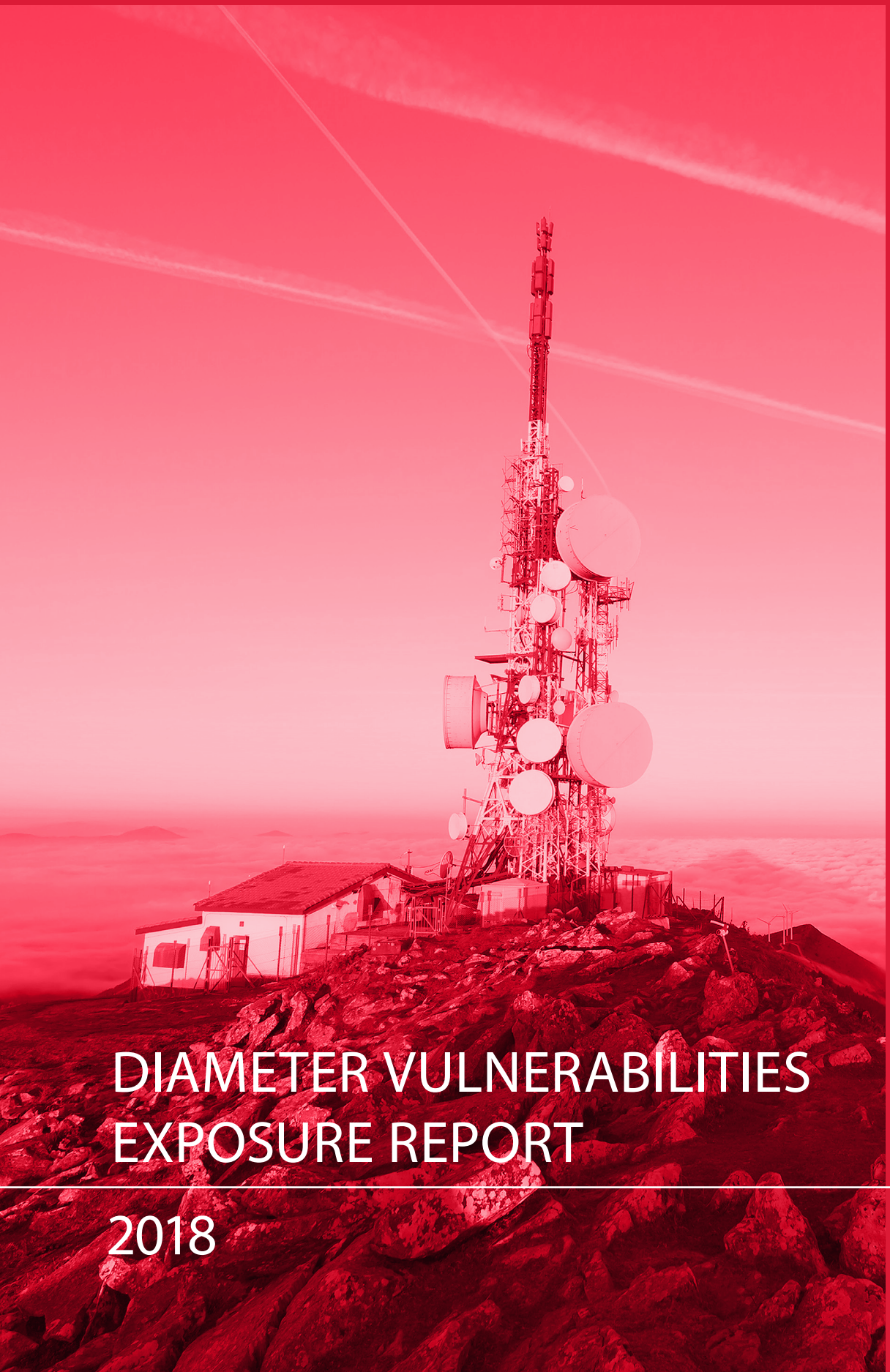
POSITIVE TECHNOLOGIES



DIAMETER VULNERABILITIES EXPOSURE REPORT

2018

CONTENTS

INTRODUCTION

New-generation 4G networks are gaining popularity everywhere, providing subscribers with high-quality service and protecting transmitted data. What is meant by data protection in telecommunications networks? What threats are concealed in everyday mobile communications, and what is the difference between 4G networks and previous network generations in terms of information security?

To transfer service data (during a voice call, for instance), 2G/3G networks used SS7, which was developed back in the days when security was not top of mind. As a result, the SS7 system is exposed to a number of vulnerabilities that we have repeatedly discussed; for example, it would be quite easy for an attacker to intercept subscriber SMS or eavesdrop on conversations.

SS7 was replaced in 4G networks by the Diameter protocol, which is used to perform most service tasks. Nevertheless, as we explained in a previous report, the Diameter protocol is by no means fully secure. Fraud, SMS interception, denial of service, and other threats are still pressing. Moreover, 4G subscribers are still largely tied to previous-generation networks, since most mobile operators currently use 4G only for Internet access, while for SMS or voice services 3G is deployed.

This study considers some practical examples of attacks that could be carried out in Diameter networks, and explores how much safer these networks are compared to SS7.

TERMS AND DEFINITIONS

Diameter is a signaling protocol used in telecommunication networks to transmit service data.

DEA (Diameter Edge Agent) typically functions on the boundary of an operator's signaling network and serves as a proxy agent for signaling traffic from other operators' networks.

DRA (Diameter Routing Agent) performs routing of Diameter traffic.

HSS (Home Subscriber Server), one of the most important elements in the infrastructure of 4G LTE networks, stores important user information and a subscriber activity history.

IMSI (International Mobile Subscriber Identity) is a unique number that identifies a mobile network subscriber worldwide.

MME (Mobility Management Entity) facilitates switching between base stations, roaming, authentication of user devices, and interaction with HSS, and is responsible for selecting the serving gateway.

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

EXECUTIVE SUMMARY

All tested networks contain critical vulnerabilities allowing intruders to track subscriber location and cause denial of service. One in three networks is at risk of fraud attacks on operators.

4G subscribers are exposed to the same threats as subscribers of previous-generation networks. Practice shows that Diameter networks are prone to attacks aiming to cause denial of service, disclose subscriber and operator information, and defraud operators. However, although the scope of attacks is limited in comparison with previous-generation networks, intruders can force a subscriber's device into 3G mode and carry out further attacks on the less secure SS7 system, including eavesdropping, SMS interception, and other actions targeted against subscribers.

To ensure network protection, an integrated approach to security is required. Most detected flaws were related not only to misconfigured or vulnerable network equipment, but also to fundamental issues in the Diameter protocol itself, requiring additional security measures. It is crucial for all security measures to be considered as a whole and to include regular analysis of network security, maintaining up-to-date security settings, continuous monitoring and analysis of signaling traffic, timely detection of illegitimate activity, and early response to emerging threats.

MATERIALS AND METHODS

To assess security of telecommunications networks, Positive Technologies experts simulate the actions of a potential attacker. PT Telecom Vulnerability Scanner is used to emulate a malicious host. The study generally assumes that the attacker is acting from a network external to the operator's, but in some cases internal attacks are also investigated. The figures below show two standard variants for connecting to the tested network.

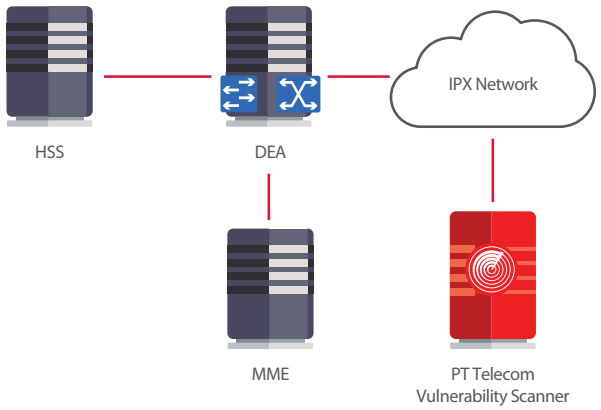


Figure 1. External connection to the tested network

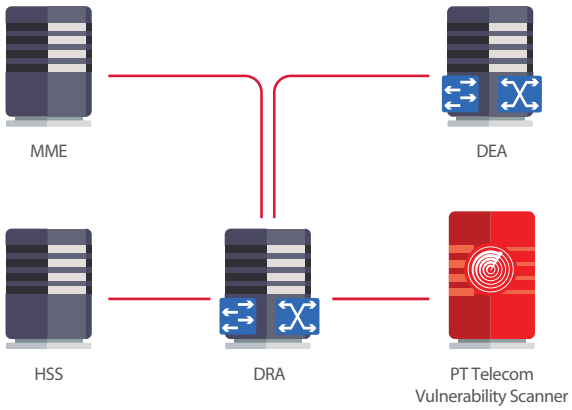


Figure 2. Internal connection to the tested network

This study presents the results of security analysis of 15 telecom operators, in which Positive Technologies employed a complete set of audit tools.

CLIENT SNAPSHOT

The research covered telecom operators from Europe and Asia. 80 percent of the participants were major telecom companies with a subscriber base of more than 40 million people.

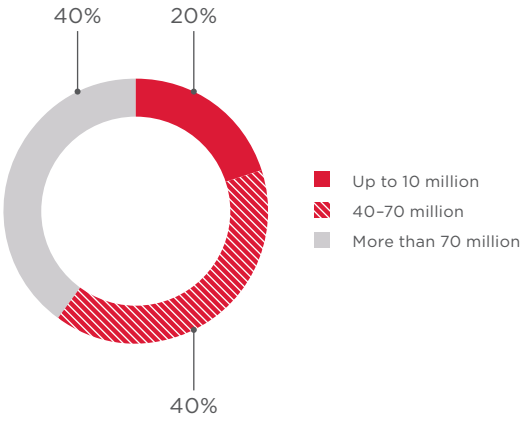


Figure 3. Operators by subscriber base size

OVERVIEW OF THREATS IN DIAMETER NETWORKS

Overall statistics

Attacks on the Diameter signaling protocol can have the following aims:

+ Subscriber information disclosure
+ Network information disclosure
+ Subscriber traffic interception
+ Fraud
+ Denial of service

We define subscriber information disclosure as attacks involving tracking subscriber location, disclosing profile details, and determining the IMSI—the subscriber's unique identifier required for further attacks. Attackers may also need information about the operator network—device addresses, network configuration.

Subscriber traffic (incoming SMS) interception in Diameter networks is theoretically possible, but difficult to implement, since SMS transmission often employs previous-generation networks or technologies that do not use the Diameter protocol. The connection for voice calls also uses other protocols.

Intruders can carry out attacks with the purpose of gaining free access to communication services, resulting in direct financial losses for the mobile operator.

Only a small number of telecom operators agree to test their equipment for denial-of-service vulnerabilities during security assessments, as this could potentially lead to downtime in the mobile network. Therefore, our report only reviews the results of tests conducted to cause denial of service for individual subscribers. It should be noted that some methods facilitate mass denial-of-service attacks, which pose the risk of serious reputational losses, since thousands of users at once can be disconnected for a long period of time (until rebooting the device or moving into the coverage area of another MME).

In 2018, we conducted a similar study of SS7 networks. Now we can compare if 4G networks employing the Diameter signaling protocol are more secure than previous-generation networks, and examine the attack success rate against networks of different generations.

Table 1. Vulnerable networks by threat type

Threat	Percentage of vulnerable networks (2017)	
	SS7 networks	Diameter networks
Subscriber information disclosure	100%	100%
Network information disclosure	63%	75%
Subscriber traffic interception	89%	– [1]
Fraud	78%	33%
Subscriber denial of service	100%	100%

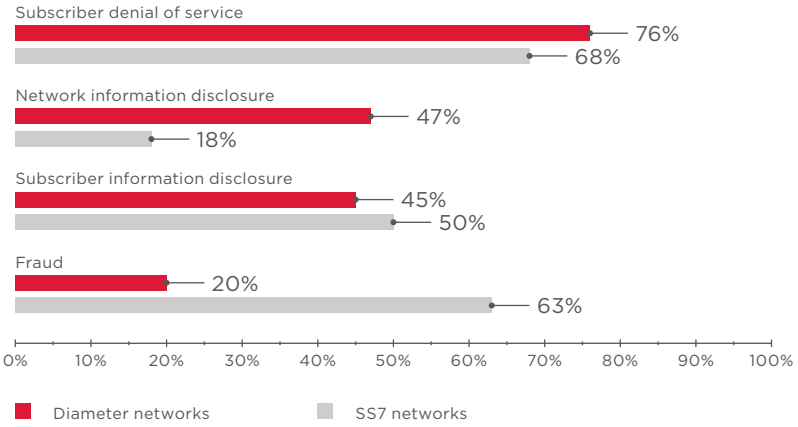


Figure 4. Successful attacks by threat types

Mobile operators lack sufficient awareness of security issues in Diameter networks

As in SS7-based networks, subscriber information disclosure and denial of service are possible in all networks that use the Diameter protocol. At the same time, the proportion of successful attacks aimed at subscriber denial of service is slightly higher. The reason may be that operators are aware of existing security problems in SS7 networks and take appropriate security measures.

75 percent of networks allowed disclosure of information about the operator network, which is somewhat worse than for networks of previous generations. This is because among Diameter signaling messages that provide data about the operator network, the share of those requiring additional checks to perform correct filtering is higher. These messages can be received from any host, and the only way to detect falsification is to match the current message with the previous one, taking into account user location and the time interval between the messages. The equipment currently found in most Diameter networks is not up to the task—it does not allow flexible configuration of filtering rules and monitoring of corresponding activity. Operators do not see these attacks, and hence do not know about the existence of security issues and the need to take protective steps.

Half as many networks were exposed to the risk of fraud. Yet this lower figure is partly because at present only a handful of attacks aimed at fraudulent operations in Diameter networks are known, while for SS7 networks many different attack variations have been studied (illegal call forwarding, exploitation of USSD queries, SMS manipulation, and subscriber profile modification).

As research shows, subscriber SMS interception is possible in 4G networks. However, all networks, for which security analysis was conducted, either had subscriber devices switched to 3G mode (where SS7 is used) during SMS transmission, which made it

1 In the tested networks, SMS transmission using the Diameter network was not carried out. To establish voice calls in 4G networks, the SIP protocol is used.

impossible to assess the security of the new technology, or used SMS transmission methods that did not allow messages to be intercepted.

In SS7 networks it was possible to intercept nine out of ten SMS messages, which means that this holds true also for the current configuration of most 4G networks under assessment. Following the introduction of IMS (and accordingly VoLTE/VoWiFi technologies), SMS transmission can be performed using SIP instead of Diameter, so attacks aimed at intercepting subscriber traffic could potentially be thwarted. During the process of establishing voice calls, subscriber devices also switch to 3G mode, and SIP is used less frequently.

Subscriber information leakage

Even in Diameter networks, subscriber privacy remains at risk. Subscriber location could be tracked in 38 percent of cases. For SS7 networks, the figure was 33 percent. The overwhelming majority of attempts to disclose subscriber profile details were also successful.

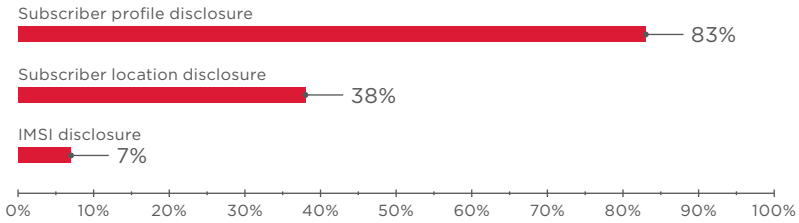


Figure 5. Subscriber information disclosure (percentage of successful attacks)

At the same time, the subscriber's IMSI was discovered in only 7 percent of cases, which is due to the safer configuration of the networks studied—interfaces not used in roaming were not accessible from an external IPX network. This indicator is extremely important in terms of security—IMSI is required for other types of attacks, so reducing the chances to disclose identifiers also hinders the implementation of other threats. Nevertheless, IMSI can be obtained by other means, for example, by exploiting vulnerabilities in the SS7 network, using fake base stations, and even through special services on the Internet.

All 4G networks allow tracking of subscriber location

In all cases, it was possible to disclose IMSI through an Sh UDR (User-Data-Request) message, which is used by the application server to request various subscriber data from the HSS. Another potential attack method, S6c SRR (Send-Routing-Info-for-SM-Request), designed to retrieve information for routing incoming messages, has yet to be successful in any tested network.

Misconfigured network equipment and in rare cases inadequate filtering of signaling messages allowed tracking of user location using the Sh UDR and S6a IDR (Insert-Subscriber-Data-Request) methods. The S6a IDR message enables the HSS to retrieve current location information from the MME. An intruder can fabricate messages, masquerading as a roaming partner's legitimate equipment.

The SLg PLR (Provide-Location-Request) message, used by the GMLC to request subscriber location information from the MME, was blocked by the operator network in each case and did not allow the required data to be retrieved.

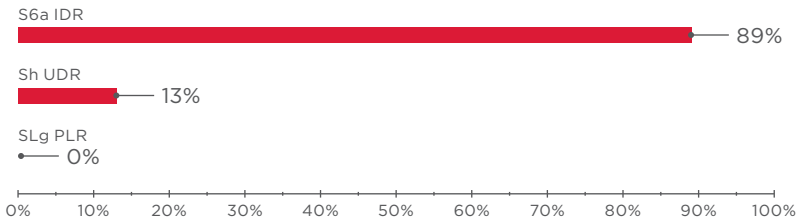


Figure 6. Disclosure of subscriber location information (percentage of successful attacks)

Subscriber profile details can be obtained using three methods: Sh UDR (already described), S6a ULR, and S6a AIR. The S6a ULR (Update-Location-Request) message contains a request to register a subscriber on a new network, but after this message is processed, subscriber profile information is additionally returned to the request source, including mobile device status, telephone number, and APN (access point) configuration. Any information obtained by attackers can be used for their own purposes. For example, phone numbers can be used to compile a subscriber base in which IMSI and mobile numbers are matched, while mobile phone status can help determine the most suitable moment to conduct a fraudulent operation in an online bank. As we shall see, the falsification of this message can have far more dangerous consequences than simple information disclosure.

S6a AIR (Authentication-Information-Request) is a message for receiving subscriber authentication keys. This message is sent by the MME in whose coverage zone the subscriber is roaming. Using data from authentication vectors, attackers can pass off a fake base station as legitimate and carry out further attacks: retrieval of subscriber information, interception of SMS and outgoing voice calls, subscriber denial of service.

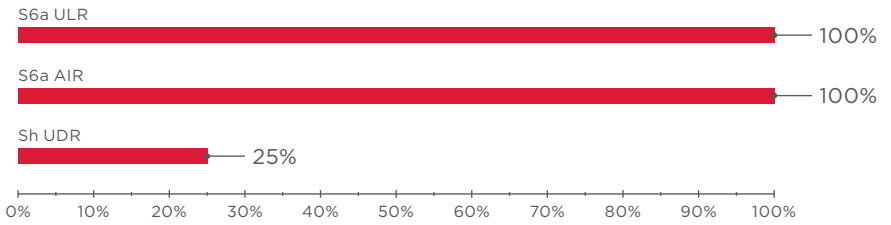


Figure 7. Subscriber profile disclosure (percentage of successful attacks)

Operator information leakage

Information about the operator network (structure, addresses, and functionality of network devices) also serves as source data for other attacks aimed at fraud, traffic interception, or denial of service for subscribers or network devices.

Since it is extremely difficult to distinguish a fake S6a AIR message from a legitimate one, the necessary information was obtained in 88 percent of cases using this method. The SLh RIR (LCS-Routing-Info-Request) method, on the other hand, did not produce the desired results—all messages were blocked because filtering was correctly configured.

Fraud

Attackers can use mobile communications for free and sell such services to third parties

Diameter networks are prone to attacks allowing the free use of communication services. There are two types of such attacks, each of which is based on modifying the subscriber profile. The first type involves modifying the billing parameters stored in the subscriber profile and is quite difficult to implement in practice, since it requires knowledge of the operator's network configuration on the part of the attacker. The values of these parameters are not standardized and depend on the specific operator; they could not be retrieved from a subscriber profile in any of the tested networks.

The second type of attack is the use of services beyond restrictions, causing direct financial damage to the operator.

Information about the subscriber profile and restrictions is transmitted to the MME using an S6a IDR message. Posing as the HSS, attackers can send a specially generated message to lift restrictions on the provision of services. As a result, the attackers have unlimited access to services not covered by their tariff plan, and will not be disconnected even if their account runs out of money and the operator disconnects them from the network. Such attacks were successful in 20 percent of cases. Services of this kind can also be sold to third parties.

Subscriber denial of service is possible in 100% of 4G networks and is critical for the Internet of Things

Subscriber denial of service

Attackers can deprive subscribers of all 4G benefits, including the high data rates and quality of service offered by telecom companies.

Slower Internet access speeds or network downtime can inconvenience the average user, but are unlikely to lead to serious consequences. The situation regarding the Internet of Things is entirely different. If the subscriber is a smart city system, a self-driving car, or industrial equipment, even a few minutes of downtime can lead to traffic chaos, shutdown of industrial processes, accidents, and even loss of life.

Subscriber denial of service can be caused by sending six types of messages:

+ S6a IDR
+ S6a DSR
+ S6a ULR
+ S6a CLR
+ S6a PUR
+ S6a NOR

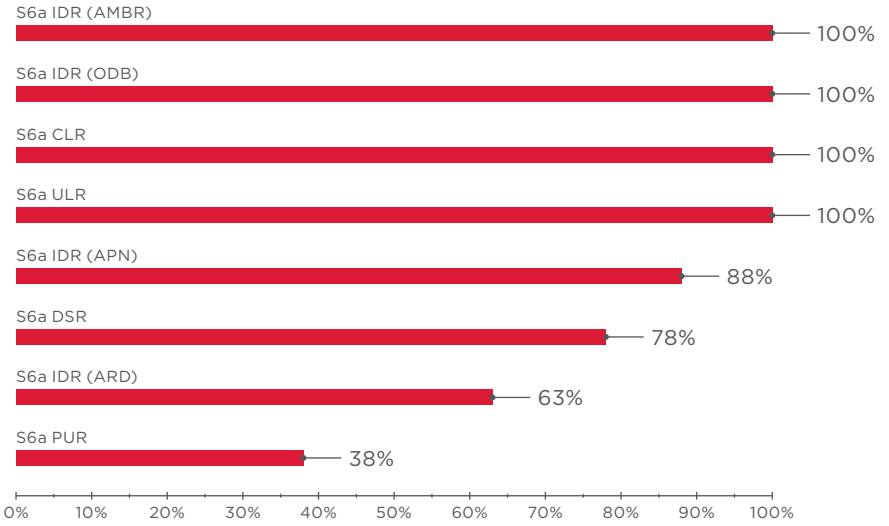


Figure 8. Percentage of successful subscriber DoS attacks

S6a IDR messages can be generated in various ways, which allows several parameters stored in the subscriber profile to be manipulated:

+ Operator-Determined-Barring (ODB) sets restrictions on the provision of communication services.
+ Access-Restriction-Data (ARD) sets restrictions on access to communication networks.
+ Max-Requested-Bandwidth-UL and Max-Requested-Bandwidth-DL (AMBR) define the maximum throughput.
+ Access Point Name (APN) is an access point that determines which network (Packet Data Network, PDN) the user transmits data through.

Changing the values of these parameters can lead to the subscriber losing Internet access (because of the connection becoming unavailable or the data transfer speed being too low) as well as 4G services (since the device switches to 3G mode). When the subscriber device switches to 3G mode, a broad range of attacks on the less secure SS7 becomes available to attackers.

An attacker can register a subscriber in a non-existent network by sending an S6a ULR message, thereby disconnecting the subscriber from the currently serving MME and depriving of all communications. The subscriber can also be cut off from the serving MME by sending an S6a CLR (Cancel-Location-Request) message, used by the HSS to inform the MME of the need to disconnect a subscriber.

Attackers can switch a subscriber device to insecure 3G mode

S6a DSR (Delete-Subscriber-Data-Request) messages are used by the HSS to delete data from the subscriber profile stored on the MME. Sending a message with a certain set of flags can lead to the complete removal of the subscriber profile and, as a result, the disconnection of the subscriber from the network.

The MME uses an S6a PUR (Purge-UE-Request) message to notify the HSS that the subscriber device is no longer served by the MME. As a result, the HSS deletes information about this MME. If an S6a PUR message is sent on behalf of the MME currently serving the subscriber, the HSS will have no information about the MME, and the subscriber will not be available for incoming calls or SMS.

The S6a NOR method facilitates attacks aimed at disabling the SMS send and receive service if SGd/GGd interfaces are used for SMS transmission on the network. However, these technologies were not used in the tested networks, so the effectiveness of this method of attack was not assessed in practice.

CAUSES OF VULNERABILITIES

The Diameter protocol has architectural flaws that cannot be offset through filtering and blocking traffic

Let's review the main differences between SS7 and Diameter and investigate why Diameter networks can be prone to the same attacks as SS7.

One of the drawbacks of SS7 is the total lack of encryption. In Diameter, encryption is, in theory, mandatory: TLS/DTLS (for TCP or SCTP, respectively) or IPsec. But in practice telecom operators almost never use encryption inside the network, and only occasionally on its boundaries. Moreover, encryption is based on the peer-to-peer principle, not end-to-end. In other words, network security is built on trust between operators and IPX providers, since there is no way to monitor if encryption was used between two hosts or even if the information was intercepted or modified.

Another deficiency is the ability to substitute the request source—in Diameter this has become even more dangerous due to the specifics of routing responses. Any request must receive a response, which always follows the same route as the request. As a result, despite substituting the source, the attacker always receives a response. This makes it easier to collect information and allows attacks to be carried out more imperceptibly.

Although many SS7 procedures in 4G networks are performed using Diameter, the rest are implemented through other protocols. For example, call setup in VoLTE uses SIP.

The 4G network is now mainly used only to provide Internet access, while voice call setup and SMS transmission are done using previous-generation networks. As a result, many actions theoretically possible in the Diameter network turn out to be impossible in practice, and the corresponding interfaces are filtered simply by virtue of the low prevalence of 4G roaming for these services.

Perhaps the most interesting example comes from SMS transmission mechanisms. In 2G and 3G networks they contain many vulnerabilities, while in 4G they are not widely used yet. Moreover, 4G networks employ three different SMS transmission techniques, only one of which makes direct use of Diameter to deliver messages.

At the transport level, the difference lies in the mandatory use of IP in Diameter networks, which can facilitate attacks due to the large number of tools available for attacking IP protocols.

Despite these differences, the security flaws identified in the tested networks are in many ways similar to the issues we noted in SS7 networks, primarily with regard to filtering of individual messages.

Filtering categories for signaling messages are defined in GSMA FS.19 Diameter Interconnect Security. The categories differ depending on the requirements specified for the list of checks.

Category 1 includes configuration of allowed interfaces and messages on DEA/DRA. Category 2 defines the configuration requirements for DEA or the signaling traffic filtering/blocking system with a view to determining the legitimacy of messages for the given IMSI from the corresponding source.

Since it is fairly straightforward to ensure the correct checks for these message categories, only 9 percent of attacks directly related to improper filtering of signaling traffic were successful.

A drawback of the Diameter architecture, which also existed in SS7, is the fundamental inability to distinguish a fake message from a legitimate one, since the procedure for exchanging certain signaling messages assumes that messages can arrive from any external host if the subscriber is roaming. Filtering category 3 should be applied to such messages. This category represents a more complex technical task that requires the use of additional security measures, such as signaling traffic filtering/blocking or attack detection systems. The operator must check that incoming messages match the subscriber tracking pattern (the subscriber's most recent recorded location and the time elapsed since the last location update).

Predictably, almost all attacks using messages to which filtering category 3 is applied (S6a ULR and S6a AIR) are successful. The lack of filtering is due to the fact that blocking legitimate messages would disrupt communication for subscribers who genuinely are roaming, and the mobile operator would lose potential profit. The financial damage can be much more significant—persistent roaming downtime could push subscribers to change operator.

Specialized systems for filtering/blocking of signaling traffic were installed in one in three tested networks, but they proved highly ineffective, and attacks were successful even with category 1 messages.

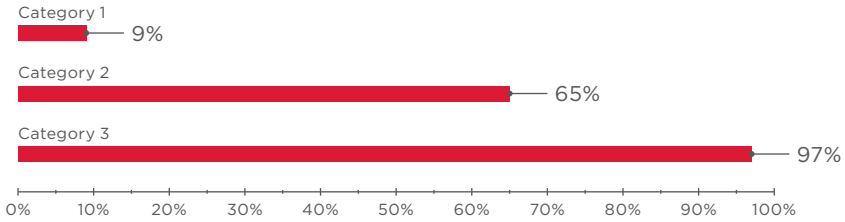


Figure 9. Percentage of successful attacks by filtering categories

The GSMA FS.19 document also describes category 0, which defines the basic traffic filtering parameters at the network level (checking addresses and message format), but we will not review this category because the corresponding tests (for equipment denial of service and correct filtering in particular cases) are rarely used in network security analysis.

Network equipment can contain many vulnerabilities leading to incorrect filtering of signaling traffic (and potentially to further attacks), and allowing DoS attacks against the operator's equipment. Security flaws due to misconfiguration of network equipment by the operator are also common. Misconfigured network equipment is responsible for a high percentage of successful attacks that filtering category 2 is intended to counter.

As we can see, the problems inherent in SS7-based networks are also relevant for the new Diameter-based generation of networks. The following diagram shows the security flaws detected and the share of attacks successfully carried out as a result of exploiting these flaws:

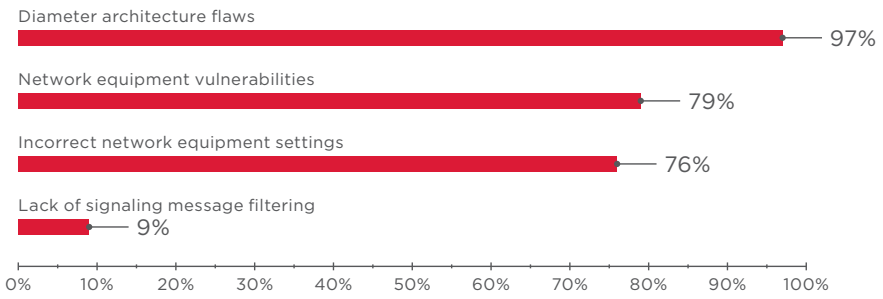


Figure 10. Network vulnerabilities and security flaws (percentage of successful attacks)

RECOMMENDATIONS FOR PROTECTION

Currently, telecom operators adopt minimal security measures in respect of Diameter signaling networks. One of the reasons may be that operators are not fully aware of existing security issues and the associated risks in next-generation networks; they are confident that the Diameter protocol is sufficiently secure against attacks in contrast to the outdated SS7. Special equipment for monitoring signaling traffic and detecting attacks is quite simply lacking in the tested networks. Taking only isolated security measures, operators do not have a full view of the situation, believing that their network is a safe environment that requires no additional costly equipment.

To protect against the attacks described in this report, an integrated security approach is required, as outlined in the GSMA recommendations in FS.19 Diameter Interconnect Security. First of all, regular analysis of mobile network security is needed to identify vulnerabilities, assess the current level of robustness and potential risks, develop security measures, and verify their effectiveness. It is important to keep security settings up-to-date and perform security assessment in the event of any changes in the network, for example, during reconfiguration or when introducing new equipment.

Furthermore, continuous monitoring and analysis of signaling messages crossing the network boundaries is necessary to ensure timely detection of illegitimate activity and response to emerging security threats at the earliest possible stage. Special attack detection systems allow analyzing signaling traffic in real time and relaying information about security incidents to additional protection systems or blocking unwanted messages without the risk of disrupting subscriber service delivery.

Security is an ongoing long-term process, not a series of one-time measures. That's why Positive Technologies takes a comprehensive approach to securing the signaling networks of its clients. Learn more by sending questions via the feedback form on our website or writing directly at info@ptsecurity.com.

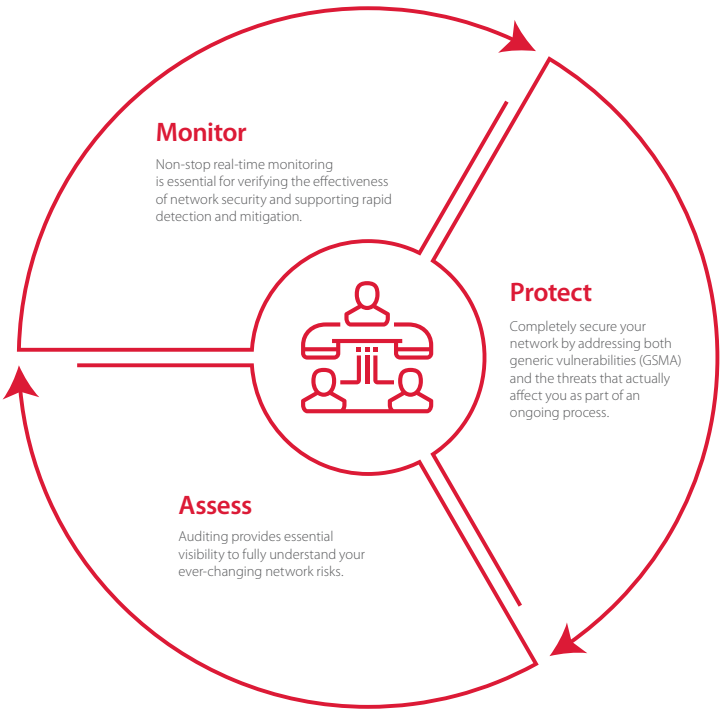


Figure 11. Recommended approach to signaling network security

CONCLUSION

Despite all protection mechanisms embedded in the Diameter protocol, attacks against both subscribers and operators are possible in the tested networks. Attackers can track subscriber location, cause denial of service, disconnecting thousands of users, or switch devices to 3G mode to exploit numerous vulnerabilities in SS7.

Thus, 4G network subscribers are exposed to the same risks as subscribers of previous-generation networks. Operators are also unprotected: attackers can gain free access to communication services, leading to major financial losses.

The vulnerabilities identified in the study are related both to flaws in the configuration of network equipment and filtering mechanisms, which can be fixed relatively easily by reconfiguration, as well as to fundamental issues with the Diameter protocol, which require special additional equipment. Moreover, operators display low awareness of existing threats, taking only minimal security measures that are insufficient to ensure safe and uninterrupted operation of the mobile network.

Positive Technologies experts conduct annual research of current threats facing modern mobile networks with the aim of highlighting security flaws and bringing them to the attention of operators. By following the above recommendations, operators can significantly improve communications security for subscribers and minimize the risks of fraud and denial of service in relation to their own resources.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com