SecurityGen

Telecom Security. Transcending Generations.

GTP vulnerabilities:

A cause for concern in 5G and LTE networks

Table of contents

Introduction

The rapid evolution of mobile technologies has revolutionized our daily lives, making mobile networks an essential part of modern society. However, as mobile networks continue to advance, they have also become prime targets for malicious actors seeking to exploit vulnerabilities for their malicious purposes. This analytical whitepaper explores the critical aspects of GTP (GPRS Tunneling Protocol) security, shedding light on potential risks and their implications for developing 5G networks. By understanding the details of GTP and its vulnerabilities, we can better equip mobile operators to secure their networks and protect user data in the face of emerging threats.

With the introduction of 5G networks, we observe a complex interplay between successive generations of mobile communication. While 5G networks take center stage, they rely on 4G networks for support, which, in turn, rely on the functionalities of 2G/3G networks. As the integration of these generations evolves, so do their essential vulnerabilities, with GTP serving as a common thread that runs through them. To comprehend the security challenges posed by GTP, we must analyze its design, functions, and potential attack surfaces.

GTP security

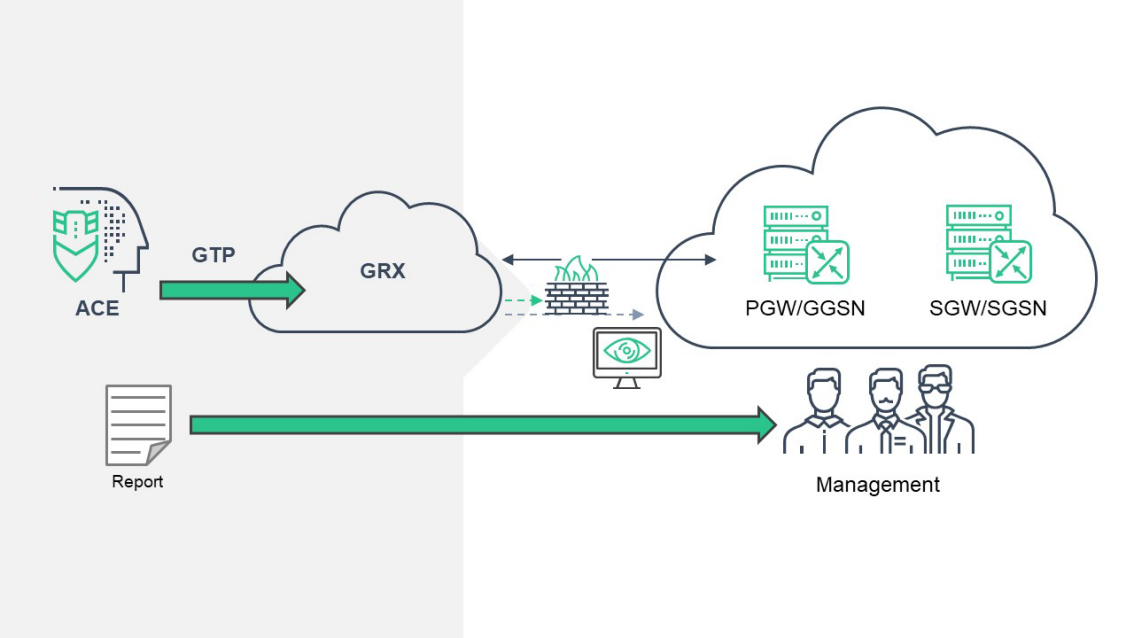
Despite its widespread use, GTP is not immune to security vulnerabilities, providing potential opportunities for attackers to intercept sensitive user data, engage in fraudulent activities, or disrupt network services. As we explore these vulnerabilities, it becomes apparent that the details of the protocol require careful consideration and robust mitigation strategies.

Like other protocols considered, GTP is fundamentally flawed due to the lack of real-time user location verification, which accounts for half of the successful attacks. The problem lies in the necessity of cross-protocol tracking, i.e., monitoring subscriber movements using SS7 or Diameter. Another architectural flaw is present in GTP, where subscriber credentials are only verified at the S-GW equipment, which is impersonated by malicious actors during certain attacks. Hence, additional checks on subscriber data, to which the signaling traffic is directed, are required.

Analytics

As Telecom cybersecurity experts at SecurityGen, one of our primary responsibilities and focus is to execute telecom security assessments (TSA) to test MNO networks for existing vulnerabilities, aiming to assess information retrieval, denial-of-service, data manipulation, fraud, and other potential threats. During these assessments, we simulate malicious actors with remote or radio interface access to MNO networks. Through regular TSAs, we have accumulated valuable statistical **data across the SEA, LATAM, and MEA regions, covering 39 MNOs in 24 countries, with over 150 TSA projects conducted during the last year.** This whitepaper highlights some of the most critical GTP-related threats, aiming to raise awareness among mobile operators and stakeholders.

The TSA methodology is as follows: we utilize a sophisticated testing tool called ACE (Artificial Cybersecurity Expert) that maintains an established connection to an IPX/GRX provider through various telecom signaling protocols, including GTP. With this connection in place, we conduct simulated malicious actions, replicating the tactics a real attacker might employ against the network under test. The attack messages are directed towards the network from the roaming interface, thus effectively emulating genuine hostile activities without any internal connection to the MNO. Each test case reproduces a specific attack scenario. This approach ensures a comprehensive evaluation of the network's security posture, enabling us to proactively identify and address potential vulnerabilities.



During most of the assessments, we used 16 basic test cases. Each test case reproduces a specific attack scenario, for instance:

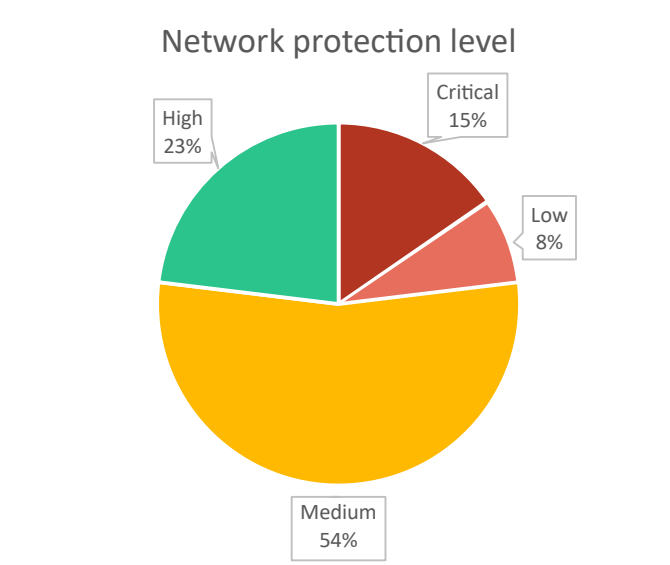
- Data interception via Create PDP Context request
- Fraud via Create Session request with a non-existent subscriber
- Impersonation via Create Session request
- Data disclosure via SGSN Context request
- Network DoS via Create Session request
- Subscriber DoS via Update PDP Context request

All these were used to verify 6 basic threats:

- Subscriber Impersonation
- Subscriber DoS
- Subscriber Data Disclosure
- Subscriber Data Interception
- Network Element DoS
- Fraud

The next chapter of the white paper contains explained results of exploitation test cases and verified threats.

Level of protection

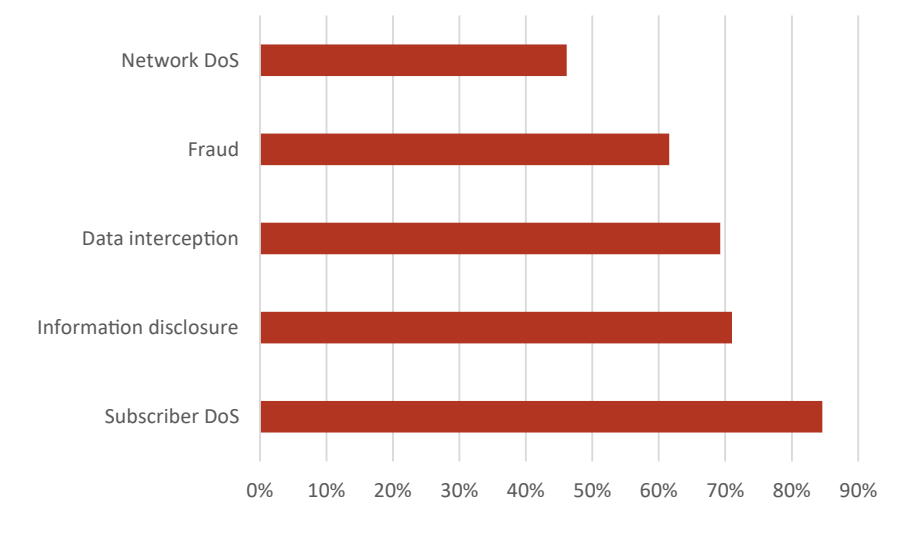


Pic. 1 – Protection levels of tested networks with exposed GTP (5G, LTE, UMTS, GSM)

First and foremost, it should be noted that **all of the tested networks exhibit some vulnerabilities in handling the GTP protocol.**

Based on the assessed level of network security, we observe that **15% of the tested networks have a critically low level of protection.** On such networks, almost all test cases were successful. **Another 8% of networks are also susceptible to numerous GTP protocol attacks,** with their level of protection evaluated as low. More than half of all networks, specifically **54%, have a medium level of security.** It is evident that network security divisions are implementing protection systems, but this remains insufficient as malicious actors can still cause significant harm to these mobile operators. **23% of networks exhibit a high level of security.** In such networks, only a few test attacks were successful. These are the same 23% of networks that strive to implement as many GSMA security recommendations as possible. The details on implemented protection measure can be found on Pic 3.

Attacks and impact



Pic. 2 - Success rate of executed attacks

1 In **71% of networks, attacks on information disclosure were successful.** Primarily, this includes obtaining the unique Tunnel Endpoint Identifier (TEID), which potential attackers require to carry out other attacks. Apart from that, the attacker could obtain all the subscriber information needed to perform other attacks as well as target other interfaces. Knowledge of encryption keys enables attacks on the radio interface. With the device IMEI, an attacker can determine the operating system on the device to target known OS vulnerabilities. Knowledge of the IP addresses of relevant PGW/GGSN and SGW/SGSN enables attacks on the GTP protocol, and after obtaining the subscriber's internal IP address, perform attacks within the network.

2 **62% of networks are vulnerable to fraudulent actions involving the GTP protocol.** The result of these actions can be the illicit acquisition of services, either at the expense of subscribers or the mobile operator itself. At present, we have not yet observed any indicators suggesting widespread exploitation of these vulnerabilities. The reasons may be either a lack of intrusion detection tools using the GTP protocol on the part of mobile operators, or the fact that fraudsters currently utilize well-established techniques with clear monetization schemes.

3 **85% of networks are susceptible to targeted attacks on subscribers,** aiming to degrade or completely interrupt the functionality of data transmission services. This involves the use of different techniques, such as establishing a fake session on behalf of a subscriber, leading to the disruption of the ongoing legitimate session; illegitimate changes to SGSN and GGSN serving nodes, causing user traffic to be directed to nodes unable to handle the respective session; and deletion of information on the subscriber's current session from databases.

4 **46% of the tested networks were vulnerable to network equipment denial-of-service attacks**. By sending numerous requests to open new connections, an attacker occupies the entire DHCP server pool or GTP tunnels pool, resulting in legitimate users being unable to connect to the internet. The attack is conducted using both real subscriber IMSIs and non-existent identifiers. Unlike attacks targeting the denial of service for individual subscribers, network equipment denial means the absence of network connection for a large number of users simultaneously.

5 **User traffic interception was successful in 69% of the networks.** The intruder can change the actual nodes that process the user traffic to their own host. In this way, all incoming traffic is handled by the intruder's equipment.

Possible protection measures

There are three main approaches to protection:

1. Filtering incoming traffic based on IP addresses of roaming partners.
2. Implementing GSMA-recommended security measures.
3. Combination of the approaches mentioned above.

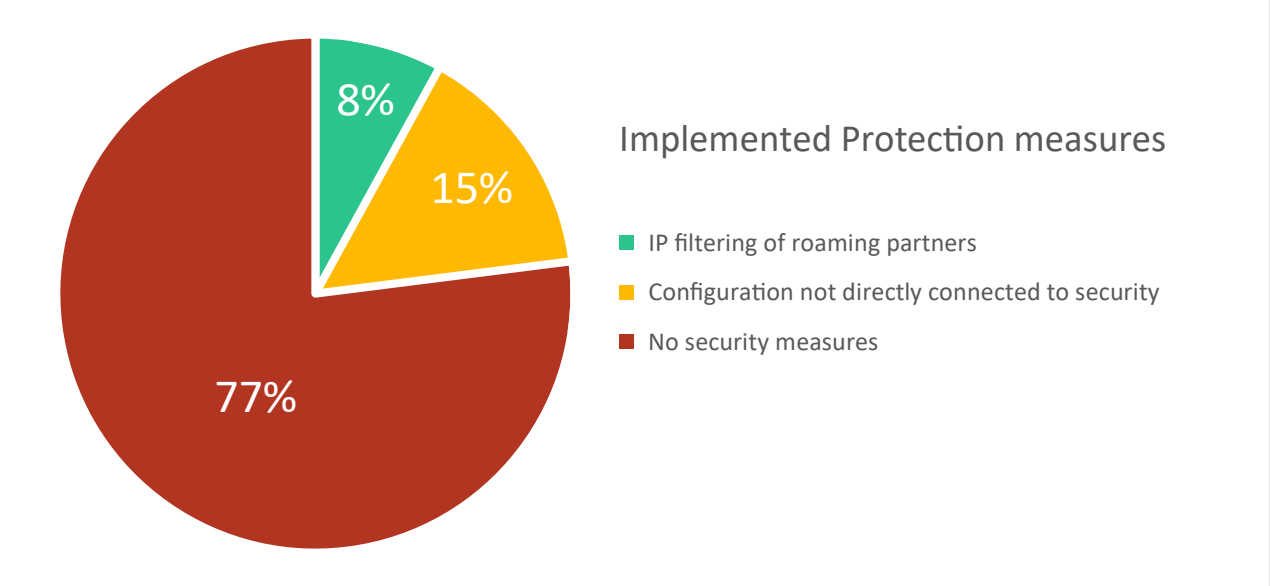
Each of these approaches has its own set of advantages and disadvantages. **The first approach** often requires no additional equipment for filtering incoming traffic, effectively blocking "wild" GTP hackers connected to a rogue provider. However, if the attacker gains GTP connection within a trusted MNO, executing attacks becomes relatively easy.

Using the second approach, mobile operators usually attempt to implement GSMA recommendations. To effectively enhance GTP security based on GSMA recommendations, the installation of specific equipment, such as a GTP firewall, is required. A well-configured and fully functional GTP firewall can effectively block any attack described in GSMA recommendations. Nevertheless, this approach comes with the challenge of integrating the firewall, as subscriber location information needs to be extracted from SS7 and Diameter protocols. Additionally, the MNO must continuously monitor and ensure that all GTP signaling traffic is properly routed to the GTP firewall.

The third approach combines the advantages of the first two, offering the highest level of security. To achieve its full potential, the operator must utilize GTP firewall solutions, which can pose challenges in terms of integration complexity. Nevertheless, once implemented successfully, this approach ensures robust protection against GTP-related threats and strengthens the network's overall security posture.

By carefully considering these approaches and their respective pros and cons, mobile operators can proactively strengthen their network security, effectively protecting against potential threats. However, we have observed that the majority of networks lack any security measures. The high level of protection in some networks is due to certain subscriber policies indirectly influencing security. This approach is not ideal as the operator does not have visibility into the security posture and lacks a clear understanding of how certain configurations impact security. To ensure robust security, mobile operators should implement comprehensive security measures and maintain a thorough understanding of their network's security landscape. This will enable them to address vulnerabilities and mitigate potential risks more effectively.

Current real security measures



Pic. 3 - Security measures implemented for GTP protection

According to our research, only 8% of networks currently implement specific security measures, particularly filtering based on roaming partner addresses. Another **15% of networks are considered to have a high-security** level due to internal node configurations that are not directly connected with security. However, a significant **77% of the networks lack any security measures altogether.** We have not come across any networks that fully implement GSMA recommendations regarding GTP security, nor have we encountered any networks using a combined security approach.

Despite the continuous efforts by GSMA and mobile operators to address GTP security since 2017, there remains a concerning lack of comprehensive security measures implemented on mobile networks. During our observation period, we were surprised to find that not a single network was protected with a GTP firewall. Even when tested mobile operators claimed to have a GTP firewall deployed, we were able to perform tests successfully, as there was no functional GTP firewall in place. This observation suggests that either the GTP firewall was not actively operational, or its filtering rules were not correctly configured or enabled.

While some mobile operators employ IP address filtering from non-roaming partners to incoming traffic, certain test attacks can still succeed. However, the deployment of a fully functional GTP firewall could significantly improve these statistics and provide more robust protection against potential threats. Adopting advanced GTP firewall solutions will undoubtedly enhance the overall security of mobile networks and protect networks against various attack vectors.

Furthermore, our observations reveal that mobile operators are not employing GTP security monitoring solutions, or at the very least, these tools are not effectively identifying unauthorized activities. Based on the information provided by the mobile operators, these communication interfaces with external networks are seemingly not supervised by a Security Operations Center or any similar system, such as intrusion detection systems (IDS). Incorporating IDS into their network security strategy would provide mobile operators with greater visibility into potential threats and enable them to take proactive security measures in response to real attacks. Implementing such monitoring solutions is crucial for maintaining a secure and resilient mobile network infrastructure.

Conclusion

The interconnected nature of mobile networks across different generations amplifies the risks posed by GTP security vulnerabilities. This study offers an overview of these challenges, illustrating the need for greater attention to network security, particularly within the context of emerging 5G technologies.

Our research underscored the pervasive and concerning lack of robust security measures across a significant proportion of examined mobile networks. Despite ongoing efforts from GSMA and individual mobile operators since 2017, we found that comprehensive security measures are, for the most part, still not in place. No network under examination was found to have a functional GTP firewall deployed, even in instances where such a firewall was claimed to exist. The absence of GTP firewalls or insufficient configuration of their filtering rules presents serious risks, opening the door for unauthorized activities and potential attacks.

Alarmingly, our findings also showed that most mobile networks are not employing crucial monitoring tools, such as GTP security monitoring solutions. The apparent absence of supervision by Security Operations Centers or equivalent entities leaves these communication interfaces dangerously exposed to potential external threats.

Given the vital role of mobile networks in today's digital society, it's imperative for the industry to prioritize the implementation of comprehensive and effective security measures. This includes the deployment of functional GTP firewalls, the application of GSMA-recommended protections, the integration of intrusion detection systems, and the regular monitoring of all network communication interfaces.

In light of our findings, we urge all stakeholders in the mobile networking industry to reassess their current security postures and to make necessary changes. Mobile network operators must not only be aware of the vulnerabilities within their networks but must also take proactive steps to identify and address potential security threats. Prioritizing security in this way will not only protect individual networks and their users but will also contribute to the overall stability and integrity of the mobile networking ecosystem.

Our research reinforces the understanding that the path to robust and effective mobile network security is not easy or straightforward. It requires sustained effort, investment, and a thorough understanding of both current and emerging threats. Yet, the importance of these efforts cannot be overstated. As mobile networks continue to evolve, and as our reliance on them grows, so too does the importance of ensuring their security. The findings of this study should serve as a wake-up call for the industry, prompting the necessary actions to secure our interconnected digital future.