

**:: Positive Technologies**

---

# **Threat vector: GTP**

Vulnerabilities in LTE  
and 5G networks 2020

[positive-tech.com](https://positive-tech.com)

<https://t.me/learningnets>

# Contents

- Executive summary ..... 3
- Introduction..... 4
- Materials and methods ..... 4
- Overview of GTP threats ..... 5
  - Denial of service against operator equipment..... 6
  - Fraud ..... 7
  - Impersonation ..... 8
  - Attacking via the Internet or from a user device..... 9
- What GTP vulnerabilities mean for 5G ..... 10
- What operators can do ..... 11
  - Why is existing protection ineffective? ..... 11
  - What's the solution? ..... 11
- Terms and definitions..... 12

## Executive summary

The GTP protocol contains a number of vulnerabilities threatening both mobile operators and their clients. As a result, attackers can interfere with network equipment and leave an entire city without communications, impersonate users to access various resources, and use network services at the expense of the operator or subscribers. Every network tested was vulnerable to DoS, impersonation, and fraud.

The risk level should be regarded as high: in some cases, an attack can be performed just by using a mobile phone.

Faults in the GTP protocol directly impact 5G networks. At the moment, 5G Non-Standalone networks are deployed on the EPC core network. Therefore, all these threats also apply to current 5G networks. The GTP protocol will partially remain in the Standalone architecture, so its security will remain a key issue for a long time.

# Introduction

The GTP protocol is used to transmit user and control traffic on 2G, 3G, and 4G networks. We have previously explored certain flaws in the protocol which can lead to interception of user data, fraud, and denial of service. In this research, we explain how GTP security issues impact the security of mobile networks today, how they can affect new 5G networks, and what operators should do.

# Materials and methods

To assess the security of SS7, Diameter, and GTP networks, our experts simulate the actions of would-be external attackers. Attackers can send requests to the operator’s network, actuating a wide range of threats if the operator does not take appropriate protective measures. Malicious actions are simulated with the help of PT Telecom Vulnerability Scanner (PT TVS). The experts also use PT Telecom Attack Discovery (PT TAD) for security monitoring and detection of bona fide attacks that target vulnerabilities in the network.

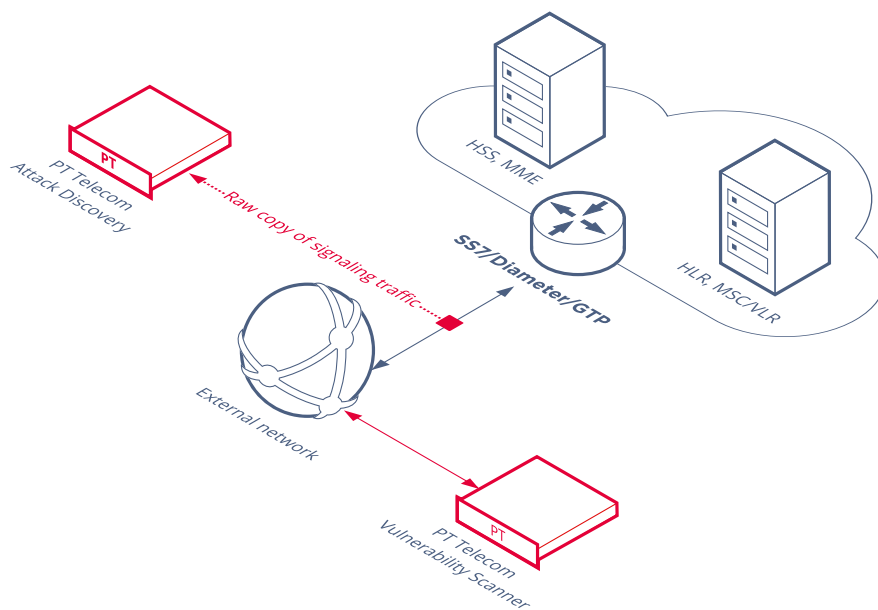


Figure 1. Workflow: security analysis

This paper encompasses the results of security assessments performed during the 2018–2019 timeframe on behalf of 28 telecom operators in Europe, Asia, Africa, and South America.

In this article, we will look at the state of security of GTP networks. For more on the biggest threats to SS7 and Diameter networks today, refer to our website.

# Overview of GTP threats

Security assessment performed in 2019 revealed that every tested GTP network carries the risk of fraud against the operator or subscribers, as well as the risk of denial of service against network equipment.

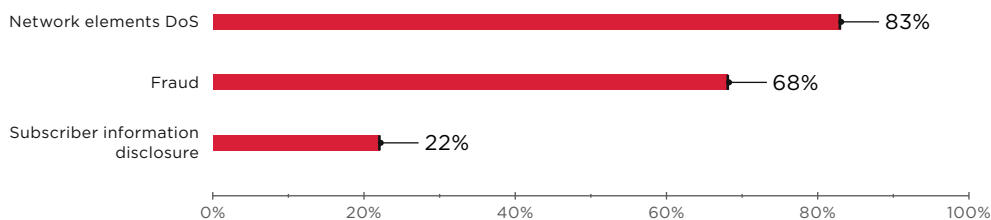


Figure 2. Successful attacks by threat type

**The GTP protocol is fundamentally flawed in that it does not check the user's actual location, which is behind half of the successful attacks**

The GTP protocol is fundamentally flawed in that it does not check the user's actual location, which is behind half of the successful attacks. Any guest network where the subscriber is currently located can send a set of signaling messages to the subscriber's home network, so it is difficult to determine whether incoming traffic is legitimate. It's a good idea to check if the subscriber really could be roaming on the network which sent a signaling message, but that would require analyzing the subscriber's movements. The problem is that location tracking must be cross-protocol, which means checking the subscriber's movements by using SS7 or Diameter. The security tools used on most networks don't have such capabilities.

There's another architectural flaw as well. In GTP, subscriber credentials are checked on S-GW (SGSN) equipment by default. However, threat actors can impersonate that host in certain attacks. This is why data for a subscriber referenced in incoming signaling traffic must undergo additional checks.

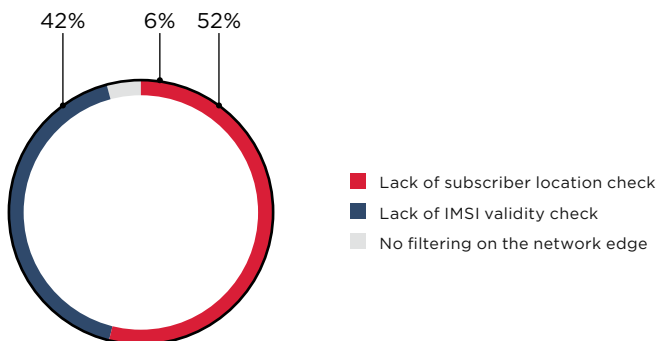


Figure 3. Vulnerabilities that enable attacks (percentage of successful attacks)

Note that to perform an attack against subscribers, the attacker first needs the IMSI (subscriber identifier) or TEID (tunnel identifier). Testers were always able to obtain the TEID, but not the IMSI. However, there are other ways to learn the IMSI, such as by attacking SS7 with a fake base station or buying a database on the darknet.

### Denial of service against operator equipment

**Bringing down a single PGW or GGSN can interrupt service for all of the operator's subscribers in an entire city or area**

Every tested network was vulnerable to denial of service against network equipment. By sending multiple requests to open new connections, the attackers exhaust the DHCP server pool or pool of GTP tunnels. The result: legitimate users cannot connect to the Internet. The attack can use non-existent IMSIs or ones belonging to actual subscribers.

Unlike DoS attacks targeted against specific users, denial of service against network equipment means loss of connection for a large number of users. A single GGSN or P-GW element is usually used to support all subscribers of the operator within a city or a region.

Mass loss of communication is especially dangerous for 5G networks, because its subscribers are IoT devices such as industrial equipment, Smart Homes, and city infrastructure.

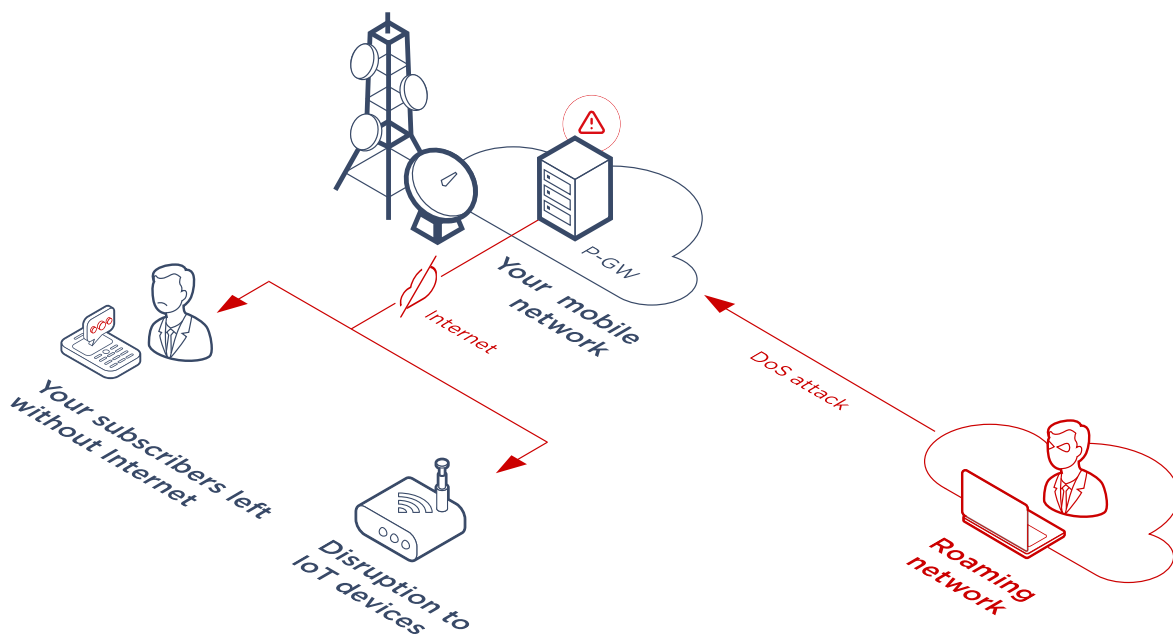


Figure 4. Diagram of a DoS attack

## Fraud

On all tested networks, it was possible to use mobile Internet at the expense of both other subscribers and the operator. If an attacker can connect using the compromised identifier of an actual subscriber, this connection will be made as that subscriber and will be paid at the subscriber's expense. If the attacker indicates a non-existent identifier, the financial losses will be incurred by the operator. These attacks can also be used by a dishonest MNO to create roaming traffic, with the MNO (falsely) charging another operator for non-existent roaming activity of that operator's subscribers.

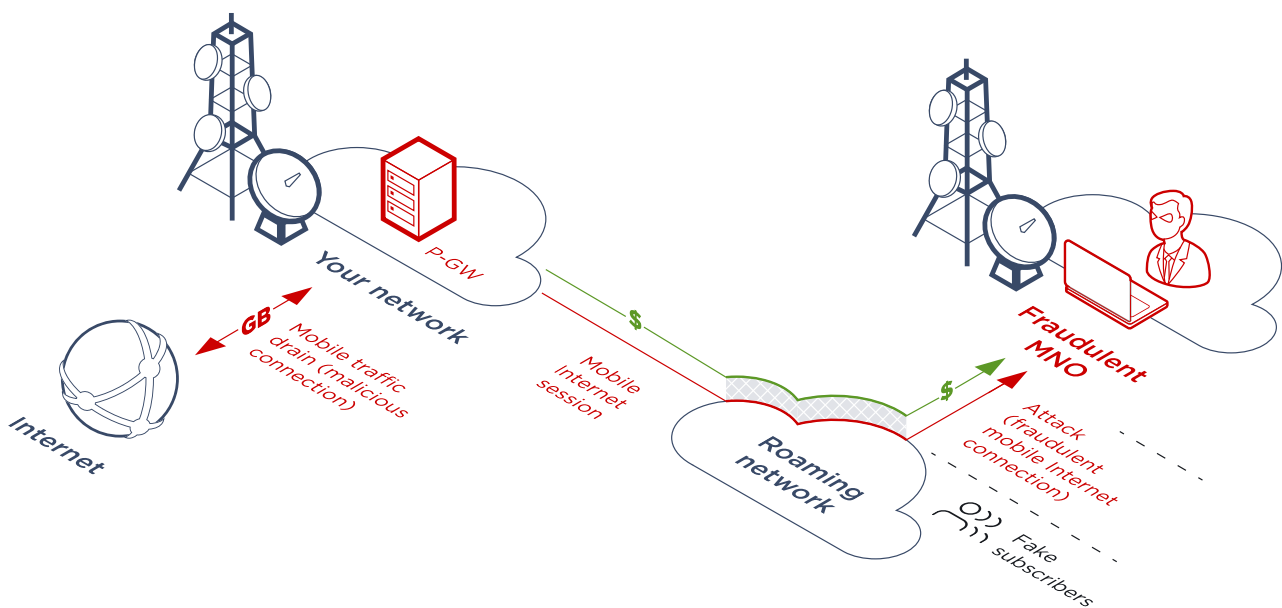


Figure 5. Diagram of an attack for fraudulent purposes

By default, subscriber credentials are checked on the S-GW or SGSN. However, in some attacks this host is spoofed. So when a request for a new connection is received, make sure the identifier matches an actual subscriber. If the subscriber really exists, verify the subscriber's location with SS7 or Diameter to make sure the subscriber does not have active sessions on the home network. Most networks did not perform such checks.

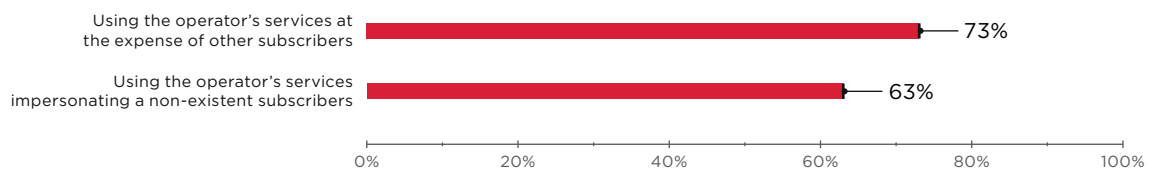


Figure 6. Attacks for fraudulent purposes (percentage of successful attacks)

## Impersonation

### Every successful attack causes

- Revenue loss
- Subscriber churn
- Damage to reputation

Another threat is access to third-party online services as an arbitrary subscriber. Such attacks can be performed in two ways: by using the method described earlier of connecting as another subscriber to impersonate that user and use the Internet at their expense, or by spoofing user session data with the identifiers (phone number) of a real subscriber. For convenience, a number of services perform pass-through authentication: the operator is sure that it is truly you because you have your SIM card, and thus automatically provides authenticated access both to its own services and those of its partners.

### Such services may be used for:

- Verifying MSISDN during account registration
- Performing anti-fraud checks (matching devices to account holders)
- Password-free authorization

This is called an impersonation attack, in which an adversary successfully assumes the identity of one of the legitimate parties in a system.

Consequences vary based on which resource or service the attacker is able to access.

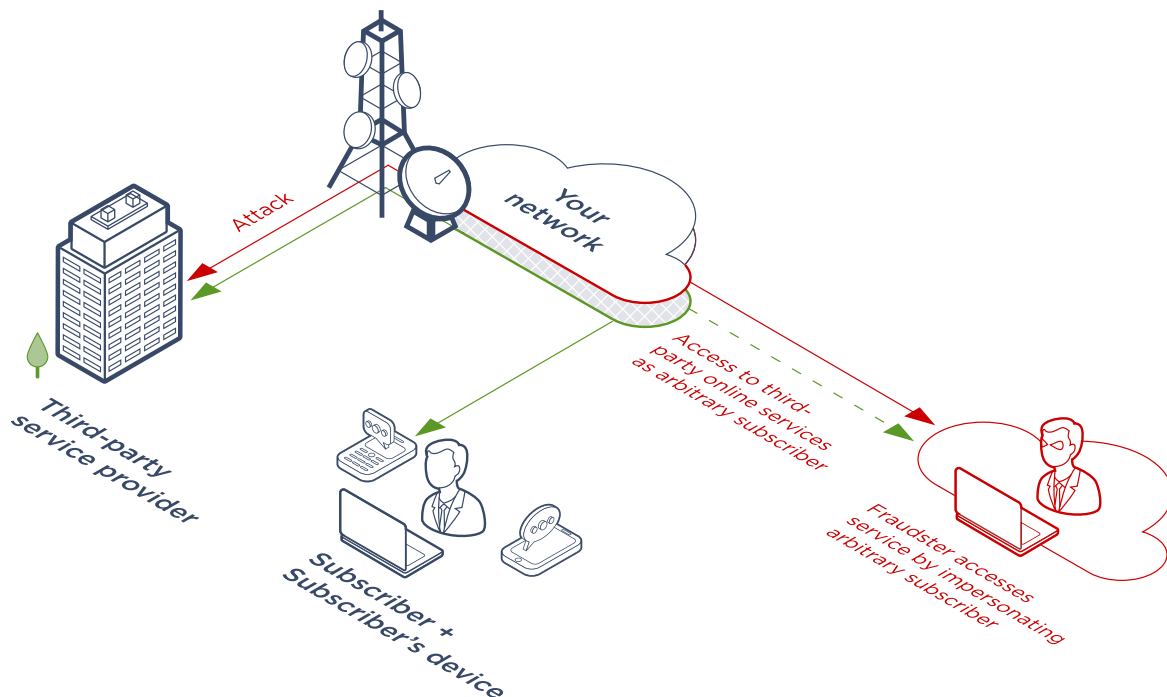


Figure 7. Diagram of an impersonation attack

In a number of cases, an attack from subscriber mobile devices was possible

### Attacking via the Internet or from a user device

During security assessment, we also check whether it is possible to attack the operator’s network without access to the inter-operator GRX: this could be via the Internet or from a subscriber’s mobile device. On the tested networks, operator equipment was not accessible from the Internet over GTP. However, in a number of cases an attack from subscriber mobile devices was possible.

Usually, the reason was that a configuration flaw on the GGSN/PGW allows encapsulating GTP-C management packets in the user’s GTP-U tunnel. In other words, attacks on GTP can be performed without access to GRX, from just a mobile phone or a modem on the network. This is a GTP-in-GTP<sup>1</sup> attack, which is very old and very well known since the early 2000s. For attackers, this is a much simpler way to achieve any of the threats described already, including denial of service against network equipment and billing fraud.

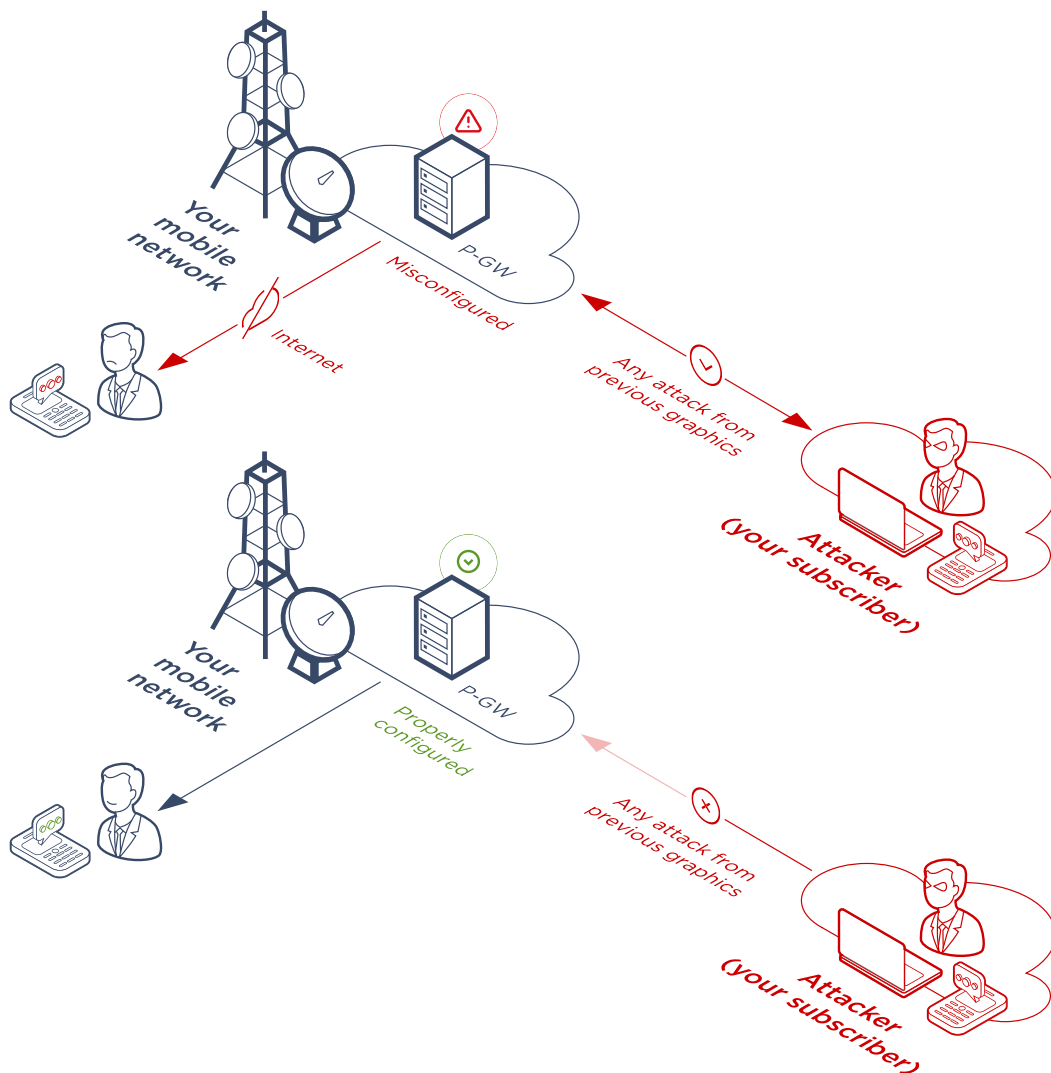


Figure 8. Diagram of a GTP-in-GTP attack

<sup>1</sup> [giac.org/paper/gsec/4364/securing-gprs-network-infrastructure-network-operator-039s-perspective/107183](http://giac.org/paper/gsec/4364/securing-gprs-network-infrastructure-network-operator-039s-perspective/107183)

# What GTP vulnerabilities mean for 5G

Testing confirmed that GTP vulnerabilities can be exploited via the inter-operator IPX network, and in some cases even from a mobile device, with adverse impacts on EPC. As of early 2020, most 5G network deployments were Non-Standalone (Option 3, for instance), using EPC as the core network for 5G. This arrangement, planned as temporary, will be the only available option for the next few years as 5G Core Standalone is being established.

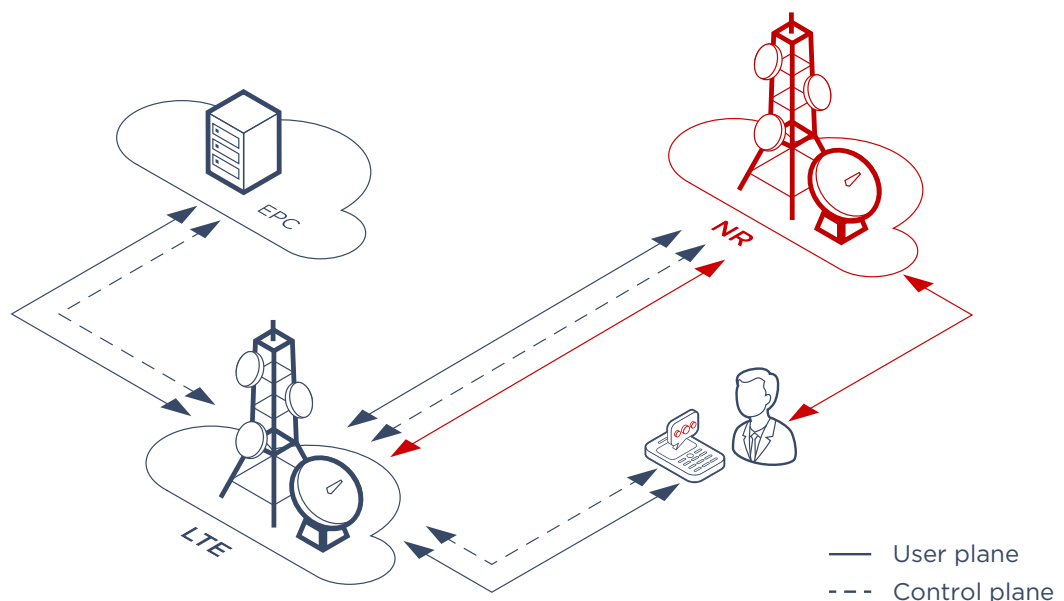


Figure 9. Diagram of Option 3



**Therefore, we can say that most of today's 5G networks, just like 4G ones, are vulnerable to the following types of attacks**

- Disclosure of subscriber information (including TEID and location data)
- Spoofing, which can be used for fraud and impersonation attacks
- DoS attacks on network equipment, resulting in mass disruption of mobile communication

GTP security issues will not go away completely even after the transition to 5G Standalone. GTP is planned for use on Standalone networks, too (including roaming), even if only to transmit user data over the GTP-U protocol. Attacks on GTP-U allow encapsulating management protocol packets in the user session (GTP-in-GTP) or obtaining data about the subscriber's connection (TEID). This is why, when 5G SA networks arrive, additional research will be required to see if the new management protocols remain vulnerable.

# What operators can do

## Why is existing protection ineffective?

The only security measure we encountered during assessment is whitelist-based IP filtering. The operator allows connections only from other operators with which it has a roaming agreement. This measure works well against third-party hosts of attackers with access to the GRX network, but falls flat when attacks come from the hacked host of a roaming operator.

Operators not only fail to protect their networks, but sometimes make serious configuration errors. For instance, on half of networks we found the S10 internal interface accessible from the outside, yielding the tunnel identifier (TEID) of a specific subscriber.

In addition, there is often lack of consistency within the company: the core network is administered by one department, but edge equipment, such as routers and firewalls, may be managed by a completely different team. The absence of overall security policies, in turn, can lead to serious configuration flaws or outright absence of security settings.

## What's the solution?

To make things better, operators need to look closely at the GTP protocol, ensure filtering at the GTP level, and deploy purpose-made security solutions.

Security must be a priority during network design. This is truer now than ever before as operators begin to tackle construction of 5G networks. Attempts to implement security as an afterthought at later stages may cost much more: operators will likely need to purchase additional equipment, at best. At worst, operators may be stuck with long-term security vulnerabilities that cannot be fixed later.

An important step is to implement [GSMA security recommendations](#). These include ongoing monitoring and analysis of signaling traffic to detect potential security threats. This can be achieved with special threat detection systems. Such solutions not only analyze traffic in real time, but also detect illegitimate activity, block it, and pass the data to other security tools.

[Security assessment](#) is a way to evaluate the effectiveness of the security tools in place. For an understanding of the current state of infrastructure, security assessment needs to be performed regularly, especially after reconfiguration or addition of network equipment.

For ultimate protection of your core network, consider Positive Technologies 5G-ready Next-Generation Firewall [Telecom Attack Discovery](#), which delivers robust active protection from multi-protocol (including GTP) attacks, DoS attacks, fraud, and network configuration errors while retaining full performance and redundancy.

**General recommendations** for securing GTP can be found in the GSMA document [FS.20 GPRS Tunnelling Protocol \(GTP\) Security](#)

## Terms and definitions

**Diameter:** signaling protocol used to transfer authentication, authorization, and accounting data on telecommunication networks

**eNodeB** (Evolved Node B): base station on LTE networks

**GGSN** (GPRS Gateway Support Node): gateway between the GPRS Core network and external packet networks

**GRX** (GPRS Roaming Exchange): network for exchanging roaming traffic between operators

**GTP-C:** protocol for managing GTP tunnels

**GTP-U:** protocol for transmitting user traffic via GTP tunnels

IMSI: International Mobile Subscriber Identity, unique to a single mobile subscriber worldwide.

**LTE** (Long Term Evolution): standard for wireless high-speed data transmission on mobile networks.

**P-GW** (Packet Data Network Gateway): gateway to data transmission networks.

**S-GW** (Serving Gateway): serving gateway for processing packets at the boundary between EPC and the radio subsystem

**SGSN** (Serving GPRS Support Node): main GPRS support node responsible for implementing all packet data processing functions

**SS7** (Signaling System 7): common channel signaling system used in international and local telephone networks around the world

**TEID** (Tunnel Endpoint Identifier): GTP tunnel identifier