:: Positive Technologies

SS7 network security analysis

2020

positive-tech.com

Contents

Introduction

SS7 (Signaling System No. 7) is a set of protocols governing the exchange of signaling messages. It is still actively used in 2G and 3G networks today, but was developed back in an era when only fixed-line operators had access to networks, and the stakes were much lower for questions of security.

Now, in our current environment, SS7 is no longer isolated: it can be accessed by both legitimate operators and by illegitimate attackers. Furthermore, it contains architectural flaws that make it vulnerable to a whole range of threats. These flaws can even be utilized to listen in on calls, intercept SMS messages, and instigate various forms of fraud.

While newer protocols do exist, security is only as strong as the weakest link. Attackers will be able to leverage SS7 vulnerabilities to their advantage as long as operators continue to implement the older GSM (2G) and UMTS (3G) standards.

Even LTE-only networks using the Diameter protocol instead of SS7 must interconnect with previous-generation networks. Thus, as practice has shown, even these networks are vulnerable to some attacks via SS7 networks.

We won't be seeing the end of SS7 any time soon. GSMA reports that the number of 4G and 5G users is only now beginning to surpass that of 2G and 3G users. There is no reason to expect any significant decrease in the number of 3G users until at least 2025; but even then, SS7 will continue to be a significant player, since 2G and 3G users are projected to still account for a quarter of all network subscribers (not counting IoT devices).

Materials and methods

In our security analysis of SS7, Diameter, and GTP networks, we simulated actions that would taken by a potential attacker coming from an external network. Attackers can send requests into a network, and these requests can in turn open up a wide range of threats, if the network operator does not take proper steps to ensure their security. We simulated these attacks using our PT Telecom Vulnerability Scanner system. The PT Telecom Attack Discovery (PT TAD) system was also used for security monitoring and to identify any real attacks that were actively exploiting network vulnerabilities.

The security analyses cited in this report were conducted on the networks of 28 telecom operators in Europe, Asia, Africa and South America, between 2018–2019.

The report is dedicated strictly to the current state of SS7 security. Questions regarding the security of Diameter and GTP networks will be discussed in subsequent publications.

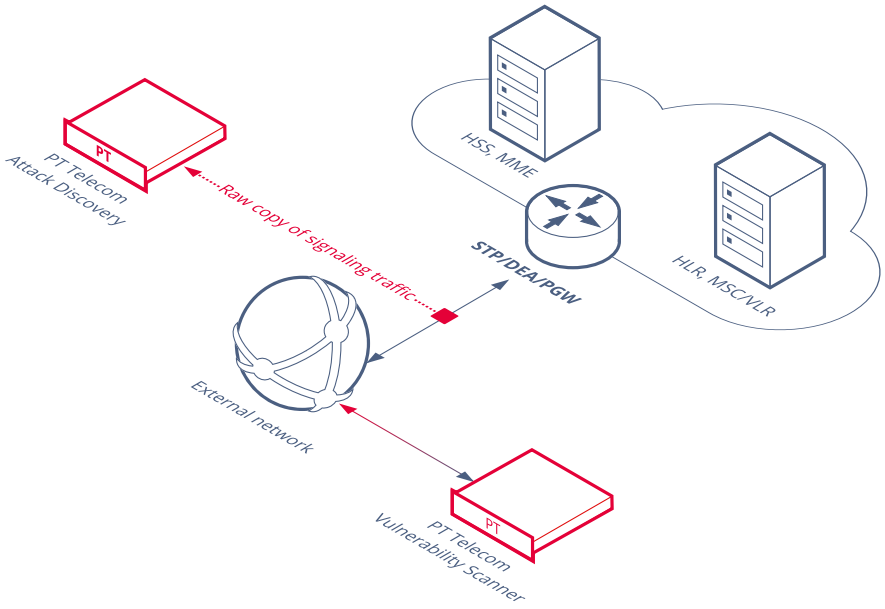


Figure 1. Security analysis visualization

Overview of threats to SS7 networks

***Security measures** are being taken sporadically, without a comprehensive understanding of the problems at hand*

In our 2018 analysis of SS7 vulnerabilities, we noted gradual security improvements in SS7 networks. Unfortunately, this positive trend has come to a halt. Operators are still taking steps to improve security, but are doing so sporadically, without a full understanding of flaws that are crippling their networks, nor of the systemic approach needed to compensate for those flaws. So long as this remains the case, there will be gaps in security that can be exploited by attackers.

Table 1. Vulnerable SS7 networks by type	**2017**	**2018**	**2019**
Subscriber information disclosure	**100%**	**100%**	**100%**
Subscriber location disclosure	75%	83%	87%
Network information disclosure	63%	68%	87%
SMS interception	89%	94%	86%
Call interception	53%	50%	58%
Fraud	78%	94%	**100%**
Subscriber DoS	**100%**	94%	93%

Leading up to 2019, the percentage of vulnerable networks increased in all threat categories. In particular, there is an increased likelihood of success for attacks aimed at committing fraud. The proportion of networks in which subscriber location can be tracked has also increased. This report will attempt to elucidate the forces behind these changes.

Why security measures don't always work

The audit is a powerful tool for operators to gain an accurate assessment of their mobile network security, and consequently of the need to invest in security improvements. Audit results can be invaluable in making decisions about the implementation of new security measures. Of the networks that we analyzed for security between 2015 and 2019, at least 41 percent currently use systems for filtering and blocking signaling traffic.

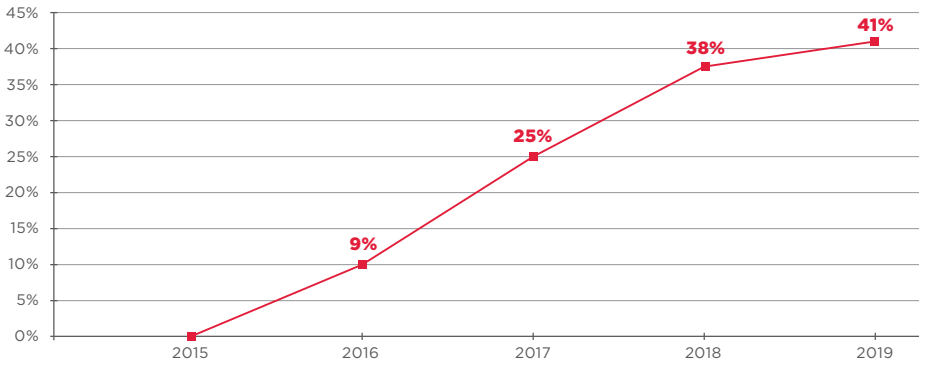


Figure 2. Networks with traffic filtering and blocking systems
(as a percentage of all networks analyzed for security from 2015–2019)

These security features, even when installed, are not always correctly configured, which creates security gaps. Thus, the increased number of successful attacks in 2019 was due to both a general lack of traffic filtering and blocking systems as well as security gaps that allowed attackers to bypass these systems. In almost half of the networks studied, configuration errors in equipment at network boundaries allowed illegitimate requests to bypass SMS Home Routing.

SMS Home Routing, which is used to guarantee proper routing of terminating SMS messages, is, strictly speaking, not a security feature. However, its use does prevent some attacks aimed at disclosing subscriber information and operator network configurations.

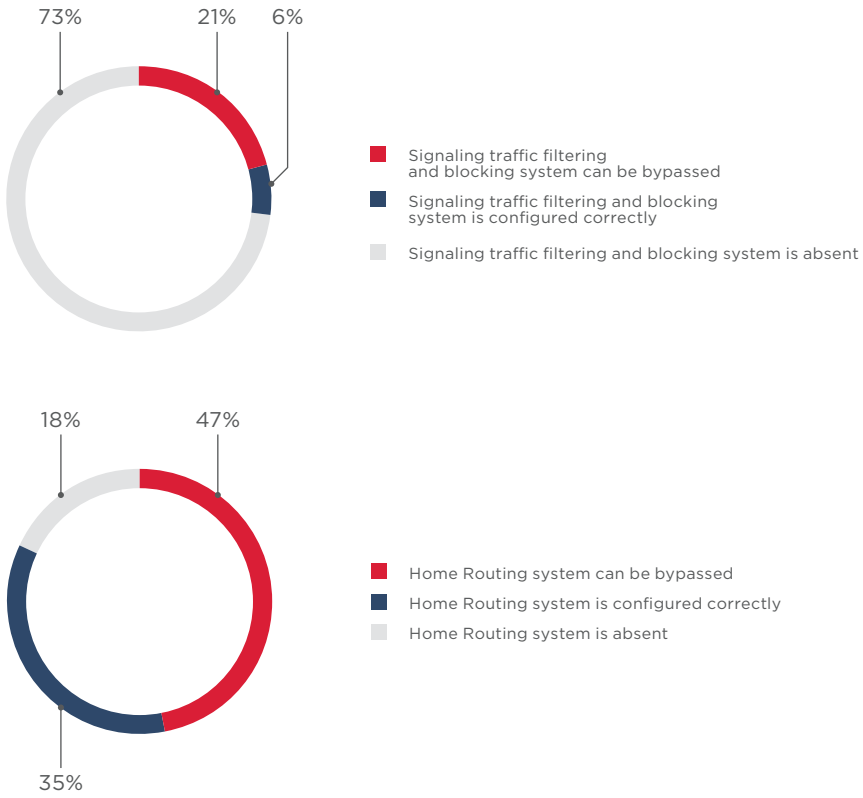


Figure 3. Bypassability of security features (percentage of analyzed networks)

Can properly configured traffic filtering and blocking systems negate all types of threats? Unfortunately, they cannot. And the guilty culprit is SS7 architectural flaws.

Fundamental configuration flaws and errors

Attacks can be carried out using standard signaling messages that are intended for rendering subscriber services. These messages can be transmitted either within one network or between networks that are owned by different operators. The messages should be filtered at network boundaries or within networks to eliminate illegitimate requests; however, the filtering is frequently ineffective, resulting in vulnerabilities. Generally, it is either errors in network equipment configuration or fundamental flaws in SS7 that are to blame. These SS7 architectural flaws can be compensated for with proper security measures, but frequently are not.

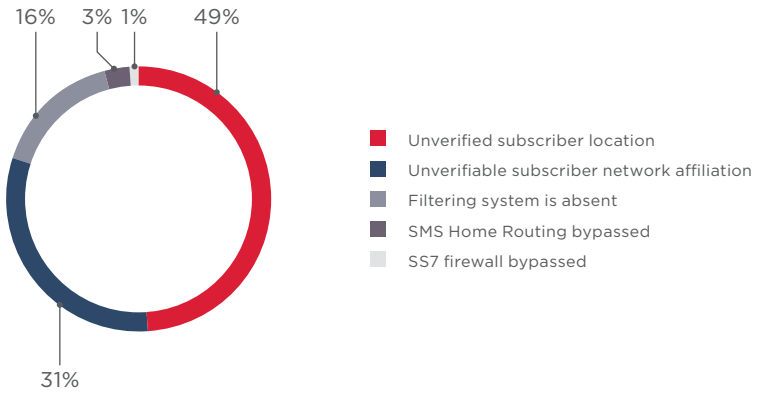


Figure 4. Vulnerabilities allowing successful attacks (as a percentage of successful attacks)

The primary culprit for network vulnerabilities is the very architecture of SS7. To describe these problems, we will have to introduce the concept of message categories. GSMA IR.82 categorizes signaling messages into three groups:

Category 1: messages transmitted between devices within one operator's network.

Category 2: messages transmitted from a subscriber's home network to a visited network.

Category 3: messages transmitted from a visited network to a subscriber's home network.

It is relatively simple to block illegitimate messages of the first category: you simply don't process any messages from external networks. When properly configured, systems for blocking and filtering signaling traffic are very effective at stopping attacks that use these types of messages. They significantly reduce disclosure risk for both subscriber information (identifiers or location) as well as for network operator information. Unfortunately, such filtering is often absent, even in specialized systems. We have encountered cases in which filtering was installed but had been deactivated after an update. The changes went unnoticed because the networks lacked configuration controls that would have brought the problem to attention.

Identifying and preventing attacks that utilize signaling messages of the second and third categories is significantly more difficult.

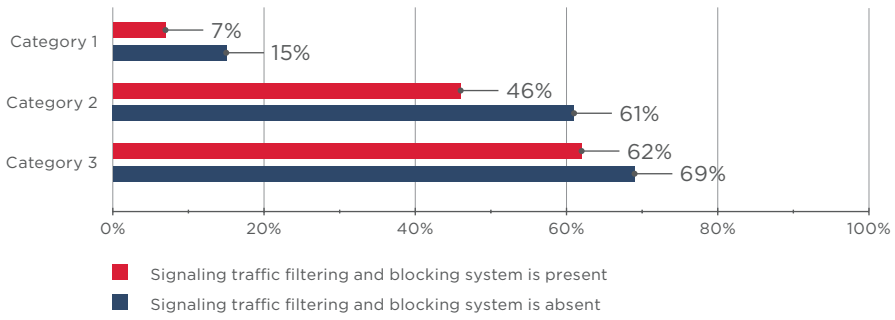


Figure 5. Percentage of successful attacks, separated by signaling message category

Attacks that use signaling messages in the second category take advantage of an SS7 architectural flaw: namely, that subscriber network affiliation is unverifiable. In these types of attacks, a network sends signaling messages to the address of a subscriber who is using roaming in a guest network. To determine whether this kind of traffic is legitimate, the subscriber's identifier must be compared with the address that the signaling message came from. If they match, then the message is legitimate. However, the source address of a message can be altered during the routing process, which means that even if the identifier and the source address do not correspond, the message isn't necessarily illegitimate. This type of signaling traffic can only be confidently marked as illegitimate when it is sent to a subscriber's address from an external network.

Illicit use of these second category signaling messages allow attackers to intercept voice calls and SMS messages, track subscriber locations, compromise the accessibility of services, and commit fraud. The fraud could also include avoiding online billing charges. Signaling traffic filtering and blocking systems mitigate the number of successful attacks, but cannot prevent them entirely.

Attacks utilizing signaling messages in the third category pose the greatest threat. These attacks take advantage of another architectural flaw in SS7: the inability to verify a subscriber's location. If an external network sends a signaling message into a subscriber's home network and the message is correctly compiled, then its authenticity cannot be determined using available information. When such a message is received, previous locational data must be referenced to confirm that the subscriber could in fact be in that visited network. The source of the request could also be run through a database that catalogues trustworthy and untrustworthy nodes as an additional check.

However, operators generally prefer not to filter these types of signaling messages at all, since there is a significant risk that such filtering could block legitimate subscribers who are using roaming. This would inconvenience subscribers, and could in turn lead to financial losses for operators. However, with the decision not to filter these terminating signaling messages, operators are making themselves and their subscribers vulnerable to fraud, denial of service, and interception of calls and terminating SMS messages. Thus, the inability to confirm a subscriber's true location is the main source of vulnerabilities that allowed for successful attacks in our security analysis.

Next, we will take a more detailed look at the risks associated with SS7 networks, and explain how the chance of a successful attack can be reduced.

Subscriber DoS

SS7 security flaws make it possible for a subscriber to be entirely stripped of service. Keep in mind that, even today, many 4G networks rely on 3G systems for transmission of calls and SMS messages. Attacks are generally carried out via requests aimed at changing settings in a subscriber's profile. For instance, toggling automatic readdressing, changing mobile device status, or changing the address of the subscriber's billing platform. As a result of these

changes, the subscriber becomes unable to receive terminating calls and SMS messages, cannot make originating calls and cannot send messages or connect to the internet. In some cases, restarting the subscriber's device is not enough to reestablish a connection—the subscriber has to actually change the network settings by hand or going to a different location in order to reconnect to another MSC.

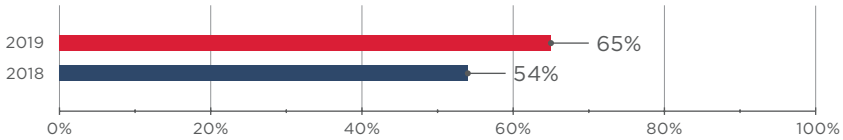


Figure 6. Percentage of DoS attacks that were successful

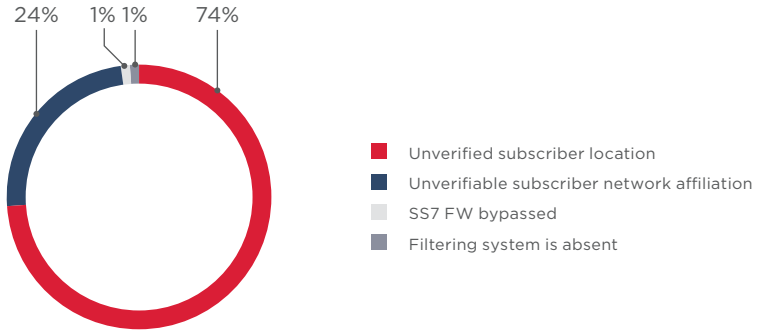


Figure 7. Vulnerabilities allowing for successful DoS attacks

Security analyses only check the possibility of DoS attacks on individual subscribers. However, if an attacker has access to an operator's IMSI subscriber database or can otherwise sort through subscriber identifiers, he could instigate a large-scale attack.

In our testing, almost half of simulated attack attempts caused DoS for subscribers. Almost three quarters of those cases were due to the inability to verify subscriber locations. In other words, filtering of individual signaling messages is no longer sufficient to substantially lower risk—DoS threats can only be effectively managed via constant monitoring of signaling traffic.

Fraud

Every network that we tested in 2019 exhibited vulnerabilities that could be exploited in financially-motivated attacks targeting both telecom providers and their clients.

Attacks that utilize falsified SMS messages can lead to direct financial losses for telecom operators. Operators establish different fees for the termination of different types of SMS messages, but an attacker might send out advertising or phishing messages via falsified terminating SMS and not pay the operator's associated fees. Operators receive a particularly large portion of revenue from terminating SMS messages sent by entities such as banks,

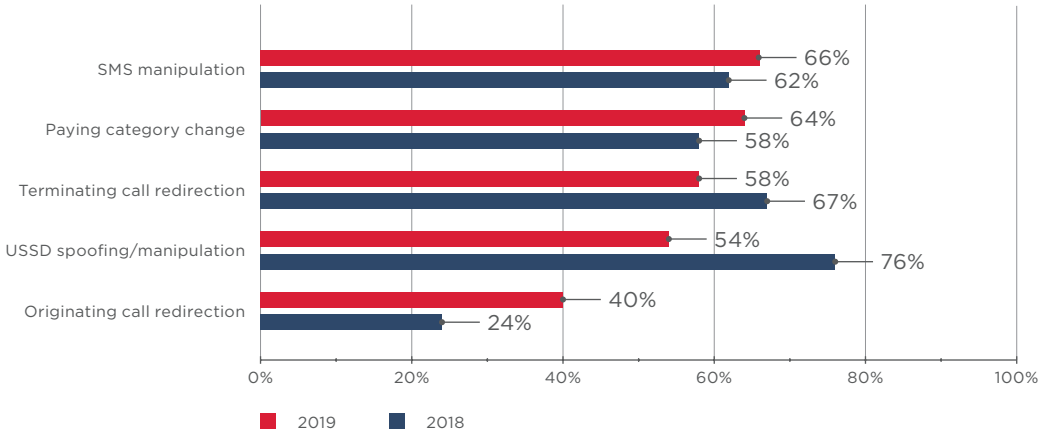


Figure 8. Percentage of successful fraud attempts

social networks, and internet services. If an attacker finds a way to distribute these types of messages at regular SMS messaging rates, a significant portion of funds will be directed to him instead of to the operator.

Changing a subscriber's payment category is a type of attack intended to bypass operators' online charging systems. O-CSI subscription settings are saved in a subscriber's profile and are used for making originating calls. Information regarding a subscriber's payment platform is among these O-CSI settings. If the address of the payment platform is changed or if a subscription is entirely deleted out of a profile, then calls will be made without contacting a legitimate payment platform. In our analysis, more than half of these attacks were successful.

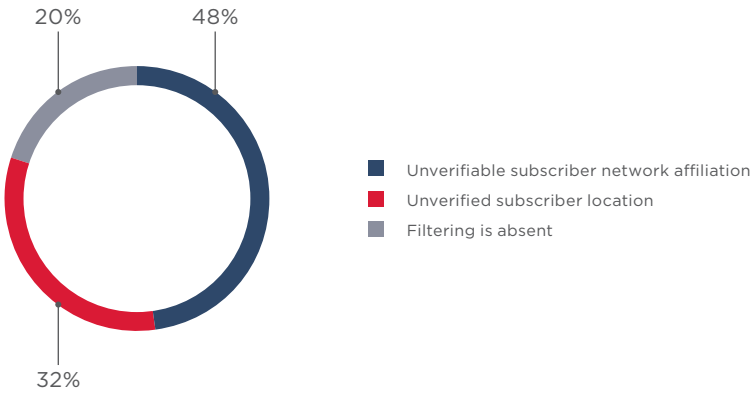
Redirecting voice calls is another type of fraud committed on mobile networks. If a subscriber is registered with a fictitious network and an altered roaming number when a call is redirected, the call will be made at the expense of the operator. However, if unconditional call forwarding is established during the course of the call, it will be paid for at the expense of the subscriber. This method can be used to forward calls to a paid number.

An attacker can also send push messages to subscribers that appear to come from a reliable service or from their operator itself via falsified USSD requests. This can be used to carry out other types of attacks.

A lack of signaling message filtering was found to be behind one in every four vulnerabilities. In some cases, filtering was absent due to incorrect configuration of specialized tools. For instance, in order to effectively prevent fraud when sending an SMS message, analysis of the message must be carried out with SMS Firewall. Knowing this, operators often don't devote sufficient attention to the filtering of other network nodes, which can play into the hands of attackers.

The remaining 76 percent of vulnerabilities were a direct result of SS7 architectural flaws. The inability to verify subscriber network affiliation leads to avoidance of online billing, fake USSD requests, and the ability to redirect originating calls. The lack of subscriber location verification allows for the possibility of fraud involving SMS and USSD requests and the ability to redirect terminating calls.

To effectively counteract fraud on mobile networks, signaling messages must undergo constant analysis and monitoring, and filtration guidelines must be correctly configured on network equipment.



Interception of SMS messages and voice calls

These types of attacks are possible due to fundamental flaws in SS7 architecture. Filtering systems, which could compensate for these flaws, are often absent.

Interception of calls and SMS messages

The interception of SMS messages is one of the greatest threats facing mobile operators today. Many services, including, for instance, mobile banking apps, send clients two-factor authentication codes via SMS. SMS messages frequently contain other types of confidential information as well. When this information is leaked, it can seriously damage an operator's reputation in the eyes of clients and lead to significant losses.

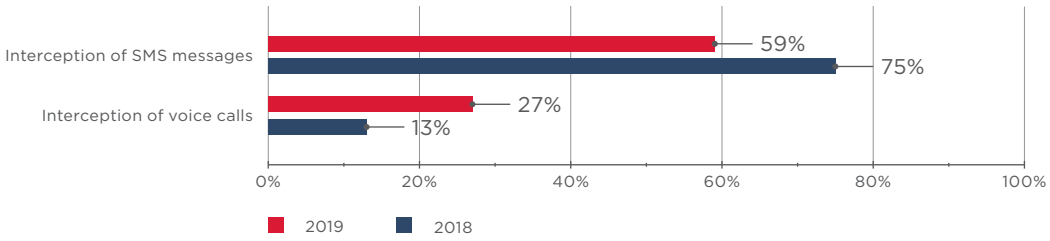


Figure 9. Percentage of successful call and SMS interception attempts

In 2018, SMS messages could be intercepted on 94 percent of networks. In 2019, the figure decreased to 86 percent. Operators are making efforts to counteract attempts at interception of subscriber traffic. They are doing this by blocking certain types of signaling messages. Although their efforts are bringing some positive results, ultimately these sporadic measures cannot provide reliable security.

Figure 10. Percentage of successful attempts at terminating and originating SMS interception

Interception of voice calls is more complex than the interception of SMS messages, as it requires a more intricate series of steps. A call must first be redirected to an attacker's network hardware before again being redirected to the subscriber's actual device. If any step in this process falls short, the attack will fail. Due to this complexity, the number of successful call interceptions is significantly lower than for SMS messages; yet even so, call interception attempts succeeded in more than half of the networks analyzed in our study.

Among all the types of attacks that we analyzed, interception of terminating calls and SMS messages is the most difficult to prevent. To counteract these attacks, signaling traffic must be constantly monitored, every message must be analyzed, subscriber location must be verified, suspicious network nodes must be identified, and list of trustworthy and untrustworthy networks must be assembled and constantly updated. In cases of originating call and SMS interception, proper filtering and blocking of requests from external networks can significantly decrease risk.

Subscriber location disclosure

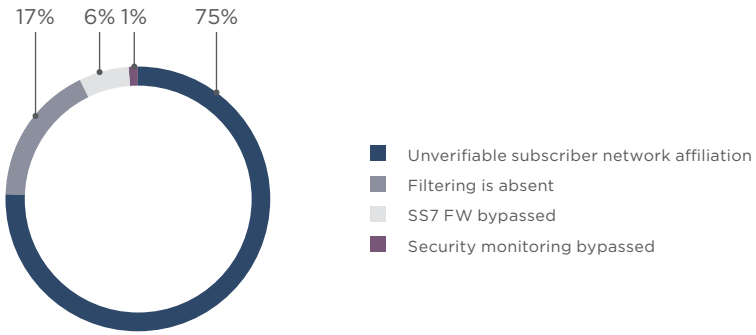


Figure 11. Vulnerabilities allowing a subscriber's location to be monitored (percentage of successful attacks)

In the past two years, the number of networks in which an attacker can track a subscriber's location has grown. Tracking can be carried out via simple requests for a subscriber's current location. It can also be accomplished by tracking a subscriber's originating calls. Since 2018, we have been investigating this vulnerability. Attackers can make changes in a subscriber's profile that allow them to receive information about the subscriber's location every time that subscriber makes a call.

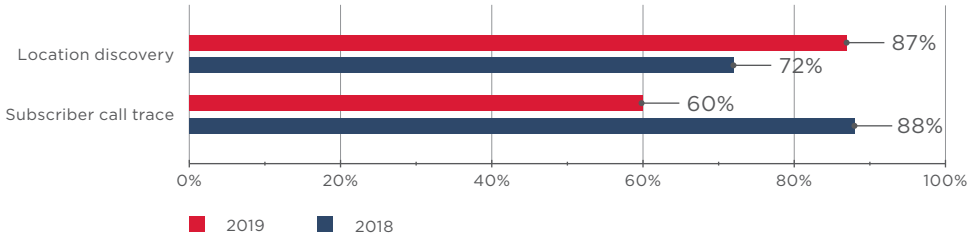


Figure 12. Percentage of successful attacks aimed at disclosing a subscriber's location

The ability for attackers to track a subscriber's location is directly related to a fundamental flaw in SS7 architecture. Namely, that in certain cases it is impossible to establish whether a subscriber is affiliated with the network from which a signaling message originated. To prevent attacks, it is essential that filtering is correctly configured on end-user equipment and at network boundaries. In addition, signaling messages must be constantly monitored and analyzed.

Subscriber information disclosure

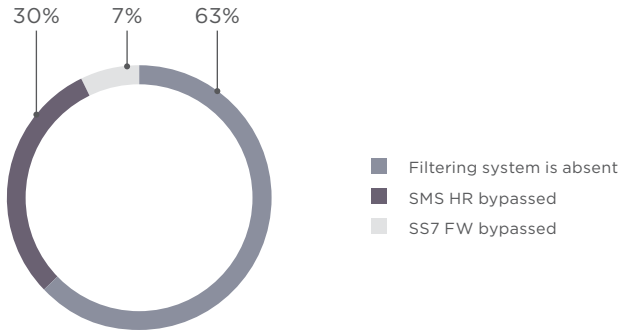


Figure 13. Vulnerabilities exposing IMSIs (percentage of successful attacks)

Generally, an attacker must know a subscriber's IMSI (International mobile subscriber identity) as well as network equipment addresses in order to carry out an attack. Almost all of the networks we analyzed (93 percent in 2019) are vulnerable to subscriber IMSI disclosure. However, operators are well-informed about this problem and are taking protective measures to prevent the disclosure of this information. Most methods used to disclose IMSIs require signaling messages that should not ever come from external networks, so it is not particularly difficult to block attacks. Thus, the proportion of successful attacks is low. That being said, an absence of signaling traffic filtering or errors that allow filtering and SMS Home Routing to be bypassed allowed our simulated attackers to obtain subscriber identifiers, just as in the case of network operator information disclosure.

All mobile networks allow attackers to access details about subscriber profiles, leading to a consistently high proportion of successful attacks. This phenomenon is easy to explain, as constant monitoring of signaling traffic and analysis of subscriber movement is needed to prevent such attacks.

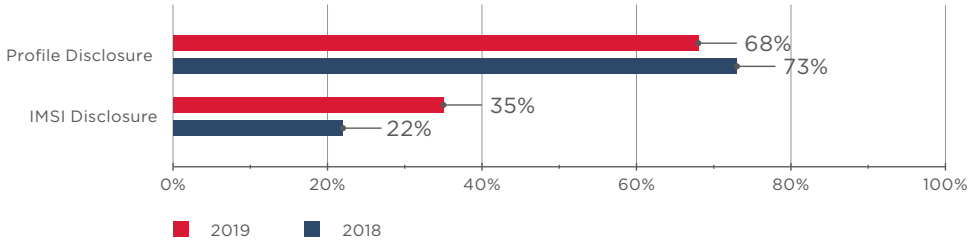


Figure 14. Percentage of successful attacks aimed at disclosure of subscriber information

Network information disclosure

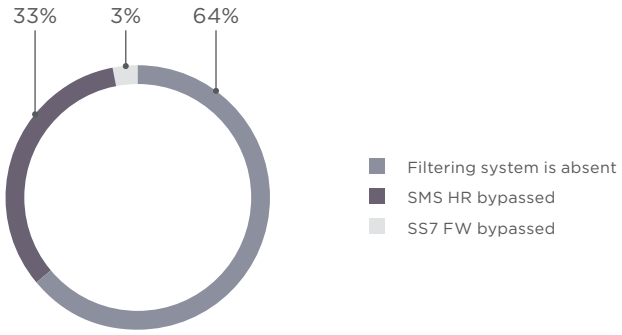


Figure 15. Vulnerabilities allowing network information disclosure (percentage of successful attacks)

Information about network configuration is necessary for most attacks, which motivates attackers to seek out the addresses and functional roles of network equipment.

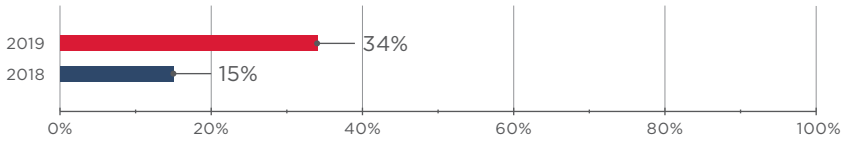


Figure 16. Percentage of successful attacks aimed at network information disclosure

In our study, the majority of successful attacks utilized the absence of signaling traffic filtering or bypassability of SMS Home Routing. In isolated cases, attackers also succeeded in bypassing the filtering of specialized security features.

Conclusions

SS7 vulnerabilities allow for all kinds of attacks, including information disclosure, interception of SMS messages and calls, and subscriber DoS. These vulnerabilities have already been leveraged to criminally obtain access to bank accounts of network subscribers. Large numbers of current 2G and 3G network users mean that SS7 will still remain a relevant part of the telecom ecosystem for years to come. This is even more definite considering that some 4G features are also still dependent on 2G/3G systems, including sending SMS message and establishing call connections.

Network operators are already aware of these threats, but many do not understand how to properly prevent them. In our study, we observed a low standard of security even in cases where expensive solutions had been implemented to filter signaling traffic. This speaks to the fact that a systemic approach to security has not been taken.

Security recommendations

Proper network security is impossible without an understanding both of relevant security threats and of the systemic approach needed to resolve them.

First and foremost, it is essential that operators adhere to GSMA security recommendations. According to ENISA, only 30 percent of EU telecom operators have implemented these recommendations. In developing countries, that figure is less than 0.5 percent.

To properly avert these threats, signaling traffic that crosses network boundaries must be constantly monitored and analyzed. In this way potential threats and configuration errors can be identified. Implementation of monitoring systems is also included in GSMA recommendations. This type of monitoring and analysis requires specialized threat identification systems that can analyze signaling traffic in real time and identify suspicious activity from external nodes. These solutions block illegitimate messages without otherwise affecting network functionality and without any risk of disconnecting legitimate subscribers. They can also interface with other security measures, increasing their overall effectiveness.