are then responsible for the associated security measures, and the countermeasures in this document should then be applied by the GRX/IPX providers. However, if a MNO only uses the GRX/IPX network as a pure transport network for GTP messages and does all processing of GTP messages in its own networks, it is solely responsible for the associated security.

2.2 GTP Brief Technical Background

GTP is one of the major network protocols that is used for exchanging messages between Nes on the mobile network. GTP is defined by the 3GPP via [1], [2], [3], [4] and [5]. It is used between various Nes. The link between each pair of different types of Nes has its own interface name, and a subset of GTP messages are specified as valid on this interface.

GTP-C is the control part of GTP and uses the User Datagram Protocol (UDP) port 2123 (assigned by the Internet Assigned Numbers Authority (IANA)). Several control messages in the core network are delivered over GTP-C, for example session management, context information delivery and location information management. This is done to provide internet access to UE. Until the development of LTE, 3GPP had specified two variants of GTP-C, based on GTPv1 and GTPv2. The specification of GTPv2-C can be found in 3GPP TS 29.274 [3] and updates the specification of GTPv1 in TS 29.060 [2]. Because of downwards compatibility of the 3GPP architecture, both variants of GTP-C may be found in a PLMN. Additionally, legacy GTP-C v0 can also be found implemented inside network elements which use the User Datagram Protocol (UDP) port 3386.

GTP-U is the part of the GTP protocol responsible for carrying encapsulated user data and signalling messages between two tunnel endpoints. Signalling messages are path management or tunnel management functions like *Echo Request/Response* and *Error Indication* functions. GTPv1-U is specified in 3GPP TS 29.281 [4].

GTP' is used for carrying charging data to the charging gateway function inside the domain of a single MNO. GTP' is defined in TS 32.295 [5].

Within the domain of a MNO, several GTP interfaces are used: e.g. Gn for GPRS and UMTS, and mainly S11, S10 and S5 for LTE. Gn uses GTPv1, and S11, S10, S5 use GTPv2.

Only two 3GPP interfaces are used between MNOs: Gp is used for GPRS and UMTS, as indicated in Figure 1. S8 is used for LTE and beyond, as indicated in Figure 2. Gp uses GTP v1, and S8 uses GTP v2.

GTP v0 [1] may be used occasionally within MNOs that have old Nes deployed, but it is considered deprecated.

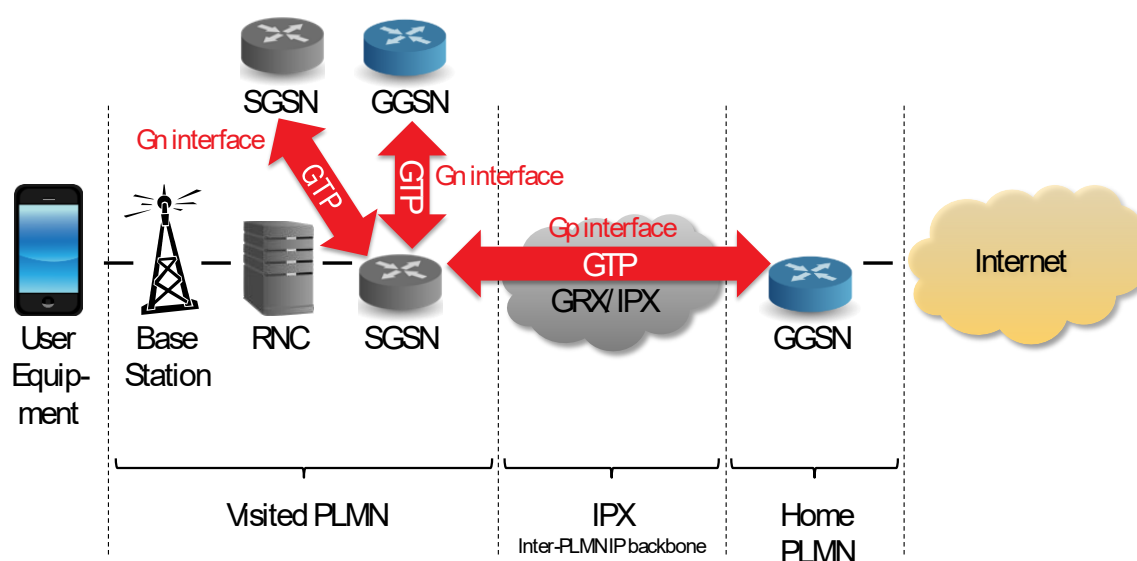


Figure 1 – GTP Interfaces (Gn, Gp) within and between MNOs

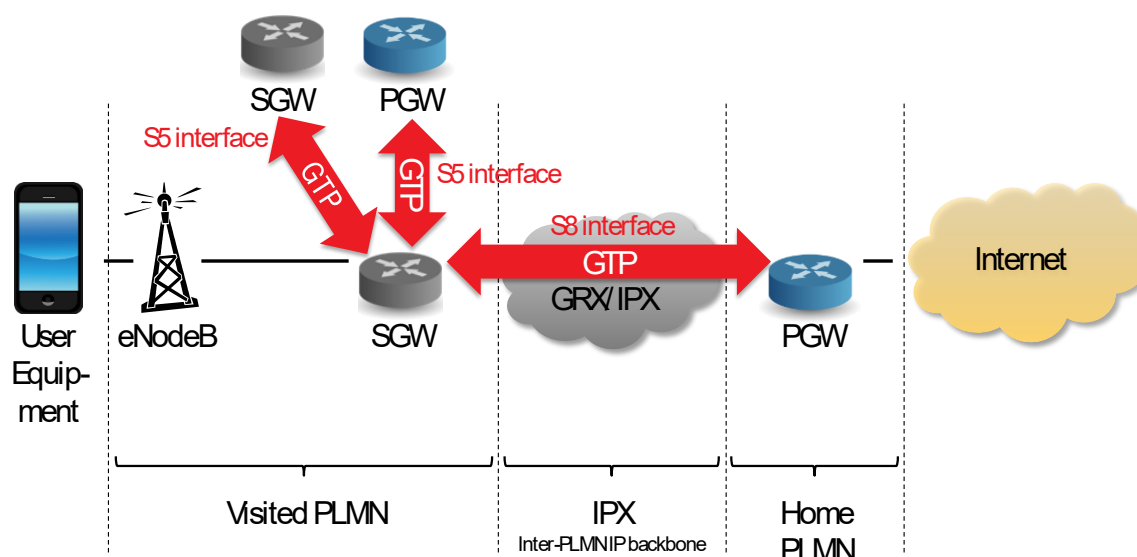


Figure 2 – GTP Interfaces (S5, S8) within and between MNOs

GTP is used in the 2.5G (GPRS), 3G (UMTS) and 4G (LTE) releases of the mobile networking standards. In GPRS and UMTS, the SGSN and the GGSN are the two most relevant Nes that use GTP. These two Nes are connected to various other Nes and

networks. Each connection exists for a particular purpose. Some of these connections leave the domain of the MNO. As a consequence, SGSNs and GGSNs are reachable from other networks too.

The SGSN is connected to the GGSN by the Gn interface, to base stations by the IuPS interface, and via the base stations to the UE, as illustrated in Figure 3. It is also connected to other Nes in the core network, such as the HLR (Gr interface). The SGSN also has a direct connection to the GRX/IPX network and is therefore reachable by all other MNOs via the Gp interface.

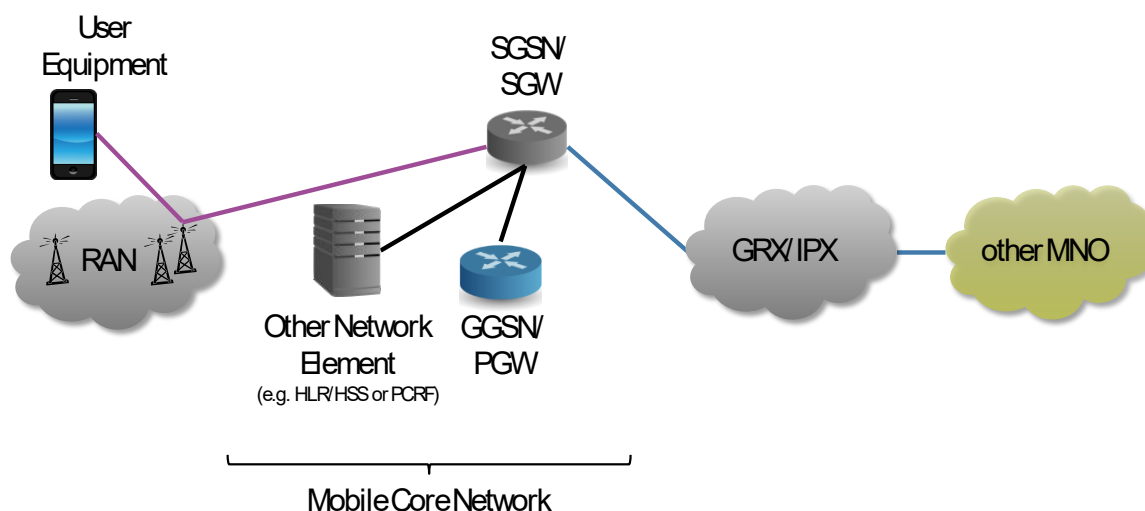


Figure 3 – Connections of the SGSN/SGW to other Nes and networks

The GGSN is connected to the SGSN and to other Nes in the core network, such as the charging gateway function (CGF). See Figure 4. It is also connected to the internet via the Gi interface, to the GRX/IPX network via the Gp interface, and to additional private networks, such as the VPNs of corporate customers.

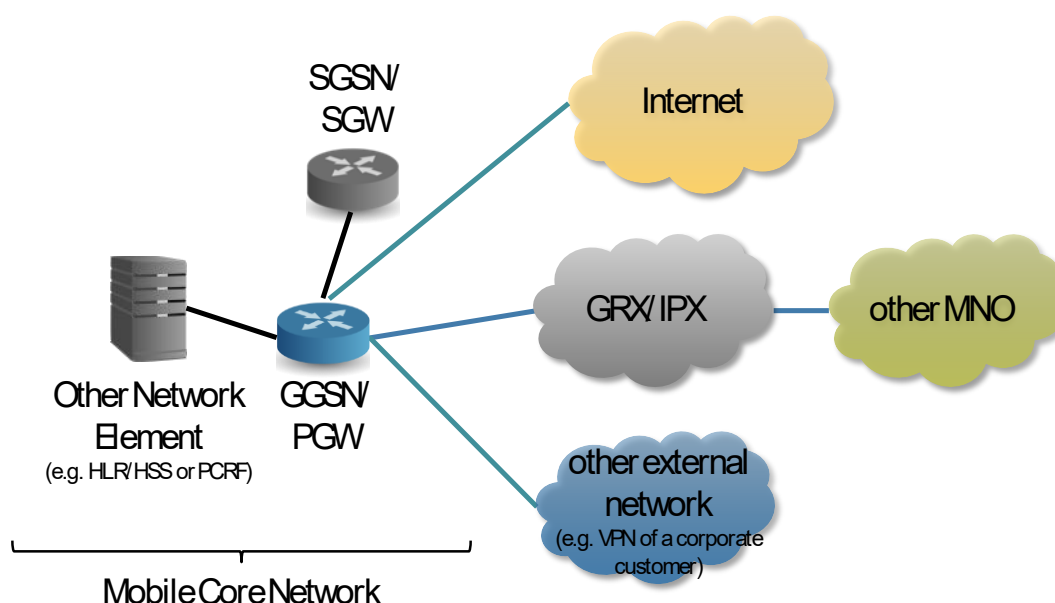


Figure 4 – Connections of the GGSN/PGW to other Nes and networks

The combined picture is depicted in Figure 5. These connections transport user data, signalling data, or both.

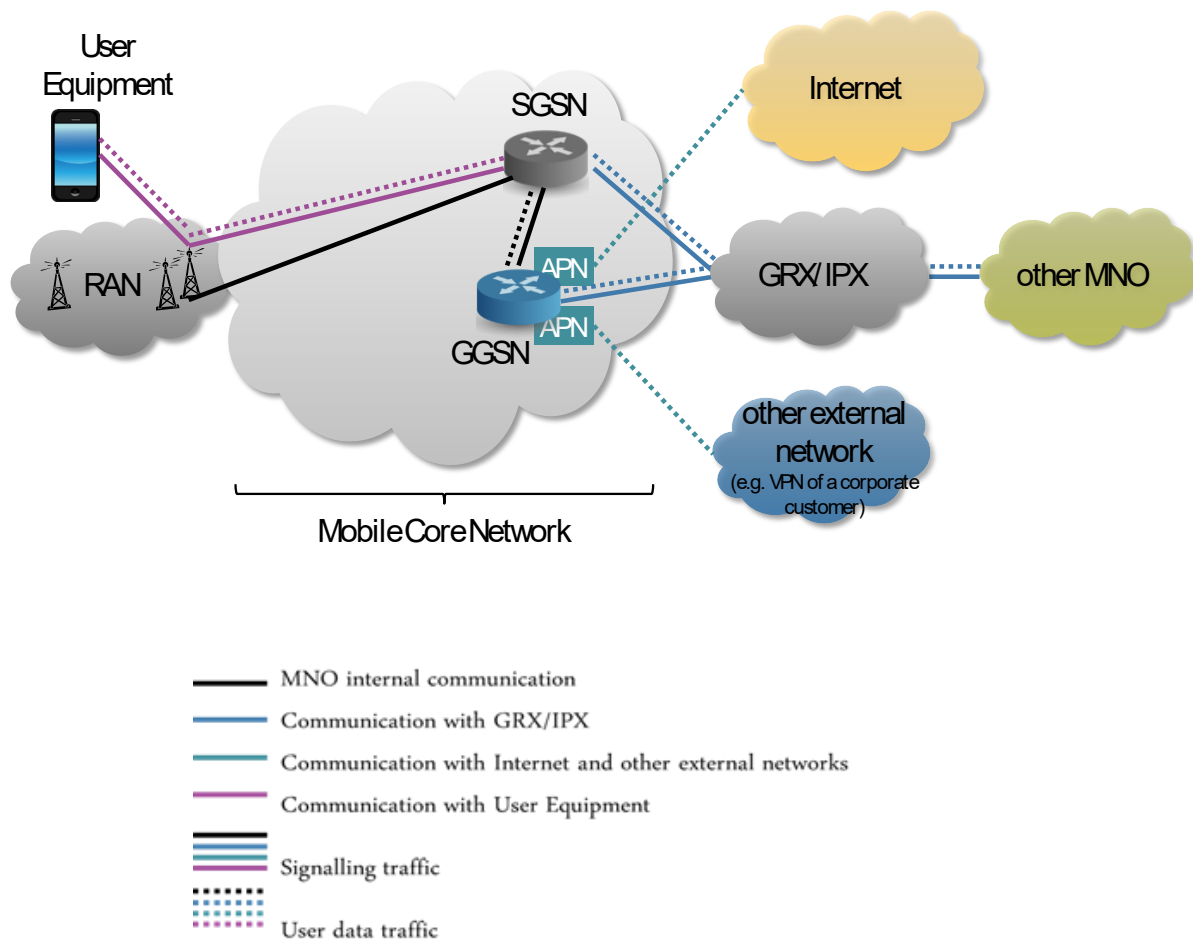


Figure 5 – Relevant connections where GTP is used in 2G and 3G

In LTE networks, the MME, the SGW and the PGW are the most relevant Nes that use GTP. Like in GPRS and UMTS networks, these Nes are connected to various other Nes and networks and connections exist for a particular purpose. Some of these connections leave the domain of the MNO and as a consequence the Nes are reachable from other networks too. Figure 6 depicts the connections in LTE.

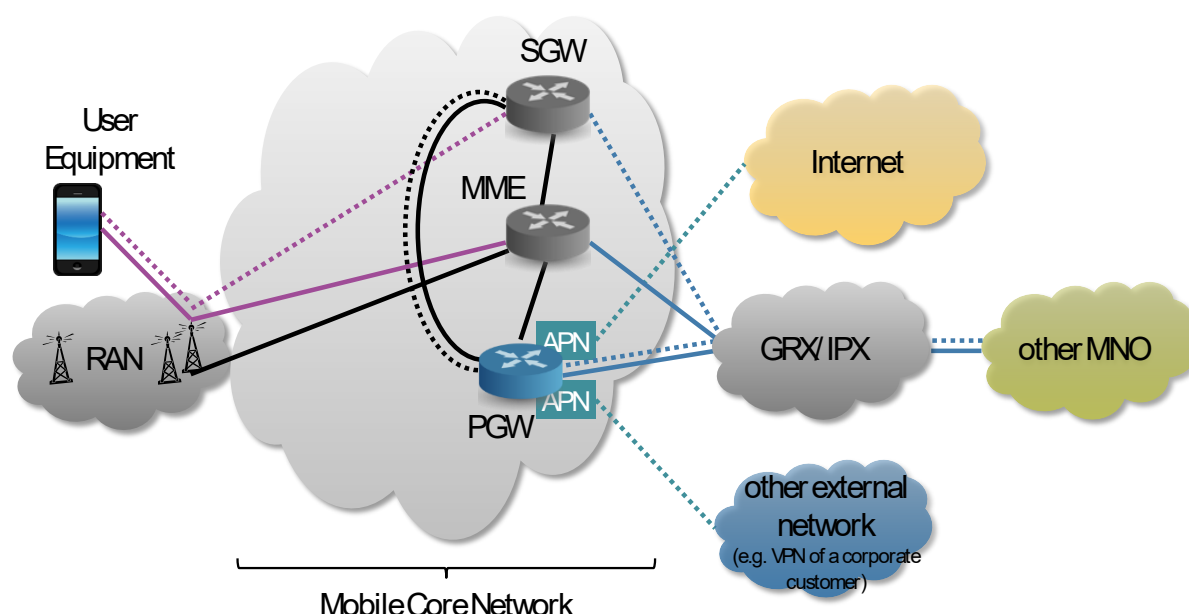


Figure 6– Relevant connections where GTP is used in LTE

In LTE, the role of the SGSN is split: The MME takes care of GTP-C traffic while the SGW handles GTP-U traffic. The MME is connected to the SGW via the S11 interface and to other MMEs via S10.

The SGW has a connection to PGW via S5, to eNodeB via S1-U and it is also directly connected to the GRX/IPX network and reachable there by all other MNOs via the S8 interface. See Figure 3 and Figure 5.

The PGW is connected to the home SGW via S5 and to other Nes in the core network. It is also connected to the internet via the Sgi interface and to the GRX/IPX network via S8. Like the GGSN, it is also connected to additional networks, such as VPNs of corporate customers. See Figure 4 and Figure 5.

For security considerations, the network topology, the borders of domains and the established connections are relevant. Since MNOs are interested in protecting Nes that are capable of GTP, they should be aware of which types of entity outside the domain of the MNO can send and receive GTP messages to and from the mobile network. This is described in section 3.1 of this document.

For handovers from one SGSN to the other, for example, the GTP message pair *SGSN Context Request* and *SGSN Context Response* are used. The existing SGSN sends to the new SGSN all the details that the new SGSN needs to serve the UE, as shown in Figure 7.

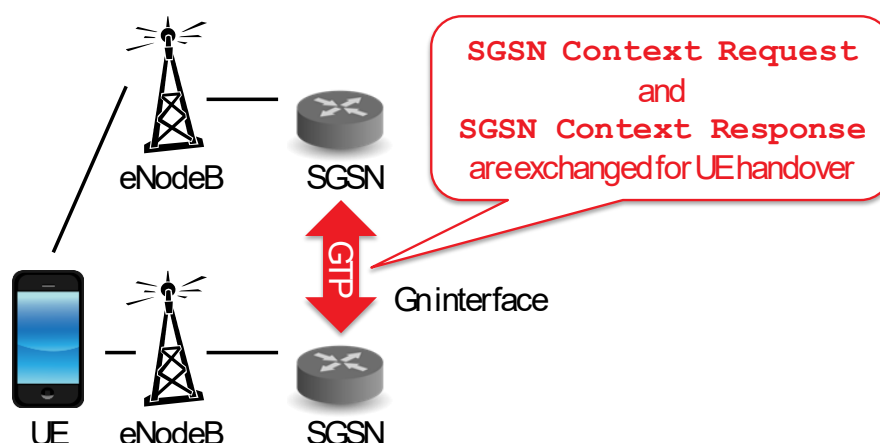


Figure 7 – Handover of a UE to a new SGSN

GTP is being used for more than what has been described in this section. The explanations provided here are limited to what is needed for the reader to understand the attacks and countermeasures described in following sections of this document. For further details on GTP, the reader is referred to the 3GPP specifications TS 09.60 [1], TS 29.060 [2], TS 29.281 [4], and TS 29.274 [3].

3 Attacks, Exploitation and Risks

In August 2015 a security researcher published ways to attack MNOs via the GRX/IPX network and the internet using GTP-C messages [9]. This was the trigger for a systematic risk analysis within some MNOs to determine the attack potential, the risks that go with the identified attacks and the gain for the attacker. As a result, countermeasures that are effective for protecting a mobile network and its subscribers were derived.

A variety of attacks have already been successfully performed on production network equipment of MNOs.

Exposure of Nes to these attacks allows attackers to exploit the mobile network by reconfiguring Nes for their purposes, by using Nes that are controlled by attackers to jump deeper inside the network to other Nes, by decrypting subscriber's packet data sessions, and by hijacking existing internet sessions of subscribers. Research is ongoing. Additional research and exploitation on this subject is likely in the future.

3.1 Network Topology and Reachability of Network Elements

A prerequisite for an attacker to succeed is that the target is reachable on a network. The Nes in the mobile network are connected to other networks but always for a particular purpose. This should be reflected in the network topology and network configuration.

The SGSN/SGW and the GGSN/PGW are exposed to the GRX/IPX network and reachable via that network. The Gp/S8 interface must be accessible for roaming partners, but only for roaming partners and not for any other parties. Any other interfaces/services that are not needed on the GRX/IPX network should not be exposed to it. See Figure 8.

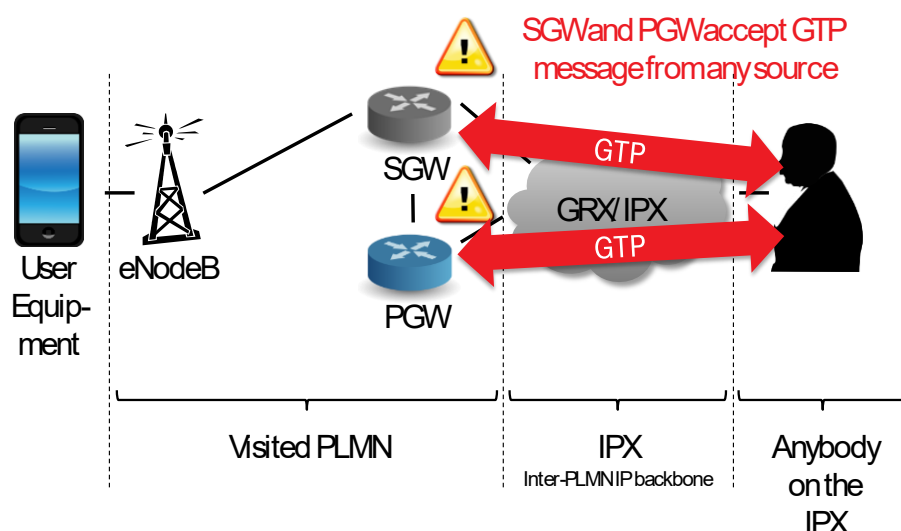


Figure 8 – Risk: The SGW may accept GTP messages from any source on the IPX Network

The GGSN/PGW also needs to be connected to the internet to allow subscribers using the internet access point name (APN) to actually access the internet through the Gi/Sgi interface. There is no need for any entity to access the GGSN/PGW as a network element (NE) directly from the internet and therefore it should not be visible there. The APN only needs to connect Ues to the internet and assign IP addresses to the Ues, but there is no need to offer services on the GGSN/PGW to the internet. See Figure 9.

Packet data from the UE needs to be forwarded to the internet. The SGSN/SGW facilitates this by receiving IP packets from the UE, encapsulating them in GTP-U messages on the Gb/IuPS/S1-U interface and forwarding them to the GGSN/PGW. The SGSN/SGW needs to receive and forward this encapsulated UE traffic from the BSC/RNC/eNodeB (referred to in former 3GPP releases as the radio network controller (RNC)/ base station controller (BSC)). The UE does not need to address any IP packets to the SGSN/SGW with the SGSN/SGW IP address as destination. None of the network services of the SGSN/SGW need to be accessible for the UE. See Figure 9. Likewise, the UE does not need to address any other NE in the core network.

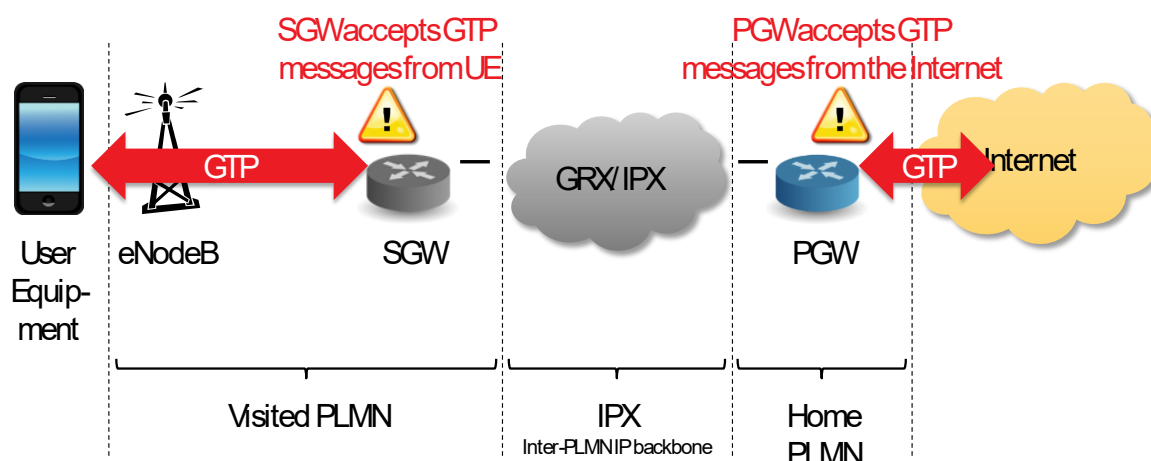


Figure 9 – Risk: The SGW and PGW may accept GTP message from any UE and from the internet

Any network service that is running on the exposed NE can be reached and used or abused through the connected networks if no countermeasures are taken. Most of the services are only needed on certain networks. For example, maintenance services like secure shell (SSH) only need to be accessed by maintenance terminals connected to an internal network. Such services should not be exposed to external networks, i.e. the internet, the GRX/IPX network, and other networks that are connected through APNs on the GGSN/PGW.

3.2 GTP-Related Attacks

3.2.1 Information Gathering

3.2.1.1 GTP Node Discovery

Any potential attacker with access to the GTP interface on the network can send valid GTP messages to the NE. The NE will process the message, send a response message, and will thereby disclose information. This can be abused to collect information about the NE itself and/or about subscribers.

Even an error response message or an *Echo Response* GTP message can reveal useful information to an attacker. If such a GTP message is sent, the attacker can learn that this NE is capable of GTP and often enough the attacker can determine the type of the NE. This is the first step of preparing more sophisticated attacks.

3.2.1.2 TEID Guessing

The most important ID in the GTP protocol is the Tunnel Endpoint Identifier (TEID). There are several methods for an attacker to figure out valid TEID, for example by sending GTP-U messages with incrementing TEID and any payload to P-GW via S8 interface, or to GGSN via Gp. If the TEID is invalid, a NE will in most cases send an error indication, otherwise – none. TEID brute force/guessing can also be performed using GTP-C messages like for example *GTP-C Delete PDP Context Request* or *Delete Session Request*.

It has been highlighted that TEID is 32-bit number field, this mean that 2^{32} attempts to exhaust all possibilities would be needed during a [brute force search](#). If a limited number of bits are used to generate TEIDs, the number of attempts is reduced accordingly.

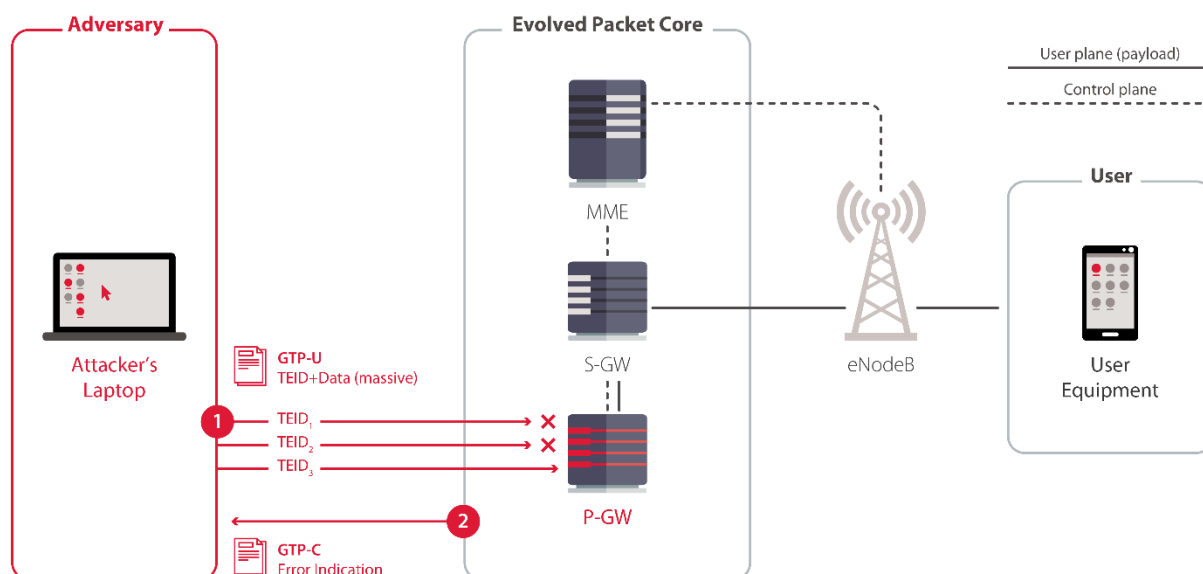


Figure 10 – Risk: Valid TEID brute force

Another way to obtain TEID is based on the use of GTP-C *Create Session Request* for GTPv2 or *Create PDP Context Request* for GTPv1.

To discover the algorithm implemented for TEID generation, an attacker can send, for example, multiple consecutive *Session Create Requests* to the target PGW and check the TEID proposed by the PGW in the F-TEID Information Element of the *Create Session Response*. It may be possible to observe that the TEIDs sent back in the *Create Session Response* were simply derived by incrementally increasing subsequent values or were derived using just a limited number of bits of the available 32. In this attack scenario, an attacker just needs to reach a target PGW and send this message with a minimal set of les; no other particular pre-conditions are needed. Passive network capture of GTP-C and GTP-U protocol messages could also be used to perform TEID entropy analysis.

TEID analysis described in [24] highlights that many implementations do not use all bits in TEID generation, and some bits have a fixed and predicted value. The study showed that TEID-C and TEID-U allocated by a node for a given session were not completely random to each other, and in a large percentage of cases, those values were exactly the same, allowing an attacker to infer the TEID-C from the TEID-U (or vice versa).

3.2.1.3 Subscriber Data Disclosure

A critical GTP message exchange is the message *SGSN Context Request* that invites an SGSN to respond for a given International Mobile Subscriber Identity (IMSI) or Temporary Mobile Subscriber Identity (TMSI) with details about a session of the corresponding subscriber, including IP addresses of GTP tunnel endpoints and the cryptographic keys for encryption/decryption (K_c) and integrity (K_i). See Figure 11. Being in possession of these keys, the attacker can decrypt a previously recorded packet data session of the subscriber.

With some additional effort, the attacker can also reroute the subscriber's packet data traffic through the attacker's equipment and eavesdrop on the content.

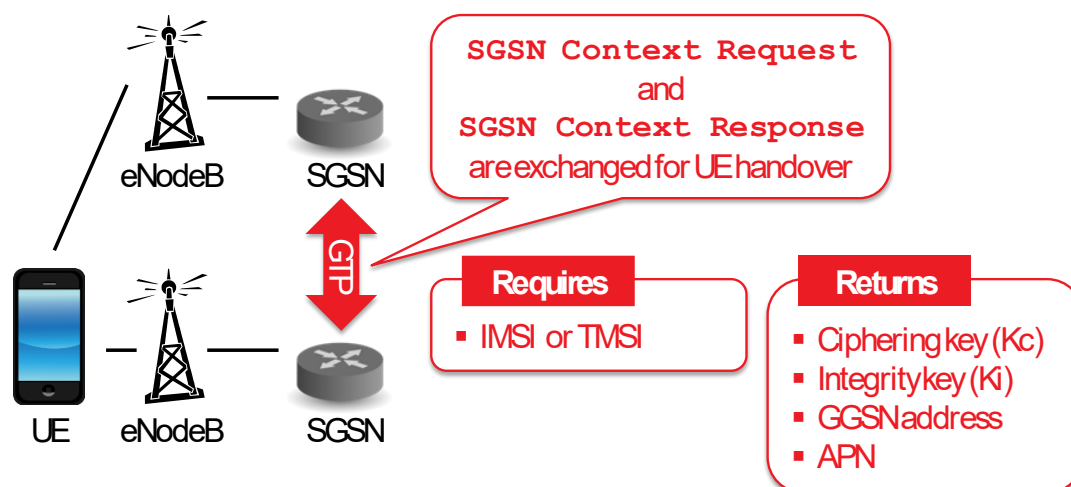


Figure 11 – Risk: Disclosure of details about the session of a subscriber

The potential for abuse of these messages highlights that it is bad practice to expose the GTP interface on Nes to networks and peers that do not need to communicate via this interface.

In LTE networks, a similar mechanism is implemented using the internal interface S10 between MMEs, so it is more secure, as this message is not defined for the S8 interface between HPLMN and VPLMN. The attacker would need to get access to the S10 interface to carry out this type of attack. If the network is not well configured, the S10 interface may be reachable from the GRX/IPX or external network.

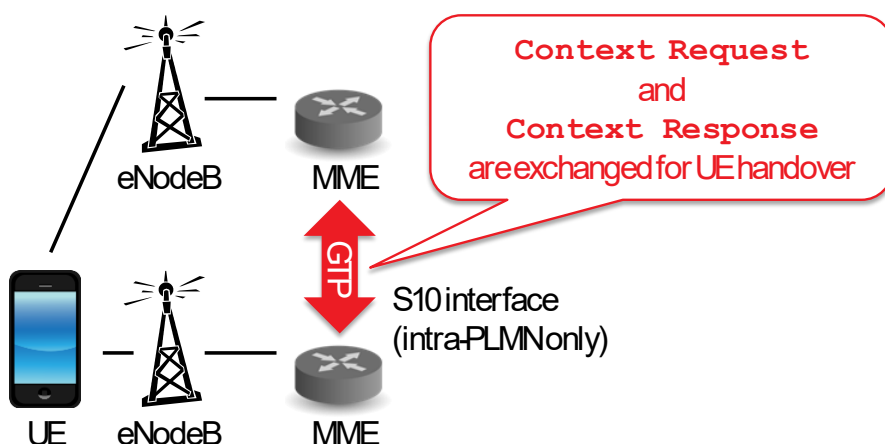


Figure 12 – Risk of disclosure of details of a subscriber's session in GTP-v2 via internal S10 interface (LTE network)

Another critical message on the internal S10 interface is *Identification Request*. An attacker can send this message with the Globally Unique Temporary Identifier (GUTI) of the subscriber and thus get the IMSI of the subscriber.

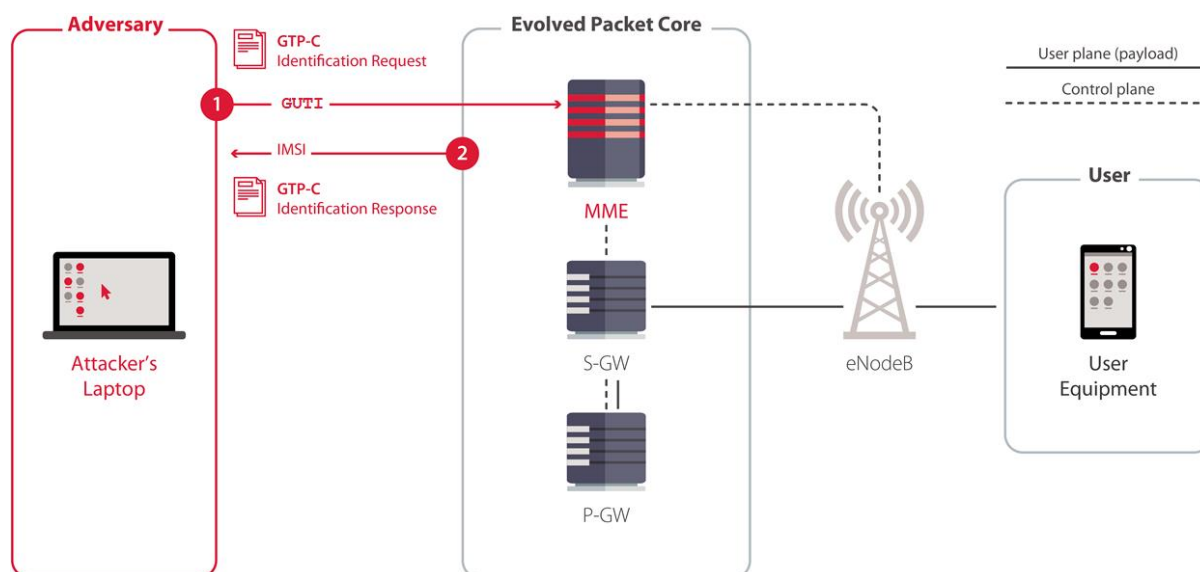


Figure 13 – Risk of IMSI disclosure in GTP-v2 via internal S10 interface (LTE network)

These examples are provided in order to emphasize the importance of proper network configuration and careful separation of all interfaces from each other.

Attackers on the internet and on a UE shall never need to communicate via GTP interface of a SGSN, GGSN, SGW, PGW or MME. On the GRX/IPX network, only the roaming partner operators should have access to the GTP interface. This limits the attack surface to potential attackers coming from roaming partner networks.

3.2.2 Subscriber Denial of Service (DoS) Attack

Attackers can perform a simple subscriber DoS attack using the GTP-C message *Delete Session Request*, *Delete Bearer Request* to PGW, or *Delete PDP Context Request* to GGSN via external S8 and Gp interface using TEID. It could be a massive subscriber DoS in case multiple messages are sent with different TEIDs.

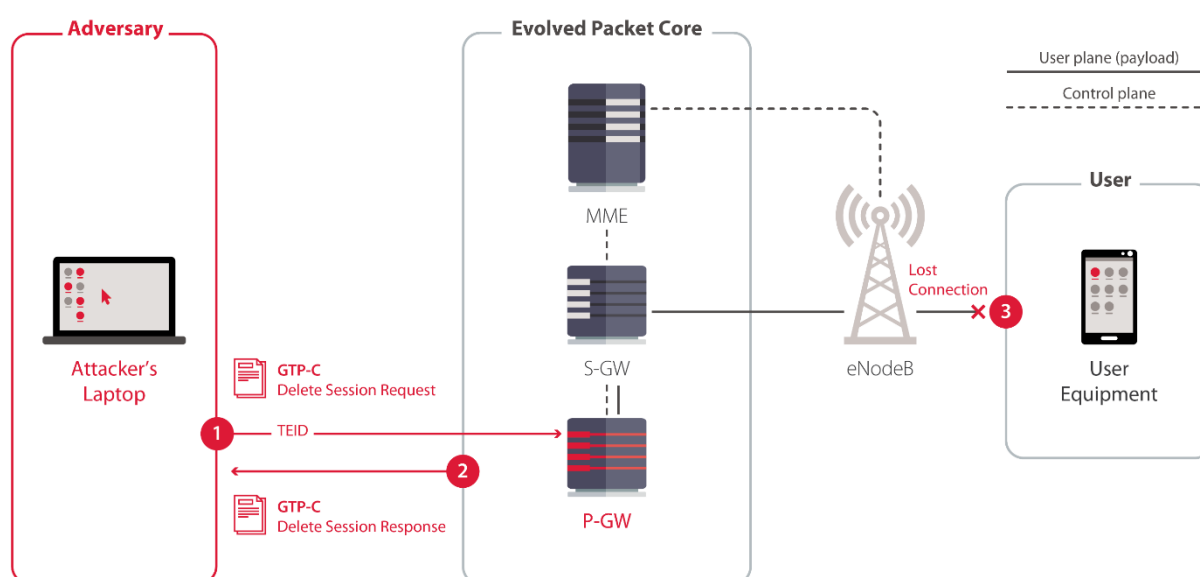


Figure 14 – Subscriber DoS

Another type of DoS for new subscribers can be performed by asking for an IP allocation for many nonexistent phones. IP address pools configured for each deployed APN on a PGW are limited, so by sending a flood of GTP-C *Create Session Requests* (with a specific APN) towards a vulnerable PGW, it is possible to allocate all the IP addresses reserved for the specified APN.

In this scenario, the attacker acts as SGW and subsequent new *Create Session Requests* are rejected with Cause 84 (*All dynamic addresses are occupied*). As a consequence, the PGW cannot create new sessions for new legitimate subscribers.

The IP addresses assigned to the attacker are released only after the flood is stopped and if the attacker does not respond to the GTP Echo requests sent by the target GGSN/PGW.

The time required to make this attack successful depends on the size of IP addresses pools configured on a target PGW and the number of active subscribers.

3.2.3 Fraud

Attackers can use services at the expense of the operator or another subscriber using invalid IMSI or any subscriber IMSI and the GTP-C message *Create Session Request* to PGW or *Create PDP Context Request* to GGSN via the external S8 and Gp interface.

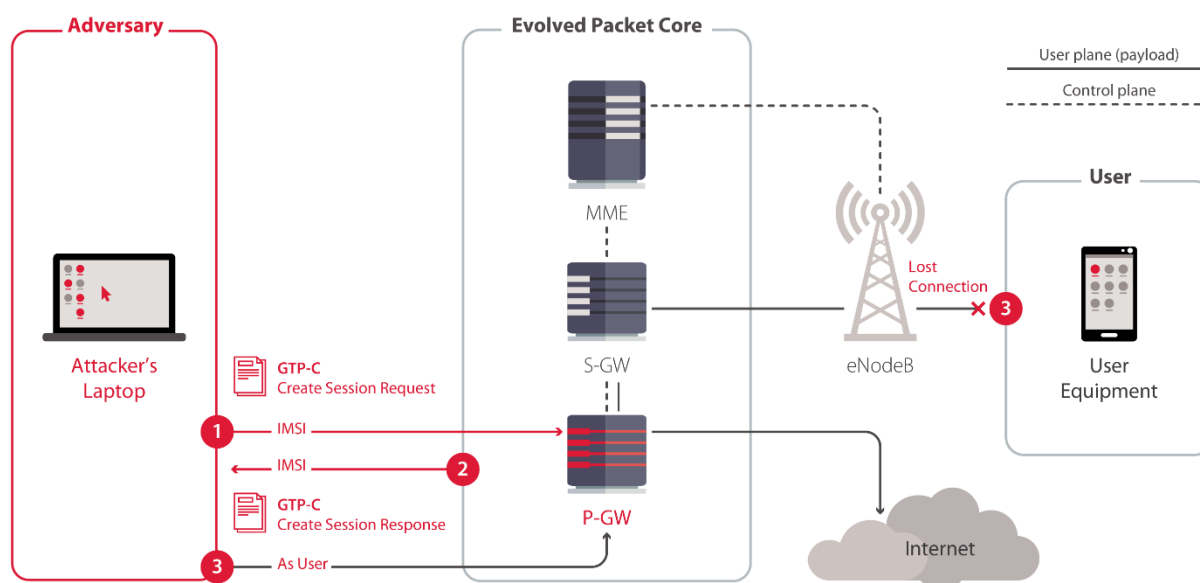


Figure 15 – Fraud using Create Session Request message

Another type of possible attack is tunnel hijacking using *Modify Bearer Request* to PGW or *Update PDP Context Request* to GGSN. An attacker can send that request with other tunnel parameters and specify a new S-GW address. So the attacker continues using the GTP-U tunnel as a subscriber. All external services will treat the attacker as a legitimate subscriber.

Another consequence of this attack is a DoS for the real subscriber, since the PGW will redirect all traffic towards the fraudulent SGW.

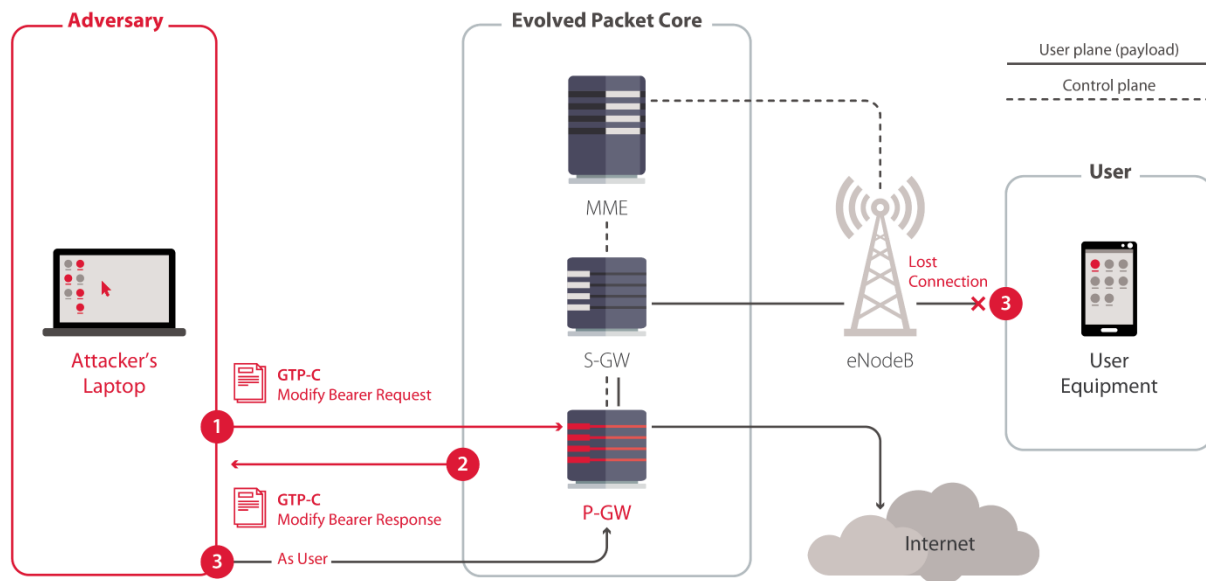


Figure 16 – Tunnel hijacking using Modify Bearer Request message

Another type of possible attack is full Main-in-the-Middle (MITM) [24] by combining the tunnel hijacking attack with a new attack vector that also redirects the SGW leg to the attacker. This is done by sending a Create Bearer Request towards the SGW with Traffic Flow Templates (TFTs) that will filter all uplink traffic to the dedicated bearer. The Create Bearer Request has the attacker's IP as User Plane PGW. After the establishment of the dedicated bearer, the attacker will receive all uplink traffic from the UE. See Figure 17

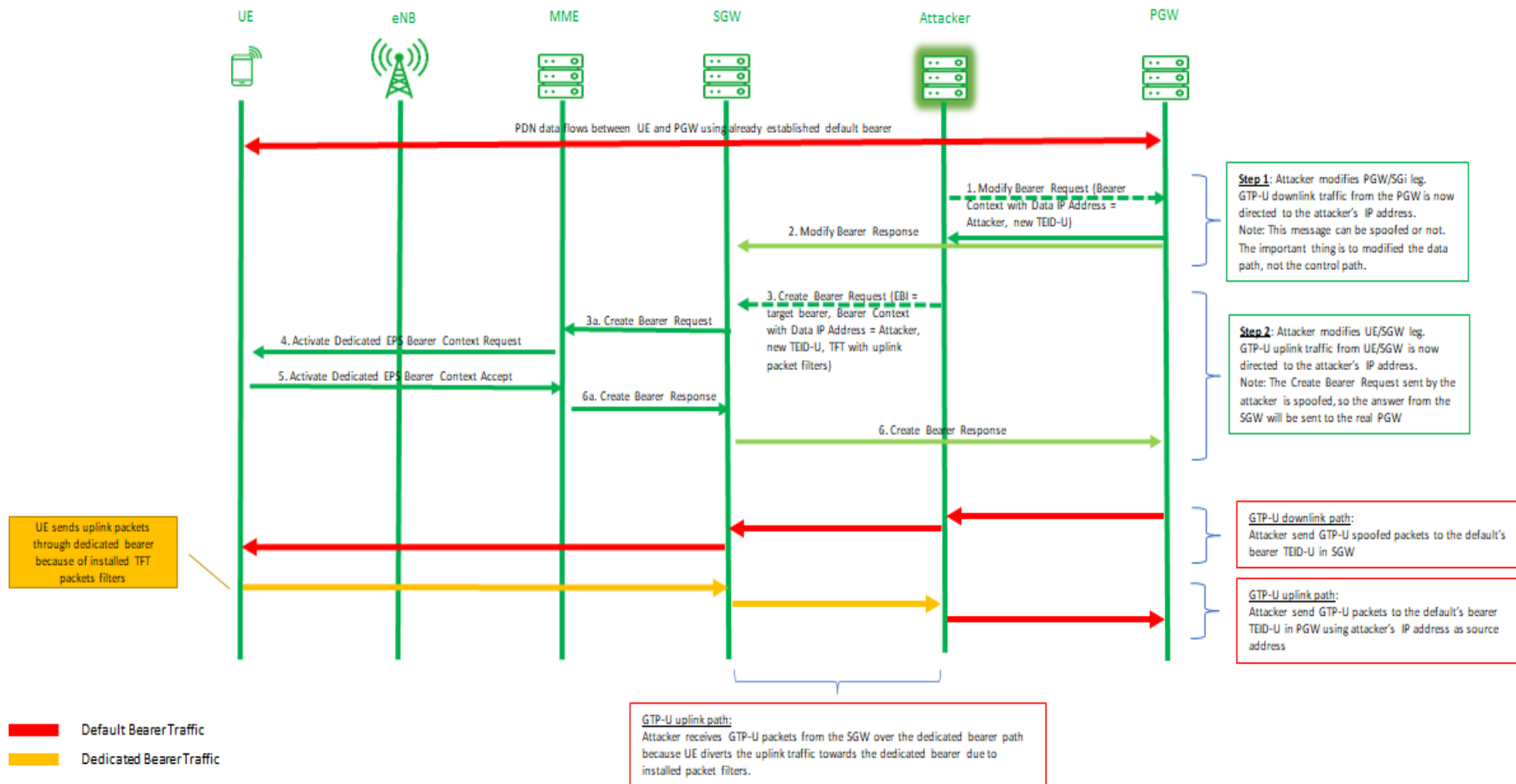


Figure 17– Session hijacking using Modify Bearer Request and Create Bearer messages

The attacker can implement only the hijacking of the SGW leg towards the UE using step 2 from Figure 17. In this scenario the attacker will have IP connectivity to the victim's UE, allowing him to process all UE traffic and to perform other types of active attacks.

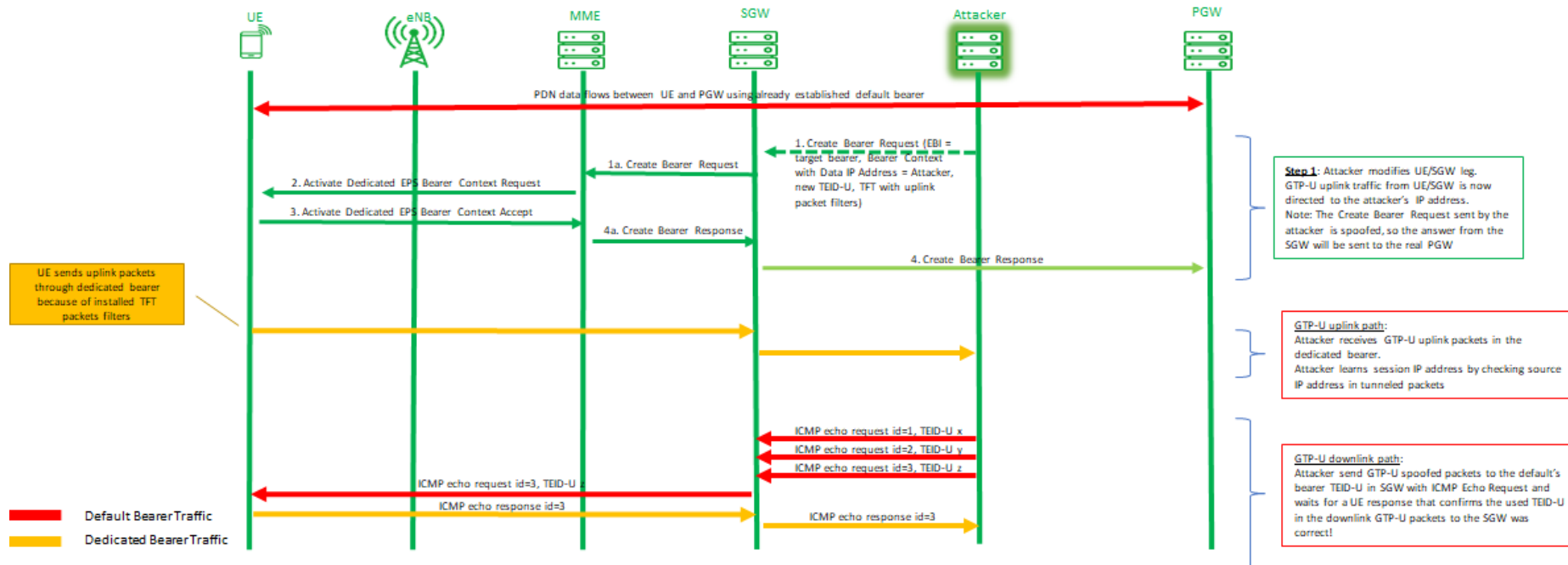


Figure 18– Tunnel hijacking (SGW leg) using Create Bearer Request message

3.2.4 Location Tracking

The attacker may use *Insert Subscription Data* (IDR) to change the APN PGW to his malicious PGW [23]. Then the attacker needs to activate the new setting, e.g. by sending a MMS, as in the example below. The next session set-up is then done via attacker's PGW and the attacker receives in the *Create Session Request* (CSR) the user's location.

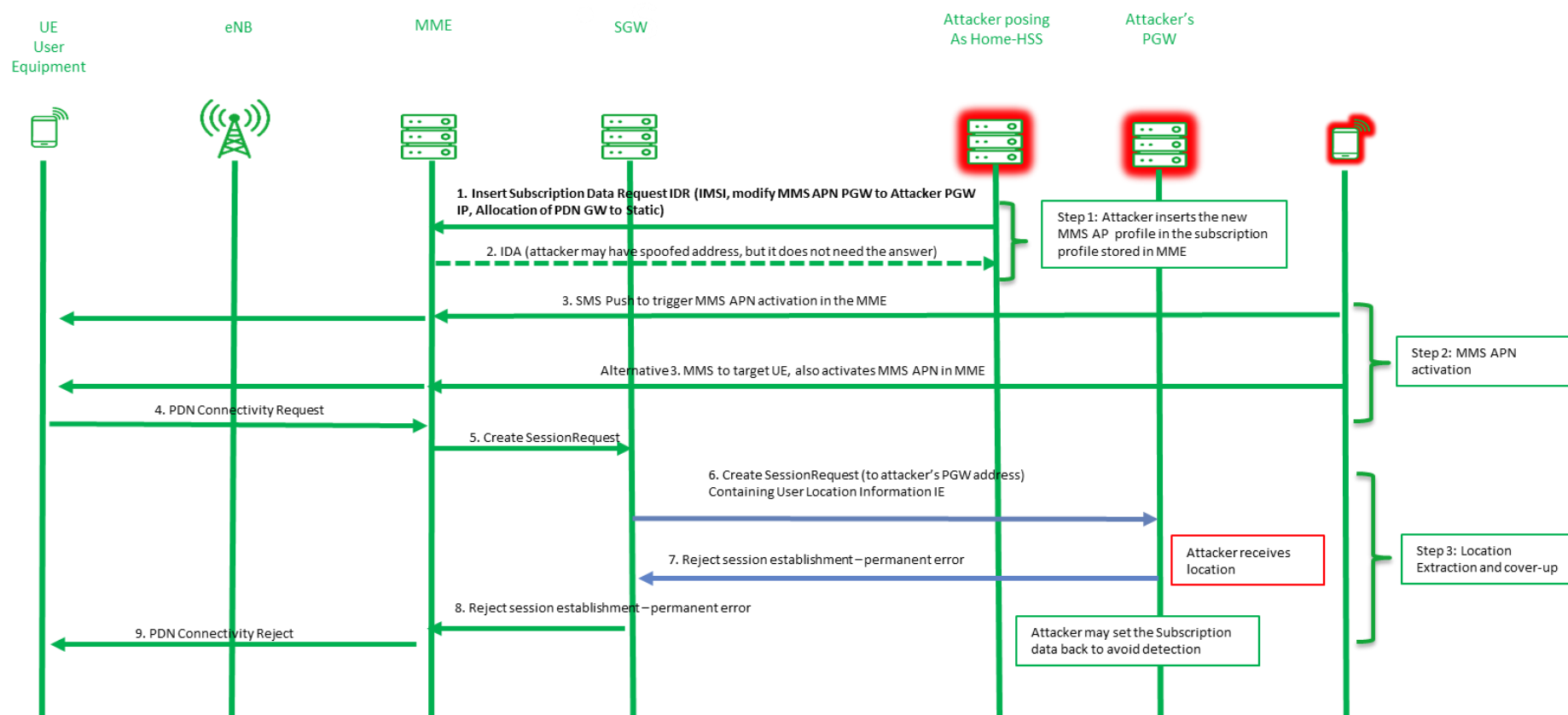


Figure 19: Location Tracking using Create Session Request

3.3 Missing Binding of Network Interfaces to 3GPP Interfaces

As described in section 3.1, the GTP interface must be accessible for roaming partners. In this context only the Gp/S8 interfaces are used outside the domain of a single MNO. All of the other interfaces (e.g. Gn, S5, S10, S11) are used internally only. Consequently, there is a need for MNOs to configure the network interfaces of their NEs that are connected to the GRX/IPX network to differentiate the 3GPP interfaces and only accept GTP messages that are assigned to the Gp/S8 interface. Most implementations of SGSNs, GGSNs, SGWs, PGWs and MMEs today do not distinguish 3GPP interfaces. Even on network interfaces to external networks, these NEs accept GTP messages that are only meant for MNO-internal use. This is why the attack outlined in section 3.2.1, where the *SGSN Context Request* message is sent across MNOs, works. This is a valid GTP message. SGSN implementations that accept this message without determining whether it originated from inside or outside the MNO's network are vulnerable to this attack.

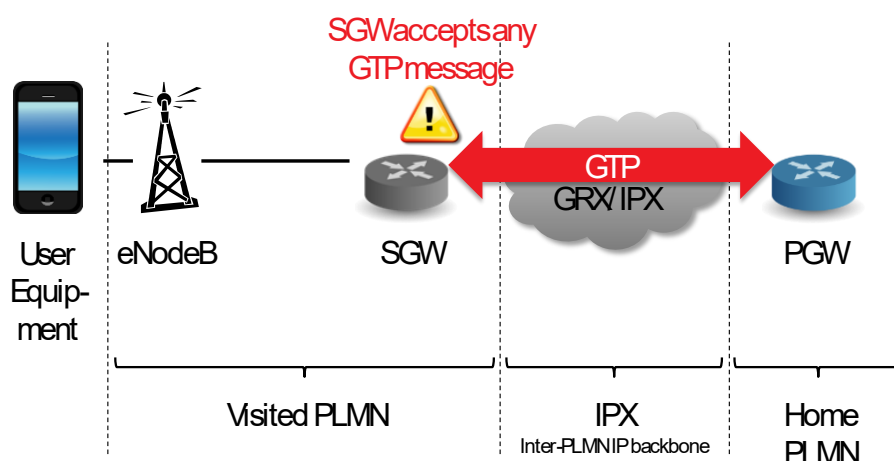


Figure 20 – Risk: The SGW accepts any GTP message

3.4 Malicious Peers and Faulty Behaviour Experienced as Attack

Sections 3.1 to 3.2 assume that the attacker has access to the internet, the GRX/IPX network, or the mobile radio access network via a UE. The attacker would create and send GTP messages to NEs that expose their GTP interfaces to these networks. This subsection considers a more advanced attacker who is part of the network of a peer MNO or an IPX provider, and who can inject fake messages with source IP addresses from valid peers or who can read and modify messages on transit.

This type of attack can and does occur, however the scenario differs significantly from sections 3.1 to 3.2 in that an attacker who is able to successfully control the GRX/IPX links and or has compromised a trusted roaming partner has practically unlimited opportunity to commit fraud and or denial of service. An attacker in control of the GRX/IPX links has clear text access to practically all information exchanged between operators and can throttle, block, intercept and manipulate any messages on the wire. This includes but is not limited to:

- Subscriber tracking at scale (all roaming traffic intercepted)
- Eavesdropping on all traffic exchanged between the target network and all of its roaming partners

- Ability to modify any traffic passing through the GRX/IPX

From a security perspective the GRX/IPX carrier is a critical point, but also essential from a business perspective. This problem stems from the way that telecommunications networks are organized and how they exchange information across the GRX/IPX. When quantifying the risk of this type of attack the MNO is encouraged to evaluate the level of trust placed in the GRX/IPX provider. An operator is likely to find itself somewhere between two extremes: Either the baseline assumption is that the GRX/IPX is always compromised, or that the GRX/IPX is never compromised. This baseline assumption must be taken into account when deciding which types of services the operator is willing to use over GRX/IPX and what types of countermeasures (if any) the operator is willing to take to limit the risk. It is however important to note that this type of risk is not limited to GTP but actually spans all protocols and services exchanged over GRX/IPX or other carrier networks.

Modified or injected GTP messages that are sent and legitimate GTP messages that are suppressed with malicious intent can cause harm to MNOs and subscribers. There are also cases in which GTP messages that relate to legitimate roaming traffic are considered as an attack by the peer MNO. This may occur when a large number of UEs try to establish a session at the same time, for example if a large number of mobile-to-mobile devices are triggered by a central service to re-establish their sessions. This can cause a high load and an exhaustion of resources on involved NEs, such as the SGSN/SGW and the GGSN/PGW, which may result in a situation where not all the requests can be processed for a period of time. This can potentially create a false perception at the recipient MNO of an incoming attack.

For the recipient MNO it is difficult to distinguish legitimate GTP messages from injected and manipulated GTP messages. The specifications of the GTP do not provide for authentication of the peer and for integrity validation of the content of GTP messages. Trust in peer MNOs is built upon the roaming agreement.

3.5 Vulnerabilities on Network Elements

A classic internet attack is to enumerate services running on a NE, to determine if they are vulnerable, to find or create associated exploit code, and to exploit the vulnerability to control parts or all of the functionality of the NE. Sometimes it is even simpler for attackers: they can just log in to the NE with the default administrator password that was not changed after deployment. Once under control, the NE can be abused as desired by the attacker. Abuse ranges from revealing session information about subscribers to changing the behaviour of the NE.

If the GTP network stack on the NE has implementation failures, this may cause the NE to enter an undefined state. Depending on the failure, the attacker may be able to access functionality of the NE that should not be accessible from outside. In other cases, the NE may freeze, and its services will become unavailable.

These attacks are common, widespread and often easy. Attackers who operate on the internet have all the equipment and expertise they need. They can easily enumerate NEs that are capable of communication via GTP. Attackers can send GTP request messages to all known IP address ranges of an MNO and see if a GTP response message is received. Alternatively, an attacker can look-up known GTP-aware NEs on search engines, such as

shodan.io¹. However, some IP/MPLS routers answer GTP Echo Request messages so this should not be confused with packet core GTP exposures.

4 Countermeasures

This section describes countermeasures that a MNO should deploy to ensure that the mobile network is not exposed to the attacks that are described in the previous section.

NOTE: Even though only LTE terminology is used, this document is applicable to all 3GPP releases of mobile network standards. See also section 2.2.

MNOs need to protect the network, the NEs, the services, and the applications on all the layers of the network stack. The data link layer, network layer (IP), transport layer (Transport Control Protocol (TCP), UDP, Stream Control Transmission Protocol (SCTP)), and the application layer (GTP) all need to be secured. Some security measures are applied independently on each layer, whereas others are cross-layer measures that deal with multiple layers. Only such a comprehensive approach to security will result in effectively countering the attacks described.

Table 1 lists security measures that can be applied at different layers of the network stack.

Layer	On Network Elements (NEs)	On links
Physical layer	Separation by separate network interface	Separation by separate network cable
Data link layer: Media Access Control (MAC)	Separation by separate logical network interface, Virtual Local Area Network (VLAN), or Multiprotocol Layer Switching (MPLS)	Separation by VLAN, MPLS
Network layer: IP	- Separation by disjoint non-routed IP address segments - Separation by Virtual Routing and Forwarding (VRF) - IP packet filter - Strict firewall rules with IP whitelisting of only allowed roaming partners (e.g. by using IR.21 [13]) - IP anti-spoofing - Rate limits	Separation by VPN
Transport layer: UDP, TCP, SCTP	- Filtering of services/ports - Binding of services to network interfaces or IP addresses - Rate limits	
Application layer: GTP	Filtering of GTP versions (v0, v1, v2, GTP'), types (GTP-C, GTP-U), messages, and IEs	

¹ Try <https://www.shodan.io/search?query=GGSN> to list all hosts that were identified as GGSN by the Shodan internet crawler.

Layer	On Network Elements (NEs)	On links
	• Filtering/whitelisting of 3GPP interfaces: Gp/S8 • Possible GTP-C Category 2 / Category 3 checks for allowed messages (e.g. comparing the location of the subscriber) • Plausibility checks of GTP messages • Detection of protocol anomalies and suspicious activities (e.g. GTP-in-GTP encapsulation) • Rate limits • GTP firewalling with strict GTP messages content validation (e.g. every GTP information element)	
Cross layers	• Plausibility checks of information that appears on multiple layers (e.g. IP addresses) • Traffic monitoring • Security Signalling Monitoring (Intrusion Detection System / IDS)	
System layer	• Secure configuration • Hardening • Up-to-date patch level	

Table 1 – Security measures by network stack layer

Protection should begin with a secure network design and by deploying security controls on all the layers of the network stack. Network Elements should be configured and operated securely. But measures specific to GTP should always be applied as well, because attacks could come from valid GRX/IPX interconnection points over the application layer, so lower layer controls would not be effective. Effective protection is only achieved if all these security controls are deployed. This section covers all of these aspects.

4.1 Secure Network Architecture

The mobile core network is connected to the GRX/IPX network for international roaming and to the internet for terminating customer traffic there. Both of these connections need to be configured to only allow the traffic that is needed and to only allow receipt of messaging from the partners that actually need to communicate with the mobile network.

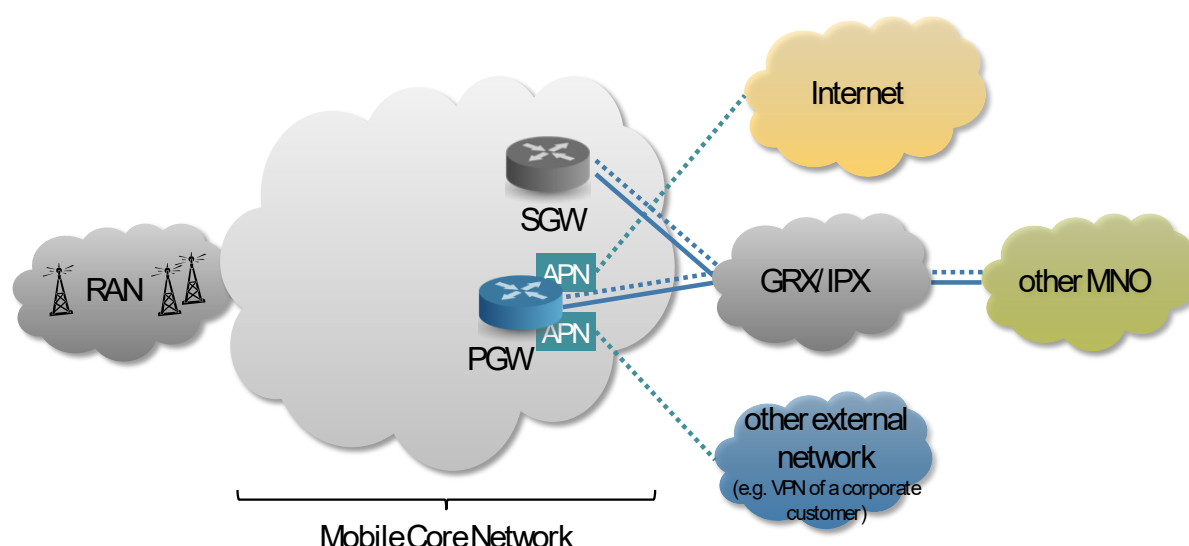


Figure 21 – Typical Connections between the mobile core network and other networks

As the simplified Figure 21 illustrates, the key component in the mobile core network is the GGSN/PGW, which is connected to many different networks. The figure only depicts connections to outside networks, as this document is about protection of the mobile network against outside networks. Thus internal connections are omitted.

This section provides a high level overview on key aspects of the complex subject of network security. The reader is invited to study the references listed in section 4.1.3 for more details.

4.1.1 Basic Network Security

A key security measure is to separate networks and to establish dedicated connection points between them that only permit exchange of traffic that is needed for normal operation. Separation can be done in several ways. The most suitable way depends on the existing network infrastructure. It is important to implement separation on both links and NEs. Only then there will be true separation. The following recommendations should be considered:

- Keep networks separated physically through the use of separate connections, or logically separate on layer 2 (e.g. through the use of a VPN or VLAN).
- Keep networks separated in shared equipment, such as routers or switches, by having independent virtual routing and forwarding instances or VLANs.
- Assign disjoint IP address segments for each of the networks.

This is a fundamental and important general security concept that provides GTP security benefits. Once networks are separated, only legitimate peers can reach GTP-aware NEs. Once the networks are separated, the GTP interface cannot be reached from UE and the internet. See Figure 22.

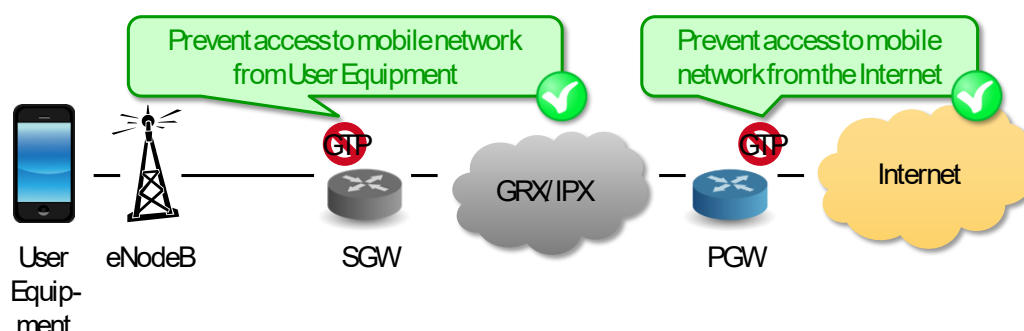


Figure 22 – Network separation prevents direct access to GTP interfaces

There should also be no routes from the internet or from UE IP addresses to infrastructure IP addresses of the NEs.

The GGSN/PGW needs internet access to forward subscribers' packet data to/from the internet. This packet data contains source and destination IP addresses that represent a UE address and an internet address only. Infrastructure IP addresses of NEs should never be specified as source or destination addresses for this packet data. Forwarding internet traffic for UE is done by the Gi/SGi interface that is configured in the GGSN/PGW. The Gi/SGi interface on the GGSN/PGW needs to be reachable from the internet to allow hosts on the internet to direct traffic to a UE IP address.

Network separation is an important tool to clearly define network edges and to prevent communications between networks that do not need to reach each other. Those networks that do need to reach each other require further security measures that are described below.

4.1.2 Network (IP) Layer and Transport Layer Security

The types of traffic that are allowed or prohibited from crossing the border to another network should be defined at the edge of each of the separated networks.

- On the network layer, filter traffic at the edge of each network based on source and destination IP addresses.
- On the transport layer, only specifically allow the application layer protocols that are actually needed on the respective network or for particular communication partners. Filter and block all other protocols.

When filtering GTP traffic, consider the following:

- Only the APNs that are connected to the internet on a GGSN/PGW need direct access to the internet. This implies that the UE that is handled by a GGSN/PGW needs direct internet access. The GGSN/PGW and all its local interfaces should not be reachable from the internet. This includes blocking all GTP traffic from the internet towards the GGSN/PGW. The same is true for UE. None of the interfaces of the GGSN/PGW should be reachable by UE.
- The GGSN/PGW, SGSN/SGW and MME are connected to the GRX/IPX network for international roaming. Through this network a MNO reaches all the other MNOs worldwide. Filters should be implemented to only accept incoming traffic from known peer MNOs to which a roaming agreement exists. They publish the IP subnets they use on the IPX in the IR.21 [13]/IR.85 [16] Roaming Exchange (RAEX) database. In

the filters, only allow communication with IP addresses of peer operators explicitly and restrict access to the application layer protocols (GTP-C, GTP-U) that are actually needed.²

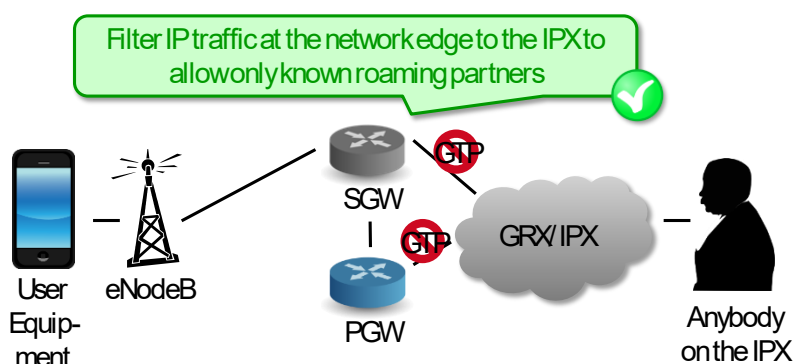


Figure 23 – IP traffic filtering at the network edge

Install a packet filter firewall on the network edge exposed to the internet (Gi/SGi Firewall) and on the network edge exposed to the GRX/IPX (Gp/S8 Firewall) in order to filter as described above. See Figure 23.

Network services are not needed on all network interfaces of a NE. If there is a separate (logical or physical) network interface for management, for example, make sure that the management-related network services, such as SSH, are only bound to this network interface. On all other network interfaces, the service should not be accessible. If there is in-band management without a separate network interface, apply filtering so that only management networks or workstations have access to the management-related network services.

4.1.3 Further Reading on Fundamental Network Security

For general GRX/IPX network security the reader is referred to PRD IR.77 [15]. This document is focussed on GRX/IPX network security, but many of the measures described there are general recommendations, and most of them can and should also be applied to other networks of MNOs.

For comprehensive references on basic network security, the reader is referred to external literature, for example:

- Security Configuration Guidance for various operating systems, network services, applications, and routers by the National Security Agency [18];
- Network Security A Beginner's Guide by Eric Maiwald [8],
- Wikipedia Handbook of Computer Security and Digital Forensics 2016 by Reiner Creutzburg et al. [7].

² Further application layer protocols (e.g. Diameter and Radius) may be needed on this interface, but this is out of scope of this document.

4.2 Network Element Security

It is essential for GTP security that the NEs are secure. Best practices from the internet industry should be applied to NEs on the mobile network. These include:

- Secure configuration of the NEs and all network services;
- Disabling of insecure and unneeded network services;
- Changing of default passwords;
- Hardening;
- Configuration and enabling of authentication and access control; Logging of all access attempts and other security-relevant events;
- Configuration of the NE to not disclose unnecessary information; and
- Continuous deployment of the latest security patches.
- Security testing and regular vulnerability scanning;

This is not an exhaustive list of recommendations. Further details can be found e.g. in PRD IR.77 [15], 3GPP TS 33.117 [6] and the references provided in section 4.1.3.

Attackers may not only have access to the internet, but also to other networks that the mobile network is connected to (e.g. the GRX/IPX network). Therefore, it is essential to secure all the NEs on the mobile network.

An important requirement is that the NE should randomly allocate the GTP TEID and any similar identifiers with sufficient entropy. This should make it more difficult for an attacker to perform session attacks, TEID guessing attacks or response attacks (e.g. crafting the response message and delivering it earlier than the real response message).

It is also good security practice to verify the robustness of the GTP protocol stack implementation to reduce the risk that NE behaviour could be compromised by illegitimate GTP traffic.

4.3 GTP Security

Once a communication partner can reach the GTP network service on a GGSN/PGW or SGSN/SGW, it is important to define the purpose of the communication. While intra-MNO communication with GTP uses the 3GPP Gn/S5 interface, communication with roaming partners is based on the 3GPP Gp/S8 interface. The MNO should ensure that only Gp/S8 traffic is granted access at the network edge exposed to the IPX network. In addition, the SGSN/SGW and GGSN/PGW should check the plausibility of values sent in GTP messages. This section covers both of these aspects.

4.3.1 GTP Message Filtering Categories

The GTP-C messages can be grouped into categories by the message type. The type and nature of the GTP-C message implies the corresponding detection and possible filtering of the message. For a high level description of the message categories, see FS.21 [22].

4.3.1.1 GTP Low-Layer Format Filtering (*Note: Not a category*)

GTP messages could be filtered on the lower layers of the protocol stack (IP layer, transport layer). Illegal messages should never be allowed within an operator's core network from an external perspective (an example could be filtering of the messages containing a spoofed

internal IP address, not allowed roaming partner's source IP address and UDP ports). The messages can be filtered on lower layers with standard firewalling of IPs, protocols and ports. See section 4.1.2 for details.

4.3.1.2 Category 1 – Interface-Unauthorised Packet (GTP Category 1)

GTP messages could be filtered on the GTP layer in the protocol stack by decoding the message type. Illegal messages that are not related to the Gp/S8 interface should never enter the operator's core network from an external source (e.g. from the GRX/IPX provider network).

4.3.1.3 Category 2 – Home-Network Packet (GTP Category 2)

GTP messages could be filtered on the GTP layer in the protocol stack. These messages must be allowed for inbound roaming subscribers from the international interconnect (from the GRX/IPX provider network). Therefore, they cannot be filtered like GTP Category 1 messages. Examples of such illegal messages could be messages coming from the interconnect that target home subscribers that are in the home network.

4.3.1.4 Category 3 – Plausible-Network Packet (GTP Category 3)

GTP messages can be filtered on the GTP layer in protocol stack by comparing the subscriber's location. These messages must be allowed from the international interconnect perspective (from GRX/IPX provider network) because of outbound roaming subscribers. Therefore, they cannot be filtered like GTP Category 1 messages. An example of illegal messages could be messages coming from the interconnect that are pretending to be sent on behalf of a subscriber during a period of time when the subscriber is located within the home network.

4.3.2 GTP Category 1 – Interface-Unauthorised Packet

At the network edge exposed to other networks it is important to only accept those GTP messages that actually need to be exchanged with the peers on the other networks. In the case of international roaming, a GTP Gp/S8 firewall should be introduced between the mobile core network, where, for example, the SGSN/SGW and GGSN/PGW are located, and the GRX/IPX network. This GTP firewall should filter GTP messages in a way that only GTP messages that belong to the Gp/S8 interface are allowed. All other GTP messages should be discarded and logged. This ensures that no unwanted GTP message types enter or leave the mobile network. See Figure 24. A list of GTP messages that belong to the Gp/S8 interface can be found in Annex A and a GTP risk classification matrix including a GTP category mapping is provided in Annex B.

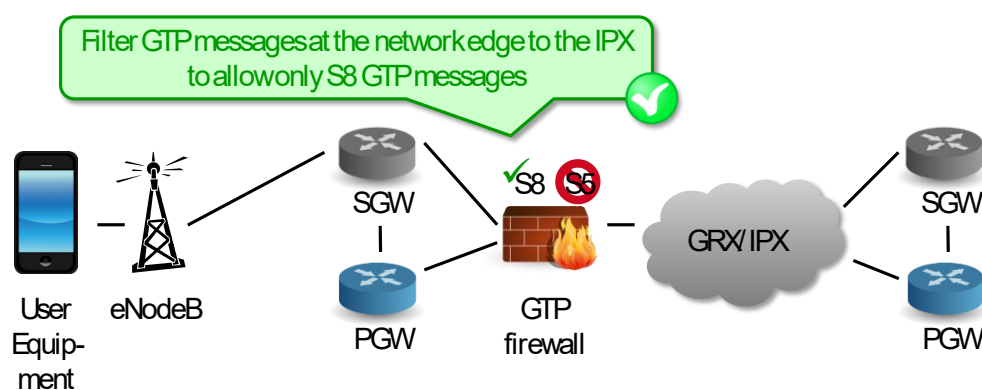


Figure 24 – Filtering of GTP messages at the network edge

With this countermeasure in place, the *SGSN Context Request* and *SGSN Context Response* messages can no longer be exchanged across PLMNs. The attack described in section 3.2 providing unauthorised access to subscriber data is no longer possible. This protection can be understood as GTP Category 1 filtering.

This countermeasure requires the GTP Gp/S8 firewall to be able to define acceptable GTP message types on a per GTP version and per 3GPP interface basis. In addition to filtering GTP versions and 3GPP interfaces (i.e. GTP Category 1 filtering), the GTP Gp/S8 firewall should validate the GTP message by GTP Category 2 filtering (e.g. APN and the selection mode, and check if the IMSI prefix (Mobile Country Code (MCC) and Mobile Network Code (MNC)) for an incoming message matches the roaming partner or belongs to an assigned trusted GGSN/SGSN or PGW/SGW group) and by GTP Category 3 filtering.

It is good security practice to log policy violation events, in order to support subsequent fraud investigations and/or prosecutions.

The GTP Gp/S8 firewall should also be able to detect message floods or denial of service attacks and have the ability to rate limit GTP-C messages with different levels of precision e.g. per GGSN/PGW, SGSN/SGW, GGSN/SGSN or PGW/SGW groups, roaming partners or globally.

GTP message length should be restricted by the GTP firewall to a configurable maximum. This makes code injection attacks more difficult or impossible.

4.3.3 GTP Category 2 – Home-Network Packet

There are few GTP-C messages that are originated from the GGSN/PGW in HPLMN towards the SGSN/SGW in VPLMN. These messages should be allowed from GRX/IPX network into the VPLMN because of the need to provide service to inbound roamers.

However, the following checks should be implemented:

- If the request message contains an IMSI/MSISDN, it should not target a home subscriber. Additionally and optionally it should belong to the proper source network, which could be correlated from source IP address and GRX/IPX DNS).
- If the request does not contain an IMSI/MSISDN, it should still not target the home subscribers GTP-U sessions. Possible protection could be implemented directly in

the SGSN/SGW because these elements can resolve corresponding IMSI/MSISDN from the existing GTP-U sessions. This is because the SGSN/SGW associates the IMSI/MSISDN to a GTP-U session in the initial GTP-C signalling and maintains it until after the session is released. This behaviour is used also when the CDRs are generated.).

4.3.4 GTP Category 3 – Plausible-Network Packet

Most of the GTP-C messages on the Gp/S8 interface are from the SGSN/SGW in the VPLMN towards the GGSN/PGW in the HPLMN. These messages should be allowed from the IPX network into the HPLMN because of the need to provide service to outbound roamers.

However, the following checks should be implemented:

- If the subscriber (identified by IMSI/MSISDN in GTP message) is currently located in the HPLMN network and the corresponding GTP Category 3 message is received from GRX/IPX network, the message should be considered as illegal.
 - The subscriber location can be determined by monitoring of SS7/Diameter traffic and performing correlation and analysis across them or by checking the current location in HLR/HSS.
- If the subscriber (identified by IMSI/MSISDN in GTP message) current location is different compared to the location seen in the GTP Category 3 message, the message should be considered as illegal.
 - The subscriber PLMN location can be determined by monitoring of SS7/Diameter traffic or by checking the current location in HLR/HSS.
 - The translation of GTP source IP into location from SS7/Diameter (e.g. MCC, MNC) is not trivial and GRX/IPX DNS should be used for the translation.
- If a GTP Category 3 message is received without previously having received a GTP-C v1 Create PDP Context message or GTP-C v2 Create Session Request.

NOTE: Before the actual deployment it is strongly recommended to validate the robustness of the checks by first monitoring/logging the signalling traffic according to the defined rules, and only then apply robust checks that do not introduce false positives.

4.3.5 Plausibility of GTP Messages and GTP message validation

Whenever possible, MNOs should perform plausibility checks, i.e. seek to determine if incoming GTP messages make sense and if they are valid and not malformed. If they don't make sense, the messages shall not be processed any further. These plausibility checks are also a task for the GTP Gp/S8 firewall.

Useful GTP-C message validity checks are:

- Presence of mandatory IEs;
- Correct sequence of IEs;

- Correct message length; and
- Correct Type-Length-Value (TLV) format of IEs.

Useful GTP-C message plausibility checks are:

- Validity of IP addresses in GTP messages;
- Cross-layer checks for validity of information that appears in multiple layers (e.g. IP addresses in IP header and GTP message IEs);
- Validity of information in IEs representing the roaming partner (i.e. IP addresses and IMSIs);
- Validity of information in IEs representing a roaming subscriber (i.e. IMSI and MSISDN);
- Verification of the occurrence of the IEs

Additional GTP-C checks that can be considered for monitoring, off-line analytics and future filtering rules of GTP firewalls are listed below.

Test	Comments
APN check	Apply policies based on the APNs
IMSI Prefix Filtering	Apply policies based on the IMSI/MSISDN
Packet Sanity Check	Validate the missing mandatory IEs, length mismatch.
PDP Context/ IP Address check	Validate the PDP context and IP address
Message-Length Filtering	Validate the maximum/minimum message length
Message-Type Filtering	Filtering to be applied on the message type.
Message-Rate Limiting	Implement GTP message rate limiting
Stateful GTP Inspection	Validate the sessions are logged and monitored in a stateful manner
IP Fragmentation (reassembling)	Validate the fragmented GTP packet
Sequence-Number Validation	Validate packet with incorrect sequence number
Nested GTP Packet Filtering	Validating nested GTP
RAT Type Filtering	Radio access type filtering
End User IP Spoofing	Perform the check to validate if the end user IP is not spoofed.
Allowing network element on IP address	Allowing policies with agreed roaming partners
GTP-U pin hole	GTP-U user plane traffic is only allowed if TEID was received before, so a pinhole was created
GTP Scan prevention	Scanning GTP-C Echo request messages
GGSN and SGSN redirection	Validate the redirect request.
Location Data Leakage	Prevention of location data leakage

Table 2 – Additional GTP-C Policies

Possible GTP-U message plausibility checks:

- GTP-in-GTP encapsulation detection

NOTE: As the focus of this document is about signalling security (see section 1.2), other GTP-U checks and analytics are currently out of scope of this document because:

- GTP-U is very different from GTP-C in terms of traffic volumes, investments, etc.
- The requirements for GTP-C firewall filtering capabilities are very distinct from the requirements for GTP-U firewall filtering capabilities.
- GTP-U checks would require Deep Packet Inspection (DPI) type of solutions and content analysis that may be subject to national regulations and privacy considerations.

This is also reflected in section C.6, which describes the options for implementing a GTP firewall in the network. This includes the dedicated GTP firewall option in C.6.1.3 in which the GTP-C traffic is separated from the GTP-U traffic to be processed in a dedicated GTP-C signalling firewall entity.

These GTP-C and GTP-U message plausibility checks are explained further below.

4.3.5.1 Validity of IP Addresses in GTP Messages

MNOs are recommended to check all of the IP addresses inside GTP messages that point to NEs. The IEs of a GTP message often contain IP addresses of SGSN/SGW, GGSN/PGW, UE, and sometimes other destinations. These IP addresses are attractive targets for attackers. If attackers can modify them, they are able to redirect traffic to their equipment. The GTP firewall should maintain a so-called *handover group* per peer PLMN. That is a list of IP address segments per peer PLMN that belong to their NEs. The GTP firewall can determine if IP addresses in GTP messages match a particular handover group. If they do, the messages are considered plausible. If they don't, they should not be processed any further and an error message should be returned. See Figure 25.

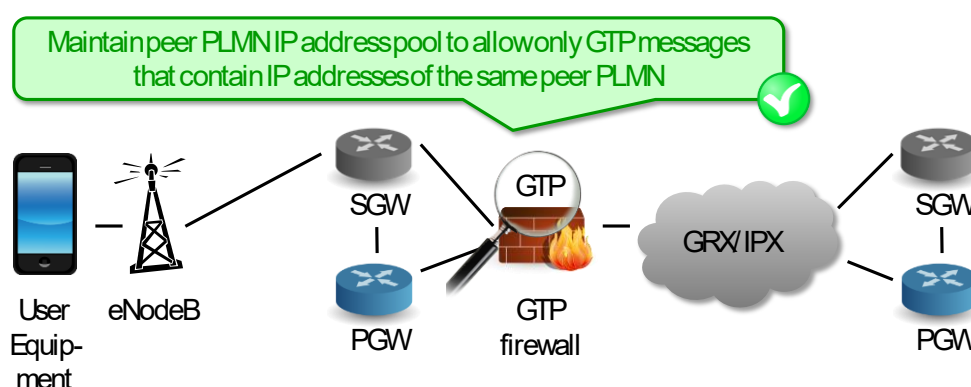


Figure 25 – Plausibility checks of GTP messages

Having this countermeasure in place prevents an attacker from hijacking the packet data session of a subscriber. As soon as the attacker puts his own IP addresses in the GTP message (which is outside the handover group assigned to a peer PLMN), the GTP Gp/S8 firewall will not forward this message to the SGSN/SGW or GGSN/PGW.

4.3.5.2 Cross-Layer Checks

Some NEs interpret only some of the information in GTP messages. When a message enters the network at the edge, messages should be checked for plausibility of information on all layers. If, for example, IP addresses on layer 3 (IP header) differ from IP addresses in respective IEs in the GTP message (layer 5), this is a hint that the message has been forged or manipulated. The GTP firewall should detect and discard these messages.

4.3.5.3 Validity of Information in IEs Representing the Roaming Partner

Several IEs represent the roaming partner. These are the IP addresses, the MCC, the MNC, and the IMSI prefix. The GTP firewall should check if all this information points to the same roaming partner. If this information is inconsistent, this is a hint that the messages have been forged or manipulated. The GTP firewall should detect and discard these messages.

4.3.5.4 Validity of Information in IEs Representing a Roaming Subscriber

Two IEs represent the roaming subscriber. These are the IMSI and the MSISDN. A relevant NE should check if all this information points to the same roaming subscriber. If this information is inconsistent, this is a hint that the messages have been forged or manipulated. The NE should detect and discard these messages.

The PCRF behind the GGSN/PGW could be used to strictly validate the GTP Category 3 messages according to the user profile which should be aligned with the HLR/HSS profile. For example, it could validate the IMSI, MSISDN and selected APN received in GTP-C signalling towards the HLR/HSS profile. If discrepancies are detected, the GTP-C signalling could be reported and rejected.

4.3.5.5 Verification of occurrence of the IEs

Multiple IEs of the same type could be crafted into a GTP packet which could violate the 3GPP specification and the number of allowed occurrences of IEs for the given message type. The messages could be validated against the standard dictionary and the illegal messages could be detected and discarded.

4.3.5.6 GTP-in-GTP Encapsulation Detection

The 3GPP specifications do not consider GTP-in-GTP encapsulation. The GTP Gp/S8 firewall should detect and discard all such encapsulated messages, as some GTP implementations cannot interpret them correctly. These faulty NEs interpret the encapsulated GTP message rather than the outer GTP message. This would allow an attacker to craft a payload that is transported through the mobile network in a way that NEs of the mobile network interpret user payload. This is critical for mobile network integrity and shall be avoided.

GTP-in-GTP encapsulation could be used to spoof other GGSN/PGWs or SGSN/SGWs or to create recursive processing of GTP messages, causing strange and unspecified behaviour that may lead to bypassing of checks or to resource shortages. Multiple embedded GTP headers can be used to exacerbate an attack. NEs should detect and discard messages if there are additional GTP headers within the outer header.

4.3.6 Protection against Manipulated and Fake GTP Messages

As described in section 3.4, a malicious peer can manipulate legitimate GTP messages or inject fake GTP messages to perform an attack. The recipient cannot distinguish these messages from legitimate GTP messages. The countermeasures described in section 3 reduce the attack surface significantly, as only peer MNOs and GRX/IPX providers would be able to perform these attacks if all of the countermeasures described here are applied. However, since GTP is not designed for validating the integrity of messages or for validating the authenticity of the sender, all of the peers from which a MNO accepts GTP messages can also send malicious GTP messages. This is a general interconnect security problem that exists within the mobile industry, as most of the interconnect protocols used were not designed with security in mind.

Operators are recommended to engage with 3GPP in order to get improvements defined and implemented. GRX/IPX providers and MNOs are recommended to try and detect integrity compromise of GTP-U traffic by statistical or analytical approaches.

4.3.7 Protection Against Location Data Leakage

If the attacker is able to change the APN settings, so that the SGSN or SGW sends the *Create Session Request* to the GGSN or PGW, then the attacker also receives in the *Create Session Request* the user location [23]. There are several countermeasures and policies that can be applied.

1. As a first step to prevent this attack, FS.19 [12], section 4.11.4 should be considered.
2. As a second layer of defense, the following should be done:
 - Remove location information from the *Create Session Request* message or replace it with suitable dummy location in the SGSN/SGW or GTP FW (i.e. with non existing Cell ID information). If the user location information is relevant for the destination PLMN (e.g. it's used in roaming value-added services, or is part of specific roaming agreements), then this measure should be skipped for those PLMNs.
 - By means of comprehensive plausibility checking via cross-correlation between *SGSN/MME* diameter ISR message, *SMS delivery* message and *Create Session Request* message for the same IMSI e.g. based on time-window. If such events occur, the *Create Session Request* should be dropped if:
 - The APN in the *Create Session Request* is the same APN that was changed via ISR, and
 - The destination IP address of the *Create Session Request* does not belong to the IMSI's PLMN network range.

4.4 Effectiveness and Coverage of Countermeasures

The countermeasures described in section 3 could be effective in countering all of the attacks described in sections 3.1 through 3.2. Only a small number of the attacks described in section 3.4 can be countered, as explained in section 4.3.6. Countering the attacks described in section 3.5 can be done through the application of common internet security measures. As summarised in section 4.2, there is a broad range of effective countermeasures that should be deployed.

5 Summary of attacks

Table 3 summarises the attacks described in the previous sections under the following headings:

- **Attack:** The type of attack in terms of impact;
- **Method:** How the attack can be realized (e.g. the message type that can be used);
- **Attack Type:** Whether the attack is passive or active;
- **Attack pre-conditions:** The pre-conditions that need to be satisfied for an attack to succeed.
- **Mitigation:** The recommended countermeasure(s).

Attack	Method	Attack Type	Attack Pre-conditions	Mitigation
Intercept user traffic	Read GTP-U plane and user payload	Passively read legitimate GTP messages in transit	Ability to capture the GTP traffic (e.g. successfully control the GRX/IPX links and/or a trusted roaming partner compromise as stated in section 3.4)	MNO to MNO GTP encryption by using DTLS, VPN or IPSec or other security mechanism.
Trace location of a subscriber	Read User Location Information (ULI) continuously if Mobile Station (MS) Info Change Notification Requests are sent between VPLMN and HPLMN		Ability to capture the GTP traffic (e.g. successfully control the GRX/IPX links, APN replacement or node compromise)	MNO to MNO GTP encryption by using DTLS, VPN or IPSec or other security mechanism.
	Receiving <i>Create Session Request</i> (to attacker's GGSN/PGW address) which contains the <i>User Location Information</i> IE.			See FS.19 [12], section 4.11.4 to avoid traffic interception. Filter outgoing location information, replacement with dummy location to avoid location data leakage.
Disclosure of subscriber credentials for an APN	APN credentials are part of the Point-to-Point Protocol (PPP) set-up in clear text (Password Authentication Protocol / PAP) or		Ability to capture the GTP traffic (e.g. successfully control the GRX/IPX links or node compromise)	Forcing PPP connections to restrict to CHAP authentication. MNO to MNO GTP encryption.

Attack	Method	Attack Type	Attack Pre-conditions	Mitigation
	by using Challenge Handshake Authentication Protocol (CHAP)			
Denial of service on all subscribers on the same SGSN/SGW	An attacker can spoof any GTP-C message (e.g. Echo response) then request increased Restart Counter and send it to the target node. The target node, since the counter has been increased, assumes a restart of the sending node and deletes all context assigned to this spoofed IP address.	Actively send malicious message	Target node IP reachability (e.g. access to the GRX/IPX, Internet exposure)	GSN nodes should not strictly follow this 3GPP functionality and thus not delete all contexts after restart counter indication to reduce the impact. Employ anti-spoofing on the IP firewall, at least to protect spoofing of internal IPs and other explicitly not allowed IP addresses. Ensure the recovery counter is sequential and monitor counter values on GTP-C messages.
Information gathering: Enumerate GTP NEs	Send fake Delete PDP Context Request, Delete Session Request, GTP Echo Request or other messages. Most times the peer provides an answer if the message is implemented.	Actively send malicious message	Target node IP reachability (e.g. access to the GRX/IPX, Internet exposure)	Employ firewall IP level 3 filtering to whitelist only valid roaming partners. For filtering of the messages from roaming partners, GTP Cat2 and Cat3 filtering is required.
Unauthorised access to an APN	Visited SGSN/SGW tells home GGSN/PGW by Selection Mode IE in Create session request/Create PDP Context Request that the home HLR/HSS would allow this access. GGSN/PGW does not validate the user profile with PCRF if the given IMSI is provisioned with the APN.		Target node IP reachability (e.g. access to the GRX/IPX, Internet exposure)	Use GTP Cat3 filtering to compare location of subscribers to reduce the attack surface. Ensure PPP connections are restricted to CHAP authentication.

Attack	Method	Attack Type	Attack Pre-conditions	Mitigation
Billing fraud: cause expenses for another subscriber	Spoofed/Stolen IMSI in Create Session Request or Create PDP Context Request		Target node IP reachability. Spoofed/stolen IMSI	Implement GTP Cat3 protection. Verify the subscriber location with current SS7 and Diameter location.
Impersonation of a subscriber on the network behind the destination APN	Spoofed/Stolen IMSI or Spoofed/Stolen MSISDN in Create Session Request / Create PDP Context Request. High risk the MSISDN is later used in HTTP enrichment and used for web authentication.		Target node IP reachability Spoofed/stolen IMSI or Spoofed/stolen MSISDN. NB. Retrieving MSISDN can be easier than IMSI. IMSI can be retrieved in several ways such as SS7 signalling messages abuse [10]. Valid APN. The APN configured for an IMSI can be retrieved, for example, on operator's website or abusing other signalling protocols like Diameter [12] or by compromising end-user's or customer's equipment configurations.	Implement GTP Cat3 protection. Verify the subscriber location with current SS7 and Diameter location.
Redirect existing GTP-U traffic to another SGW/PGW	Send Update PDP Context or Modify Bearer Request message with parameters that change the SGW.	Actively send malicious message	Target node IP reachability, Valid TEID retrieved in advance by means of other attacks. Bearer ID (default 5 can be used or it can be guessed by a brute force on 4 digits)	GTP Cat3 filtering function to Monitor location of subscribers on MAP/Diameter.
	Send <i>Insert Subscription Data</i> (IDR) with PGW set to Attacker PGW IP and allocation of PDN GW		Knowledge of IMSI	See FS.19 [12], section 4.11.4

Attack	Method	Attack Type	Attack Pre-conditions	Mitigation
	to Static for the target APN. Next <i>Create Session Request</i> is sent to the Attacker PGW IP.			
	Send Create Bearer Request with uplink TFTs that change uplink traffic to the attacker's PGW via the newly established dedicated bearer.		Target node IP reachability, Valid TEIDs retrieved in advance by means of other attacks. Bearer ID (default 5 can be used or it can be guessed by a brute force on 4 digits)	Employ firewall IP level 3 filtering to white list only valid roaming partners IP sources, and allow modification of User Plane session parameters only for the same partner IP sources. Check abnormal number of Create Bearer Request messages, or the establishment of dedicated bearers for unknown use cases. CDRs are created for the dedicated bearers established, so this could also be detected by fraud management.
Denial of service on all subscribers on one board of a SGW	Send Delete PDN Connection Set Request with a valid FQ-CSID		Target node IP reachability Valid FQ-CSID	Employ firewall IP level 3 filtering to white list only valid roaming partners IP sources.
Denial of service on all subscribers on the same GGSN/PGW	Create PDP Context or Create Session Request message is constantly being sent to exhaust the pool of IP addresses assigned to a PGW	Actively send flood of malicious messages	Target node IP reachability, Valid IMSI prefix. Valid APN	Employ firewall IP level 3 filtering to white list only valid roaming partners IP sources.
Steering of roaming/ Denial of service to all subscribers	Always send fault cause in response to Create PDP Context Request/Create Session Request	Actively suppress legitimate message and send malicious message	Man on the Side (MOTS) or Man in the Middle (MITM) (e.g. achieved by successfully controlling the GRX/IPX links or node compromise). Please note	Monitor the number of inbound roamers versus the utilisation of GTP-U traffic.

Attack	Method	Attack Type	Attack Pre-conditions	Mitigation
			this pre-condition is non-trivial and requires the correct timing and a valid TEID.	
Injecting GTP messages by prediction of TEID	Attacker is able to predict TEID and therefore able to inject illegal messages in the GTP-U tunnel or even inject the GTP-C response messages. The attack is applicable and more easily to conduct if non-random TEID allocation is used.	Actively send messages while knowing TEID. This attack enables advanced attacks and allows exploits using additional messages.	Target node IP reachability MoTS or MITM (not mandatory) Valid TEID	Employ firewall IP level 3 filtering to white list only valid roaming partners IP sources. Ensure TEID values are randomized. Employ plausible network traffic checking and drop any unauthorised traffic.
DoS or other exploitation of network element.	Malformed messages could cause DoS or otherwise affect or exploit the vulnerable protocol stack or vulnerable network element from certain vendors. These types of signalling vulnerabilities do not result from network architecture or protocol design, but are vendor and implementation dependent.	Actively send one or more malformed messages	Target node IP reachability	Ensure network element is protected against fuzzing attacks or empty IEs. Use GTP firewall to check formats and validate messages.
GTP integrity compromise	Injection into the GTP-U user plane is possible allowing quantum inserts and exploitation by targeting the users based on IMSI/MSISDN	Actively send malicious message	MITM (e.g. realized by successfully controlling the GRX/IPX links or node compromise)	Employ firewall IP level 3 filtering to white list only valid roaming partners IP sources. Employ GTP Cat3 protection. Verify the subscriber location with current SS7 and Diameter location.

Table 3 – Summary of Malicious GTP Attacks

6 Resources and Complexity

It is important to understand that securing GTP requires time and expertise. MNOs need to implement a secure network architecture, to configure NEs and to deploy and configure a GTP firewall. In addition, it is not enough to configure the GTP firewall once. Experts need to be available to operate and maintain the firewall and to test the network after firewall deployment. For example, the firewall configuration will need to be updated if peer operators change their IP addresses. There might also be a need to change some firewall parameters over time in order to cope with bandwidth requirements and scalability issues. Therefore, it is also recommended to implement independent signalling monitoring (or signalling IDS) which could continuously monitor and validate the network protection by detecting the exploited attacks and signalling anomalies.

Beyond that, all of the other GTP-aware NEs need to be configured securely and be kept up-to-date. Investing in the resources to perform these tasks is necessary if a MNO wishes to keep full control over its network and to prevent attackers from gaining access to the sessions or session information of subscribers.

The key to success is to implement a well-designed network architecture, and to establish an expert team that deals with firewall, signalling security monitoring and NE maintenance. GTP firewall maintenance is not a full time job, and it may be possible to include this in the responsibility of the teams who maintain the mobile core network and/or the access to the IPX network.

Annex A List of GTP Messages

A.1 GTP Messages of the S8 Interface (GTPv2)

The following GTPv2 messages belong to the 3GPP S8 interface. They need to be allowed for inter-PLMN communication on the IPX network.

The classification of the messages between GTP-C and/or GTP-U is as specified in 3GPP TS 29.060 [2].

Message Type	GTP Message	Reference	GTP-C	GTP-U
1	Echo Request	3GPP TS 29.274, TS 23.007	X	X
2	Echo Response	3GPP TS 29.274, TS 23.007	X	X
3	Version Not Supported Indication	3GPP TS 29.274	X	
32	Create Session Request	3GPP TS 29.274	X	
33	Create Session Response	3GPP TS 29.274	X	
36	Delete Session Request	3GPP TS 29.274	X	
37	Delete Session Response	3GPP TS 29.274	X	
34	Modify Bearer Request	3GPP TS 29.274	X	
35	Modify Bearer Response	3GPP TS 29.274	X	
38	Change Notification Request	3GPP TS 29.274	X	
39	Change Notification Response	3GPP TS 29.274	X	
164	Resume Notification	3GPP TS 29.274	X	
165	Resume Acknowledge	3GPP TS 29.274	X	
64	Modify Bearer Command	3GPP TS 29.274	X	
65	Modify Bearer Failure Indication	3GPP TS 29.274	X	
66	Delete Bearer Command	3GPP TS 29.274	X	
67	Delete Bearer Failure Indication	3GPP TS 29.274	X	
68	Bearer Resource Command	3GPP TS 29.274	X	
69	Bearer Resource Failure Indication	3GPP TS 29.274	X	
71	Trace Session Activation	3GPP TS 29.274	X	
72	Trace Session Deactivation	3GPP TS 29.274	X	
95	Create Bearer Request	3GPP TS 29.274	X	
96	Create Bearer Response	3GPP TS 29.274	X	
97	Update Bearer Request	3GPP TS 29.274	X	
98	Update Bearer Response	3GPP TS 29.274	X	
99	Delete Bearer Request	3GPP TS 29.274	X	
100	Delete Bearer Response	3GPP TS 29.274	X	
101	Delete PDN Connection Set Request	3GPP TS 29.274, TS 23.007	X	

102	Delete PDN Connection Set Response	3GPP TS 29.274, TS 23.007	X	
162	Suspend Notification	3GPP TS 29.274	X	
163	Suspend Acknowledge	3GPP TS 29.274	X	
200	Update PDN Connection Set Request	3GPP TS 29.274, TS 23.007	X	
201	Update PDN Connection Set Response	3GPP TS 29.274, TS 23.007	X	

Table 4 – GTP Messages of the S8 Interface (GTPv2)**A.2 GTP Messages of the Gp Interface (GTPv1)**

The following GTPv1 messages belong to the 3GPP Gp interface. They need to be allowed for inter-PLMN communication on the GRX/IPX network.

The classification of the messages between GTP-C and/or GTP-U is as specified in 3GPP TS 29.060 [2].

Message Type	GTP Message	Reference in TS 29.060	GTP-C	GTP-U
1	Echo Request	7.2.1	X	X
2	Echo Response	7.2.2	X	X
3	Version Not Supported	7.2.3	X	
16	Create PDP Context Request	7.3.1	X	
17	Create PDP Context Response	7.3.2	X	
18	Update PDP Context Request	7.3.3	X	
19	Update PDP Context Response	7.3.4	X	
20	Delete PDP Context Request	7.3.5	X	
21	Delete PDP Context Response	7.3.6	X	
22	Initiate PDP Context Activation Request	7.3.12	X	
23	Initiate PDP Context Activation Response	7.3.13	X	
26	Error Indication	7.3.7		X
27	PDU Notification Request	7.3.8	X	
28	PDU Notification Response	7.3.9	X	
29	PDU Notification Reject Request	7.3.10	X	
30	PDU Notification Reject Response	7.3.11	X	
31	Supported Extension Headers Notification	7.2.4	X	X
96	MBMS Notification Request	7.5A.1.1	X	
97	MBMS Notification Response	7.5A.1.2	X	

98	MBMS Notification Reject Request	7.5A.1.3	X	
99	MBMS Notification Reject Response	7.5A.1.4	X	
100	Create MBMS Context Request	7.5A.1.5	X	
101	Create MBMS Context Response	7.5A.1.6	X	
102	Update MBMS Context Request	7.5A.1.7	X	
103	Update MBMS Context Response	7.5A.1.8	X	
104	Delete MBMS Context Request	7.5A.1.9	X	
105	Delete MBMS Context Response	7.5A.1.10	X	
112	MBMS Registration Request	7.5A.2.1	X	
113	MBMS Registration Response	7.5A.2.2	X	
114	MBMS De-Registration Request	7.5A.2.3	X	
115	MBMS De-Registration Response	7.5A.2.4	X	
116	MBMS Session Start Request	7.5A.2.5	X	
117	MBMS Session Start Response	7.5A.2.6	X	
118	MBMS Session Stop Request	7.5A.2.7	X	
119	MBMS Session Stop Response	7.5A.2.8	X	
120	MBMS Session Update Request	7.5A.2.9	X	
121	MBMS Session Update Response	7.5A.2.10	X	
128	MS Info Change Notification Request	7.5B.1.1	X	
129	MS Info Change Notification Response	7.5B.1.2	X	

Table 5 – GTP Messages of the Gp Interface (GTPv1)**A.3 GTP Messages of the Gp Interface (GTPv0)**

The following GTPv0 messages belong to the legacy 3GPP Gp interface. They need to be allowed for inter-PLMN communication on the GRX/IPX network, if the peer PLMN only supports GTPv0. Since GTPv0 is deprecated, GTPv0 messages should be dropped by default.

The classification of the messages between GTP-C and/or GTP-U is as specified in 3GPP TS 29.060 [2].

Message Type	GTP Message	Reference in TS 29.060	GTP-C	GTP-U
1	Echo Request	7.4.1	X	X

2	Echo Response	7.4.2	X	X
3	Version Not Supported	7.4.3	X	
16	Create PDP Context Request	7.5.1	X	
17	Create PDP Context Response	7.5.2	X	
18	Update PDP Context Request	7.5.3	X	
19	Update PDP Context Response	7.5.4	X	
20	Delete PDP Context Request	7.5.5	X	
21	Delete PDP Context Response	7.5.6	X	
22	Create AA PDP Context Request	7.5.7	X	
23	Create AA PDP Context Response	7.5.8	X	
24	Delete AA PDP Context Request	7.5.9	X	
25	Delete AA PDP Context Response	7.5.10	X	
26	Error Indication	7.5.11		X
27	PDU Notification Request	7.5.12	X	
28	PDU Notification Response	7.5.13	X	
29	PDU Notification Reject Request	7.5.14	X	
30	PDU Notification Reject Response	7.5.15	X	

Table 6 – GTP Messages of the Gp Interface (GTPv0)

Annex B GTP Risk Classification

The following annex contains messages mapped to corresponding message categories, and an indication of associated risk. Explanations of message categories can be found in section 4.3.



GTP Risk
Classification.xlsx

Annex C GTP Firewall Recommendations

C.1 Introduction

This section provides guidelines aimed at MNOs implementing and/or maintaining GTP signalling firewall solutions and seeking to achieve adequate protection of their network and the mutual protection between networks against signalling vulnerabilities in GTP. Solutions may vary and be implemented differently to, or go beyond these rules. These rules are however intended to provide a description of an adequate, broadly implementation-agnostic version of the required rules to protect against the potential threats currently understood and documented in Annex B. This Annex does not attempt to address the specific issues encountered in “real world” signalling such as roaming hubs and operator group services. This section only discusses aspects for the protection of the GTP protocol and does not address the details of the GTP protocol or other signalling protocols.

The requirements in this section focus on three aspects to be supported by a GTP signalling firewall solution:

1. The rules specification in a vendor-agnostic and human readable ‘pseudo-code’ with the purpose to provide MNOs with the same type of protection for vulnerabilities irrespective of the vendor of the GTP signalling firewall solution.
2. The rules detailed in this document are intended to be applied to the GTP traffic incoming from the external Point of Interconnect (POI) of the GTP firewall.
3. The logging generation in a vendor-agnostic manner to define standard contents and formats of logging data to enable:
 - The minimal set of information to be output by the GTP signalling firewall in order to exchange information about GTP vulnerabilities between networks
 - The exchange of information between MNOs about threats and new vulnerabilities.

This version of the document contains a simplified set of filtering rules as explained in more detail in section C.3.1.4. Possibly more restrictive filtering will be specified in the future if attack vectors become more sophisticated, requiring additional protection via correlation of information only available in other network nodes and via other protocols.

The implementation of specific rules needs to take into account roaming hubs, technology gateways, network changes and centralised services in an operator group. These are not considered in this document.

An overview of the signalling vulnerabilities, prevention and recommended counter measures is to be found in other GSMA documents like the LTE and EPC Roaming Guidelines in GSMA PRD IR.88 [17], and other GSMA fraud and security related documents and guidelines.

C.2 Definitions

The rules described later in this section require a number of concepts to be defined. The list of definitions in the following table avoids repeated use of references within the GTP firewall rules specification later in this section.

Term	Description
roamingPartnerIPList	The union of all IP addresses of roaming partners identified by sensing IP Address, IP_Address_List
blackListIPAddress	A list of IP addresses that may be used to block inbound messages from hostile GTP network nodes
whiteListIPAddress	A list of IP addresses that may be used to allow inbound messages from friendly GTP network nodes
unusedGtpMessageType	A list of GTP message types that may be used to block vulnerable messages
ownNetworkRealm	The realm value allocated for routing the messages to the set of GTP nodes of the own network
roamingPartnerRealms	A list of realms used as GTP IDs by nodes in partner roaming networks
GTPC_MessageTypeAllowedOnPOI	Message Type = 1-3, 24-25 and 255 in both directions on Gp for GTPv0 1-3, 31 and 255 in both directions on Gp for GTPv1 1-3, 101-102 in both directions on S8 for GTPv2 Note: Additional message types are allowed on the POI subject to the Cat 2/3 GTP-C requests as per the definitions below
GTPC_MessageTypeNotAllowedOnPol	Message Type = 4-7 in both directions on Gp and S8 for all GTP versions 0, 31-254 in both directions on Gp for GTPv0 0, 32-127, 130-254 in both directions on Gp for GTPv1 0, 8-31, 42-63, 70-94, 103-161, 166-199, 202-256 in both directions on S8 for GTPv2
GTPC_Request_Cat3_OnPol	Message Type = 16-23 and 29-30 on Gp for GTPv0 16-21, 29-30 and 128-129 on Gp for GTPv1 32-41, 64-69, 162-165 and 200-201 on S8 for GTPv2
GTPC_Request_Cat2_OnPol	Message Type = 27-28 on Gp for GTPv0 22-23 and 27-28 on Gp for GTPv1 95-100 on S8 for GTPv2
GTPU_MessageTypeAllowedOnPOI	Message Type = 1, 2, 26 and 255 in both directions on Gp for GTPv0

Term	Description
	1, 2, 26, 31 and 254-255 in both directions on Gp for GTPv1 (the 254 end marker message type is not normally used on Gp interface) 1 and 2 in both directions on S8 for GTPv2 (normally there is no GTP-U in v2 version but the echo could be supported by some network element implementations)
Last_Sub_SS7_Loc	Last subscriber location seen from SS7 signalling based on IMSI or MSISDN
Last_Sub_Diameter_Loc	Last subscriber location seen from Diameter signalling based on IMSI or MSISDN

Table 7 – GTP definitions for firewall rules

C.3 GTP Firewall Rules

C.3.1 General

C.3.1.1 Scope

The focus of the GTP firewall recommendations in this document are on signaling protection as described explicitly in section 4.3.5. As a result, the GTP-U aspects are covered in a limited manner only.

In addition, the document focusses on the roaming interfaces, so non-roaming interfaces like S5/Gn are not addressed in this document.

The GTP firewall rules in the subsequent sections describe:

4. Filtering of GTP messages over the S8 interface for GTPv2 as in section A.1.
5. Filtering of GTP messages over the Gp interface for GTPv1 as in section A.2.
6. Filtering of GTP messages over the Gp interface for GTPv0 as in section A.3.
7. Essential sets of firewall rules for:
 - GTP Low-Layer Format filtering with the rules for GTP L3/L4 filtering in C.3.2.1
 - GTP Category 1 with the rules for GTP-C and GTP-U message types in C.3.3
 - GTP Category 2 with the rule to protect home subscribers in C.3.4
 - GTP Category 3 with the rule to protect subscribers that are not roaming in C.3.5.
8. Additional capabilities like the possibility to define customized filtering rules.

The GTP firewall rules reference the GTP risk classification table in Annex B for the categorization of vulnerabilities. This table also outlines what GTP message types are risky.

C.3.1.2 Implementation considerations

The implementation of the GTP firewall needs flexibility to add additional codes based on experience and/or updates suggested in future versions of this PRD.

The order in which the GTP firewall rules are executed is not implied by the rule descriptions in this document. This is implementation specific and may vary per operator and/or network situation.

The characteristics and volumes are very different from SS7 and Diameter and given the very different purposes of GTP-C and GTP-U messages. Hence a modular approach may be considered as for the relationship between the IP firewall functions and the application signalling firewall functions that are described in GSMA PRD FS.21 [22]. The simpler checks of GTP-U messages are more comparable to the checks performed by an IP firewall versus the more in-depth application signalling checks of GTP-U messages and potential risk of multi-domain attacks as described in section C.3.1.5.

C.3.1.3 Differences between GTP-C and GTP-U

In terms of network signalling vulnerabilities, GTP-C and GTP-U exhibit a number of differences, which need to be taken into account when considering mitigations:

- a) Attackers will invariably depend on GTP-C signalling as a first step before attacking over either GTP-C or GTP-U.
- b) The MNO tasked with signalling protection is typically not the owner of applications that the UE connects to over GTP-U.
- c) Passive discovery or intercept attacks over GTP-U require a number of magnitudes more resources to mitigate versus GTP-C. The volumes on GTP-U traffic are driven by user application adoption and grows exponentially. GTP-C traffic is growing more predictably and linearly based on population and mobility.
- d) In order to monitor GTP-U Echo Request/Response, such messages must be identified/isolated by the signalling firewall from the vast amount of user GTP-U application payload
- e) Attackers get more return on their effort over GTP-C and similarly MNOs get more protection value for their investment on GTP-C versus GTP-U.

As a consequence, in Table 7 a split is made between the definitions for GTP-C messages and the definitions for GTP-U messages that may ease network implementations where the protection of GTP-C and GTP-U will be split in different functional entities.

C.3.1.4 Filtering mechanism

Considering the simplified set of filtering rules for GTP in the current version of the document, as explained in section C.1, different policies apply to the type of filtering mechanism.

It is recommended to implement the execution of the GTP firewall rules according to the whitelist principle for both the Low-Layer Format Filtering rules in section C.3.2 and the Category 1 Filtering rules in section C.3.3. This ensures a restrictive filtering principle that only allows the passing of information that is explicitly defined by the GTP firewall rules. Consequently, the GTP firewall rules in the subsequent sections are notated following the "ALLOW" description.

This "ALLOW" principle for whitelist filtering aligns with the standard 'default deny' working of IP firewalls and Internet firewalls whereby traffic is blocked by default unless the received

message conforms to upfront defined criteria (whitelist). It is important, however, to note that using the “ALLOW” principle, all rules must evaluate to ALLOW to eventually allow the message, whereas under the “BLOCK” principle, a single rule that evaluates to “BLOCK” shortcuts the processing and the message can be blocked without evaluating the subsequent rules.

However, in the current version of the document the less restrictive “BLOCKED” principle is specified for both the Category 2 filtering rules in section C.3.4 and the Category 3 filtering rules in section C.3.5 and so offering the following network protection:

- Category 2 – Only protecting home subscribers in the home network but no protection of inbound roamers
- Category 3 – Only protecting home subscribers in the home network but no protection of outbound roamers.

These simplified “BLOCKED” definitions are followed to ensure that messages are only blocked based on the information available within the GTP-C messages to avoid the generation of unnecessary false/positives and undesired customer service degradation incidents.

Not in scope in the current version of the document are:

- More sophisticated solutions providing additional information about the exact location of the subscriber e.g. via either reverse DNS resolution or other protocols like SS7, Diameter and SIP
- Signalling firewall filtering rules based on the additional GTP-C policies in Table 2 in section 4.3.5.

It is recognised that the “ALLOW” principle deviates from the way the SS7 firewall rules are described in GSMA PRD FS.11 Annex B [11] based on the “BLOCK” principle. However, the situation for SS7 is different as the vulnerabilities in SS7 MAP are already widely known and there are no initiatives anymore to further develop the SS7 MAP protocol.

The implementation of a firewall could equally use the “BLOCK” principle (i.e. where rules for threats are defined) or the “ALLOW” principle (i.e. where rules for valid traffic are defined). The rules herein can simply have logic reversed if the “BLOCK” approach is used.

In the clauses hereafter, the default action is proposed but for each rule, it should also be possible to enable just logging or a combination of the logging with the “BLOCK” or “ALLOW” action.

C.3.1.5 Protection against multi-domain attacks

The firewall rules in this Annex C are specified for the GTP interfaces. However, attack vectors may span multiple domains like IP layer 3, IP layer 4, SS7, Diameter and GTP.

Such multi-domain attacks do not require additional GTP firewall rules since the current proposed recommendations address the known vulnerabilities:

- The retrieval of information such as TEID, IMSI, MSISDN and location information can be done in different ways using GTP, Diameter and SS7, where MNOs facilitate

access via GTP, Diameter and SS7. In such cases the GTP connections need to be protected with the firewall rules as described in this document and the SS7 and Diameter connections with the SS7 firewall rules in GSMA PRD FS.11 [11] and the Diameter firewall rules in FS.19 [12], respectively.

- This protection against multi-domain attacks can be achieved by a multi-protocol integrated GTP/Diameter/SS7 signalling firewall. However, a modular approach may also be considered with the exchange of information between different modules to distribute the risk (and to avoid the combined firewall is working as a honeypot for attackers) as well as to have distributed firewall execution with local protection per GTP service instance, Diameter service instance or SS7 service instance. See also the implementation considerations in section C.3.1.2.
- For IP layer the relationship between the IP firewall functions and the application signalling firewall functions are described in FS.21 [22].

C.3.2 Low-Layer Format Filtering

C.3.2.1 GTP L3/L4 Filtering

The following Layer 3 and Layer 4 rules should be included for all later filtering.

Title	Rule	Rationale
GTP-C Message L3/L4 filtering	for each inbound GTP-C message, If Dst UDP Port = 2123 If IPAddress = whitelistIPAddress then ALLOW	Allow only received GTP-C messages from trusted partners

Table 8 – GTP-C Message Layer3 and Layer4 filtering rule

Title	Rule	Rationale
GTP-U Message L3/L4 filtering	for each inbound GTP-U message, If Dst UDP Port = 2152 If IPAddress = whitelistIPAddress then ALLOW	Allow only received GTP-U messages from trusted partners

Table 9 – GTP-U Message Layer3 and Layer4 filtering rule

C.3.3 Category 1 Filtering

C.3.3.1 GTP-C Message Type filtering

This rule covers the filtering of GTP-C messages with Message Type values that are not allowed/supported on the POI.

Title	Rule	Rationale
GTP-C Message Type Cat.1 filtering	for each inbound message, If MessageType = GTPC_MessageTypeAllowedOnPOI then ALLOW	Allow only received GTP-C messages with message type values that are allowed/supported on the POI/roaming interface

Table 10 – GTP-C Message Type Cat.1 filtering rule

NOTE: This includes the message types marked as both “For future use” and “Reserved ...” in the GTP Risk Classification in Annex B. If received, these message types shall be treated as an unknown message and discarded.

As part of this firewall rule the GTP firewall should perform a consistency check of UDP filtering + check GTP version in header + check the GTP message type according to the following UDP port specifics as in TS 29.060 [2]:

- For the GTP v0 messages for all functions, the GTP messages (so including the GTP-C messages) should be received on UDP port 3386
- For the GTP messages with header v1 and header v2, the GTP-C messages should be received on UDP port 2123.

C.3.3.2 GTP-U Message Type filtering

This rule covers the filtering of GTP-U messages with Message Type values that are not allowed/supported on the POI.

Title	Rule	Rationale
GTP-U Message Type Cat.1 filtering	for each inbound message, If MessageType = GTPU_MessageTypeAllowedOnPOI then ALLOW	Allow only received GTP-U messages with message type values that are allowed/supported on the POI/roaming interface

Table 11 – GTP-U Message Type Cat.1 filtering rule

As part of this firewall rule the GTP firewall should perform a consistency check of UDP filtering + check GTP version in header + check the GTP message type according to the following UDP port specifics as in TS 29.060 [2]:

- For the GTP v0 messages for all functions the GTP messages (so including the GTP-U messages) should be received on UDP port 3386
- For the GTP messages with header v1 and header v2, the GTP-U messages should be received on UDP port 2152

C.3.4 Category 2 Filtering

C.3.4.1 GTP-C Category 2 filtering to protect home subscribers

This rule covers the filtering of GTP-C Category 2 inbound messages that target the home subscribers.

Title	Rule	Rationale
GTP-C Message Type Cat.2 filtering	for each inbound message, If (IMSI or MSISDN) is from HPLMN and MessageType = GTPC_Request_Cat2_OnPoI then BLOCK	Block Category 2 messages targeting home subscribers if the message contains IMSI or MSISDN. (For MSISDN checks also number portability with national roaming should be considered.)

Table 12 – GTP-C Message Type Cat.2 filtering rule to protect home subscribers

C.3.5 Category 3 Filtering

C.3.5.1 GTP-C Category 3 filtering

This rule covers the filtering of GTP-C Category 3 inbound messages if the subscriber is located in HPLMN.

Title	Rule	Rationale
GTP-C Message Type Cat.3 filtering	for each inbound message, If (Last_Sub_SS7_Loc is in HPLMN or Last_Sub_Diameter_Loc is in HPLMN) and MessageType = GTPC_Request_Cat3_OnPoI then BLOCK	Block Category 3 inbound messages from international interconnect if the subscriber is currently in home network on last known location based on IMSI or MSISDN.

Table 13 – GTP-C Message Type Cat.3 filtering rule to subscribers in home network

Note: Alternatively the location information of the subscriber may be retrieved by querying the HSS/HLR in the same way as for the Cat.3 plausibility checks with SS7 and Diameter.

C.4 Firewall Node Hardening

As recommended in section 4.2, the firewall node should be hardened according to well-known industry guidelines.

C.5 Firewall Data Sharing

C.5.1 General

The aim of this section is to provide advice on standard contents and formats of logging data generated by the GTP signalling firewall as a result of the firewall rules execution service logic as specified in section C.3. This may ease both the integration of the signalling firewall with other technical elements like third party systems for analytics and reporting, and sharing information between MNOs to quickly implement protection against vulnerabilities and new threats.

Such data may be generated in real-time for the interfaces with analytics systems in order to facilitate immediate alarming of new vulnerabilities. Solutions like Internet Protocol Flow Information Export (IPFIX) may be considered for this purpose. This universal IETF standard will facilitate the formatting and transfer of the data streams of multiple firewall instances to a

central collector for further processing. The data to monitoring systems may be near real-time or offline as this refers to aggregated data.

C.5.2 GTP Firewall Data Sharing

The specification of the GTP firewall data sharing in this section refers to the GTP firewall rules in section C.3 in conjunction with elements of the GTP signalling messages.

C.5.3 Data Sharing for GTP Analytics

This refers to the data generated by the GTP firewall where the GTP firewall rules execution service logic detects violations of which the details need to be reported. The reported data should contain all relevant details associated with the specific GTP vulnerability occurrence and the handling by the GTP firewall.

The specification below provides a general format that equally applies to the individual rules in section C.3. The advised format below is based on the GTP firewall rule in section C.3.3.1 (GTP-C Message Type Cat.1 filtering) as an example.

Field	Value
GTP firewall rule (name as in rule table)	GTP-C Message Type Cat.1
• Action (Passed or Blocked)	Blocked
○ Associated return action	With
○ GTP Message Name	###
○ ...	...
• Origin Host details:	...
○ IP layer 3 address	...
○ Origin-Host	...
○ Origin-Realm	...
○ ...	...
• Destination Host details	...
○ IP layer 3 address	...
○ Destination-Host	...
○ Destination-Realm	...
○ ...	...
• IE details	...
○ IMSI	...
○ MSISDN	...
○ MEI	...
○ ...	...
• GTP Message details	...
○ GTP Message Name	...
○ Sending IP layer 3 Address	...

Field	Value
○ ...	...

Table 14 – Example data sharing format for GTP analytics

C.5.4 Data Sharing for GTP Monitoring

This refers to the data generated by the GTP firewall for KPI reports, statistics, etc. This should contain aggregated data associated with the execution of the GTP firewall rules.

The specification below provides a general format that equally applies to the individual rules in section C.3. The advised format below is based on the GTP firewall rule in section C.3.3.1 (GTP-C Message Type Cat.1 filtering) as an example.

Field	Value
GTP firewall rule (name as in rule table)	GTP-C Message Type Cat.1
• Passed Normal	
○ GTP Message Name a	
▪ Sending IP layer 3 Address z	
▪ ...	
○ GTP Message Name b	
▪ Sending IP layer 3 Address y	
▪ ...	
○ ...	
• Passed Monitor	
○ GTP Message Name c	
▪ Sending IP layer 3 Address x	
▪ ...	
○ GTP Message Name d	
▪ Sending IP layer 3 Address w	
▪ ...	
○ ...	
• Blocked Silently	
○ GTP Message Name e	
▪ Sending IP layer 3 Address v	
▪ ...	
○ GTP Message Name f	
▪ Sending IP layer 3 Address u	
▪ ...	
○ ...	
• Blocked with Error	
○ GTP Message Name g	

Field	Value
▪ Sending IP layer 3 Address t	
▪ ...	
○ GTP Message Name h	
▪ Sending IP layer 3 Address s	
▪ ...	
○ ...	

Table 15 – Example data sharing format for GTP monitoring

C.6 Implementation of a GTP firewall in the network

Building on the high-level principles outlined in GSMA PRD FS.21 [22], this section provides guidelines specific to the implementation of a GTP firewall in an MNO network. This is not an exhaustive list. Its purpose is to act as a guide for MNOs that are installing a GTP firewall and are at the network architecture stage.

The implementation isn't limited to a specific deployment architecture, vendor type or hardware (e.g. commercial off-the-shelf hardware, network function virtualisation, software as a service).

The following aspects are not further detailed hereafter:

- For international traffic, the GTP firewall may also be situated in the IPX network.
- In situations where national traffic should be protected by the same firewall resources as for international traffic, the national traffic may be looped through the same routing model as for the IPX traffic.

The following sections describe different implementation options and the characteristics of each. Please also refer to the considerations described in "Use of IP network layer information in Signalling Firewalls" in GSMA PRD FS.21 [22].

C.6.1 Combined Firewall (IP + APP)

The MNO can take the advantage of the existing firewall by adding the GTP filtering rules as described in section C.3 and the associated features described in this Annex C if supported and compliant by the vendor. Hardware requirements should be taken into account if merging both the firewall functions to avoid the risk of resource exhaustion.

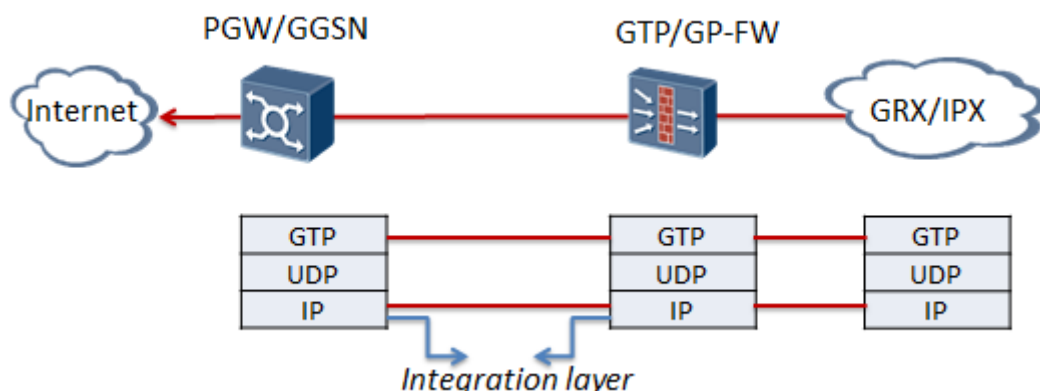


Figure 26 – Combined Firewall Implementation

- Advantage: Single point of management, end to end layer network security.
- Disadvantage: More complex firewall implementation and increased security risk with bundling of different functionalities.

C.6.2 Dedicated GTP Firewall for GTP-C and GTP-U

This deployment model separates the application from the IP layer security requirements. The Gp firewall is used to provide IP layer screening and policy control functions. The GTP firewall implements the GTP filtering rules as described in section C.3 and the associated features described in this Annex C.

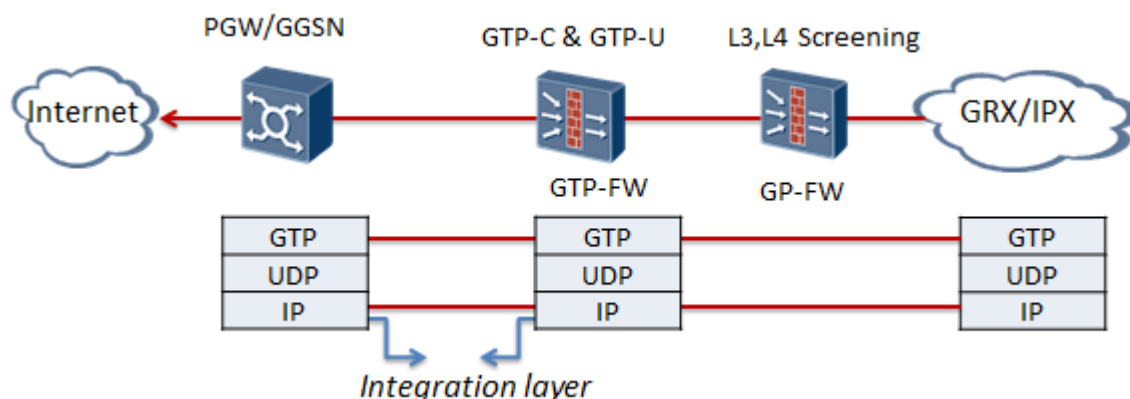


Figure 27 – Dedicated GTP Firewall (GTP-C & GTP-U) Implementation

- Advantage: Dedicated application firewall meeting the MNO's security requirements.
- Disadvantage: Doubling of functionality as the GTP firewall also will process the high volumes of GTP-U traffic that may be checked adequately by Gp firewall functions.

C.6.3 Dedicated GTP Firewall for GTP-C

This implementation has been derived from the previous deployment model which required significant hardware resources. In this approach, the GTP-C and GTP-U messages have been separated using the unique UDP ports. This allows GTP-U traffic to bypass the GTP firewall and pass directly from the Gp firewall to the PGW/GGSN.

Although this method requires policy-based routing to be placed on the Gp firewall, it allows the GTP firewall to only inspect the GTP-C traffic which is less resource intensive compared to also inspecting GTP-U traffic.

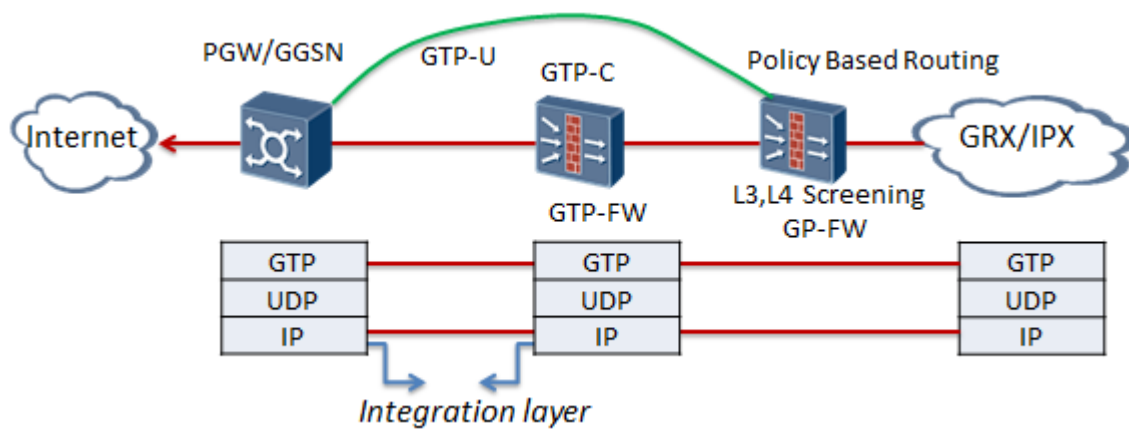


Figure 28 – Dedicated GTP Firewall (GTP-C) Implementation

- Advantage: Cost effective and transparent to the network.
- Disadvantage: The PGW needs to maintain alignment between GTP-C and GTP-U sessions to ensure adequate policy enforcement handling.

Annex D Document Management

D.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	27 Feb 2017	First version	PSMC	Sven Lachmund, Deutsche Telekom
2.0	4 May 2018	Add new attacks and variants. Add GTP risk classification matrix and GTP message categories	FASG	Pavel Novikov, Positive Technologies Martin Kacer, Philippe Langlois, Thomas Coudray, P1 Security
3.0	18 Feb 2019	Added description of subscriber DoS attack using IP address pool exhaustion. New section 5 added with summary of attacks including mitigation recommendations. Add GTP firewall rule recommendations and network implementation guidelines.	FASG	Rosalia d'Alessandro (TIM), Martin Kacer (P1 Security), Pavel Novikov (Positive Technologies) Jerry Norris, (Mobileum) Pieter Veenstra (NetNumber), Martin Kacer (P1 Security), Imran Saleem (STC) and other SIGFW members
4.0	12 Nov 2019	Explanations added in Annex B to clarify that the filtering rules in this document focus on signaling of GTP and roaming support Note added in C.3.3.1 about the handling of message types marked as "For future use" and "Reserved ..." in the GTP Risk Classification in Annex B	FASG	Gennady Dosovitsky (A10 Networks), Pieter Veenstra (NetNumber), Martin Kacer (P1 Security), Imran Saleem (STC)
5.0	23 Mar 2022	Added new data interception and location tracking attack variants	FASG	Fabricio Ferraz, (MEO), Silke Holtmanns, (AdaptiveMobile)
6.0	26 Sep 2022	Added TEID analysis and MITM attack.	FASG	Fabricio Ferraz (MEO)
6.1	21 Apr 2023	Updated GSMA logo.	N/A	David Maxwell, GSMA

D.2 Other Information

Type	Description
Document Owner	FASG
Editor / Company	Sven Lachmund, Deutsche Telekom

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.