Positive Technologies

Security assessment of Diameter networks

2020

positive-tech.com

Contents

Introduction 3

Materials and methods 3

Overview of Diameter threats 4

- Causes of vulnerabilities 5
- Denial of service 5
- Subscriber location disclosure 6
- Subscriber information disclosure 7
- Network information disclosure 7

What operators can do 8

Introduction

4G networks use the Diameter signaling protocol, which—just like SS7—contains security flaws. In fact, vulnerabilities in the Diameter protocol allow hackers to conduct almost the same range of attacks on subscribers and mobile operators as on previous-generation networks.

In this paper, we will discuss the current state of protection of mobile networks and implications for security of nascent 5G networks. Read on to learn what causes vulnerabilities in mobile networks and what operators can do to protect themselves.

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, leading to a wide range of threats if the operator does not take appropriate protective measures. Malicious actions are simulated using 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.

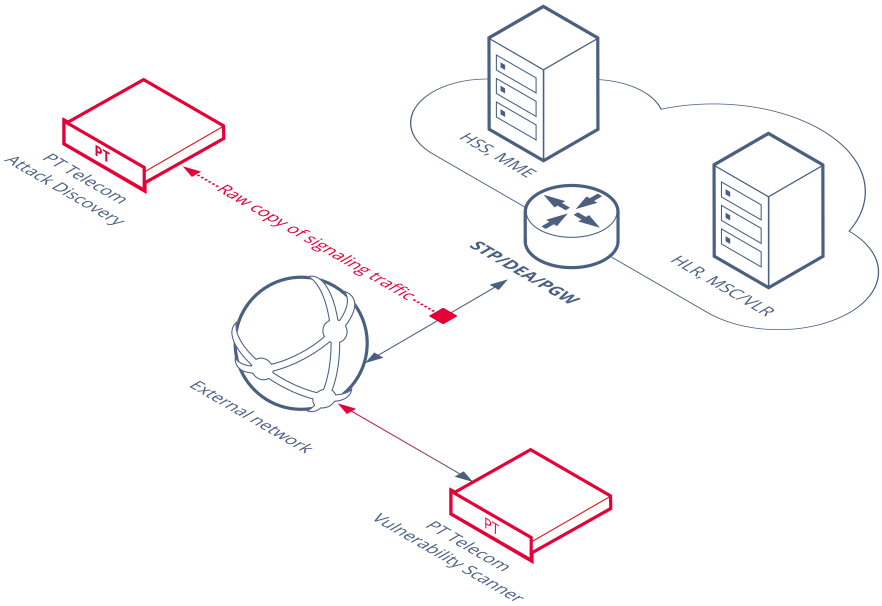
PT
PT Telecom Attack Discovery
Raw copy of signaling traffic
HSS, MME
STP/DEA/PGW
HLR, MSC/VLR
External network
PT
PT Telecom Vulnerability Scanner

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.

We will also discuss the state of security of Diameter networks. Future publications will address the security of GTP networks. For more on the biggest threats to SS7 networks today, refer to our website.

Overview of Diameter threats

The last two years have brought almost no improvement in the security of Diameter networks. The biggest threat—one we identified on all tested mobile networks—was denial of service.

It is important to remember that these threats affect users of both 4G and 5G networks. The first generation of 5G networks (5G Non-Standalone) is based on the LTE network core, which means that 5G inherits all the vulnerabilities found in LTE. Therefore, the first step to protect 5G subscribers should be to improve the security of 4G networks.

Table 1. Percentage of Diameter networks vulnerable to particular threat	**2017**	**2018**	**2019**
Subscriber information disclosure	**100%**	**100%**	**100%**
Subscriber location disclosure	**100%**	**100%**	75%
Denial of service	**100%**	**100%**	**100%**
Network information disclosure	75%	**100%**	**100%**

According to our research in 2018, one third of networks were vulnerable to fraud. Attackers can lift restrictions in order to use communication services on Diameter networks for free. In this year's report, we have omitted fraud-related statistics because almost all tested networks either did not support mechanisms that could be attacked using known methods, or else such testing was outside of testing scope. In the cases when fraud tests were conducted, attackers were indeed able to bypass operator-set restrictions and use services even when such services were not included in the subscriber's rate plan.

Operators still rely on 3G networks for SMS and voice traffic

Methods for intercepting SMS messages on Diameter networks exist but are difficult to implement in practice. First, most operators still do not transfer SMS messages via 4G. Instead, subscriber devices switch to 3G and thus become vulnerable to all the security issues of SS7. In 2019, 86 percent of SS7 networks were vulnerable to SMS interception. Second, only one out of the three existing technologies for transferring SMS messages on 4G networks uses the Diameter protocol.

4G networks use the SIP protocol for voice calls, but by and large devices still tend to switch to 3G. Voice calls could be intercepted on 58 percent of tested SS7 networks.

Causes of vulnerabilities

External security assessments revealed architectural flaws in Diameter. Networks do not check the subscriber's actual location, nor do they verify the origin network of signaling messages for a subscriber.

Operator networks can send signaling messages to their roaming subscribers (GSMA Category 2 signaling messages). If the source address and subscriber IMSI correspond to the same operator, then that network is the home network for the subscriber in question. However, the source address can be modified during transmission. Therefore, we can determine with certainty that signaling traffic is fake only when traffic is sent from an external network to the operator's own subscribers.

The failure to check the subscriber's actual location relates to GSMA Category 3 signaling messages—those sent from a roaming network to the operator's home network. Since any network in which the subscriber is roaming can send such requests to the subscriber's home network, it is impossible to determine whether the message is legitimate based on the message parameters alone. This is why operators should check whether the subscriber is truly roaming on the network in question and cross-reference new requests against previous location data.

To counter attacks that exploit these flaws, constant monitoring and thorough analysis of signaling traffic are required.

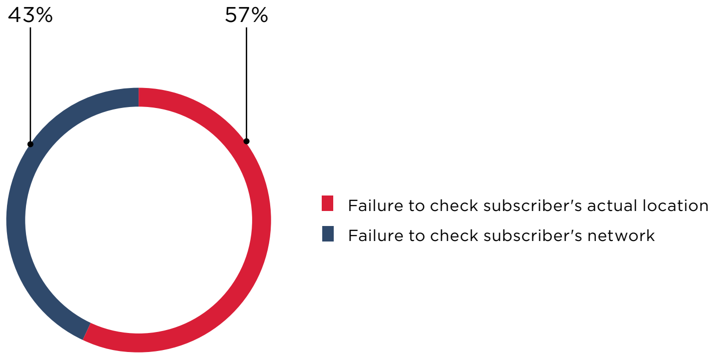

Figure 2. Vulnerabilities that enable attacks (percentage of successful attacks)

Telecom demand is increasingly driven by IoT devices, which are highly sensitive to downtime and disruptions

Denial of service

When choosing a mobile operator, subscribers think about more than just price. They associate 4G with a certain standard of high-quality service and bandwidth. Downtime may become a reason for subscriber churn. The main consumers of communication services are no longer people, but Internet of Things devices. These devices are particularly sensitive to failures in mobile networks. An alarm system that fails to activate during an emergency, industrial sensors that go offline, smart city systems that can no longer communicate—all these things have the potential for much greater consequences than an Internet slowdown for home users.

Every tested network was vulnerable to denial of service. The low success rate for attacks does not mean that operators are making an effort to protect themselves. Rather, they simply did not have such functionality present on their networks. Many pentesting methods will come up empty on networks that lack modern mechanisms such as SMS in MME and Voice over LTE (VoLTE). On networks that used VoLTE for voice calls, the testers could downgrade subscribers to 3G and degrade service. And even on the networks without such functionality, operator devices may handle incoming messages incorrectly.

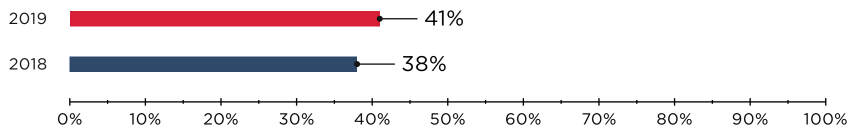

Figure 3. Percentage of successful DoS attack attempts

Test attacks caused dropped or significantly slower connections, which prevented the subscriber from using the Internet. In some cases, the subscriber device reconnected in 3G mode.

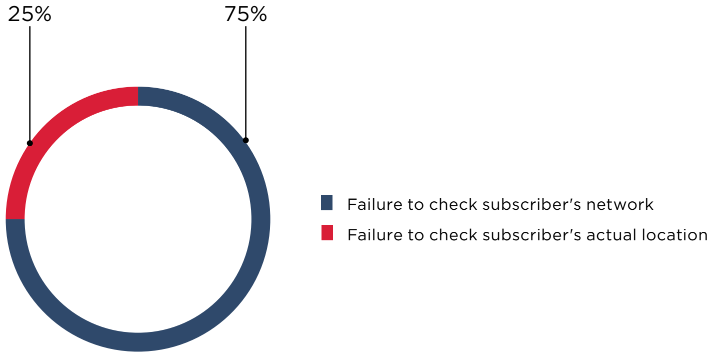

Figure 4. Vulnerabilities allowing to cause denial of service (percentage of successful attack attempts)

Subscriber location disclosure

Subscriber location could be tracked in 89 percent of cases

Subscriber location could be tracked in 89 percent of cases. The tactic was, impersonating a roaming partner, to send a signaling message requesting the location of a subscriber. Networks should return a response only if the message is addressed to a subscriber of that roaming partner. But determining this is impossible, so what an operator can do is to block messages coming from an external network to the operator's subscribers. Unfortunately, operators often fail to perform such checks. Only one network did not respond to such messages, thanks to the configuration of the eGLR (Gateway Location Register) on the network border.

Subscriber information disclosure

Attackers can make great use of information from subscriber profiles, such as phone number, mobile device status, and APN (access point) configuration. The subscriber's profile also stores billing parameters and restrictions on mobile services. This data can be modified by attackers for fraudulent purposes.

In addition, an attacker can access the subscriber's authentication keys and use them to create a base station. A fake base station allows attackers to collect subscribers' IMSIs, intercept outgoing voice calls, and conduct DoS attacks.

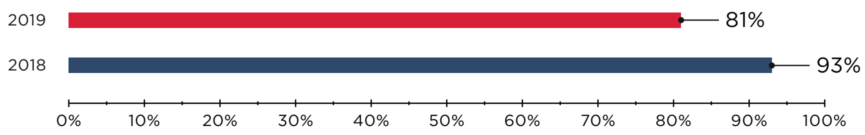

Figure 5. Percentage of attack attempts in which information was successfully obtained from subscriber profiles

In most cases, the testers successfully accessed subscriber profiles. As mentioned, this happens because operator networks neglect to consider the actual location of a subscriber when receiving signaling traffic from an external network. However, there is no other way to tell a fake message from a legitimate one. Correct filtering of incoming messages, including cross-referencing of subscriber location, could help to prevent disclosure of information about the operator's network and subscribers. This, in turn, would hinder more complex attacks.

Network information disclosure

To perform more complex attacks, attackers need information about the operator's network. To cause denial of service, for example, attackers need to know the addresses of network elements.

All the attacks attempted during external testing were successful at obtaining information about network equipment. The fake messages used in attacks are extremely difficult to distinguish from legitimate ones. Filtering such messages requires that the operator verify the subscriber's location and cross-reference each received message with the previous ones in order to determine whether the subscriber is actually on the network from which the request originated. Today, operator equipment does not allow performing such analysis of traffic.

Disclosure of information about the operator's network and subscribers is possible when operator's equipment does not cross-check subscriber locations and fails to correctly filter signaling traffic

Takeaways

The Diameter protocol has vulnerabilities allowing attackers to track subscriber location, obtain sensitive information about the operator's network and subscribers, and bypass operator restrictions on use of mobile services. Some methods allow downgrading the subscriber to insecure 3G. All the tested networks were vulnerable to denial of service, which pose a direct threat to IoT devices.

5G networks currently have the non-standalone architecture, which is based on 4G. Therefore, subscribers who count on the advantages of 5G, including improved security, are still susceptible to the threats associated with 4G networks.

What operators can do

Security must be a priority during network design

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.

Signaling traffic must be monitored and analyzed as it crosses the network border. This identifies potential threats and configuration errors. Such monitoring is encouraged by GSMA guidelines. To implement this, operators need to employ special threat detection systems that can analyze signal traffic in real time and detect illegitimate activity by external hosts. These solutions block illegitimate messages without impacting network performance or subscriber availability. They can also relay information to other protection systems for maximum effectiveness.