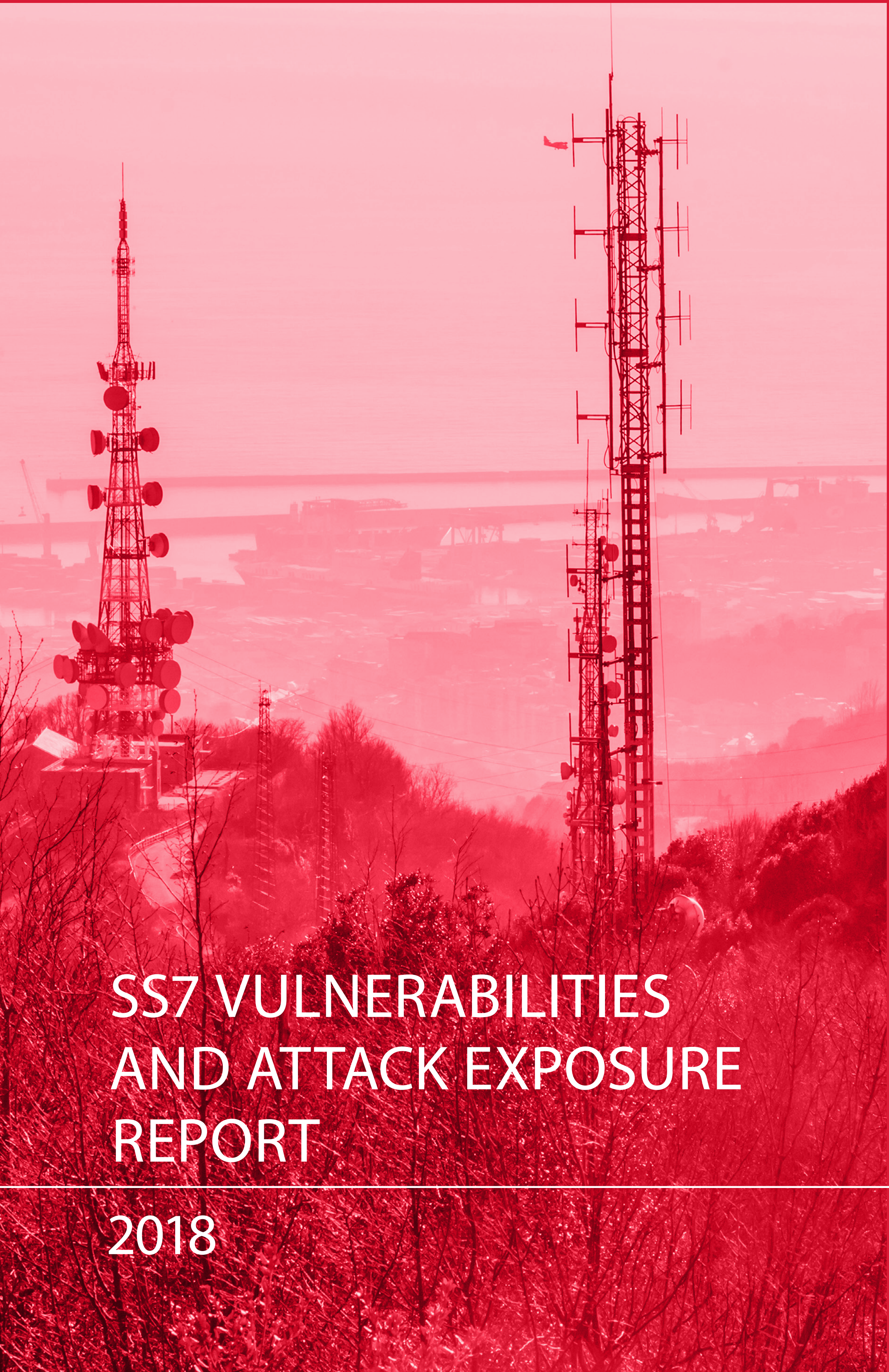
POSITIVE TECHNOLOGIES



SS7 VULNERABILITIES AND ATTACK EXPOSURE REPORT

2018

CONTENTS

INTRODUCTION

These days it is hard to imagine life without telecommunications. Anyone who uses e-banking, online payment, online shopping, e-government are long used to one-time passwords for transaction confirmation. The security of this authentication method is based merely on restricting access to telecommunication networks.

While the internet of things is spreading widely into industrial processes and city infrastructure, failures in the mobile network can paralyze them, causing not only occasional interruptions in smart home or car devices, which dissatisfy the operator's customers, but also more critical consequences, such as traffic collapses or power outages.

This report reveals the results of SS7 security analysis. Signaling System 7 (SS7) is used for exchanging data between network devices in telecommunications networks. While this standard was being developed, only fixed-line operators had access to the SS7 network, so its security was not first on the priority list. Today the signaling network is not isolated, and this allows an intruder to exploit its flaws and intercept calls and SMSs, bypass billing, steal money from mobile accounts, or affect mobile network operability.

Although new 4G networks use another signaling system, Diameter, SS7 security issues have not been forgotten, because mobile operators should ensure 2G and 3G support and interaction between networks of different generations. Moreover, research shows that Diameter is prone to the same threats. This protocol's vulnerabilities along with possible cross-protocol attacks that use Diameter and SS7 flaws will be outlined in the next report.

To demonstrate the extend of security problems in modern communication networks, this report shows not only the vulnerabilities that we revealed during SS7 networks security analysis, but also the exploitation of these vulnerabilities as would happen in real life. We have been monitoring SS7 security over the past three years and learned what protection methods are used by telecom operators and whether they are effective in real conditions.

TERMS AND DEFINITIONS

HLR (Home Location Register) is a database storing all information about subscribers in the home network.

MSC is a mobile switching center.

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

STP (Signaling Transfer Point) is a host that routes signaling messages.

VLR (Visitor Location Register) is a database that contains information about all subscribers located within its area (home subscribers and roamers), including subscriber location data.

SUMMARY

All networks contain critical vulnerabilities

All analyzed networks contain critical vulnerabilities that lead to subscriber services disruption. It was possible to intercept a subscriber's conversation or text message in almost every network; 78 percent of networks were prone to fraud.

Intruders know about vulnerabilities

PT Telecom Attack Discovery detects real attacks on operator networks. These attacks are mostly aimed at gathering information about subscribers and network configuration. However, there are attacks that are likely used for fraud, traffic interception, and subscriber availability disruption.

Operators are aware of the risks

Operators take measures to reduce the risk of threat exploitation. They succeed in reducing subscriber and network data leakage. In 2017, all analyzed networks used SMS Home Routing, and every third network had signaling traffic filtering and blocking enabled.

Existing solutions are not sufficient

Despite additional protection measures, all the networks were prone to vulnerabilities caused by occasional incorrect setup of equipment or faults in SS7 network architecture that cannot be eliminated using existing tools. Only a comprehensive approach that combines security analysis, network setup maintenance, regular monitoring of signaling traffic, and timely detection of illegitimate activities can ensure a higher level of protection against criminals.

If you have any questions, do not hesitate to contact us directly. We would be glad to assist you: info@ptsecurity.com

VULNERABILITIES IN SS7 NETWORKS

Materials and methods

Every year, Positive Technologies experts analyze the security of SS7 signaling networks. During analysis, they simulate the actions of a potential intruder supposedly attacking from a foreign or home network. The intruder can send application layer protocol requests that lead to the realization of different threats against the operator and its subscribers if the operator does not take adequate protection measures. For malware host emulation, PT Telecom Vulnerability Scanner is used.

We selected 24 most informative projects in 2016 and 2017, during which maximum security tests were performed. A comparative study includes data obtained during an analysis we performed in 2015.

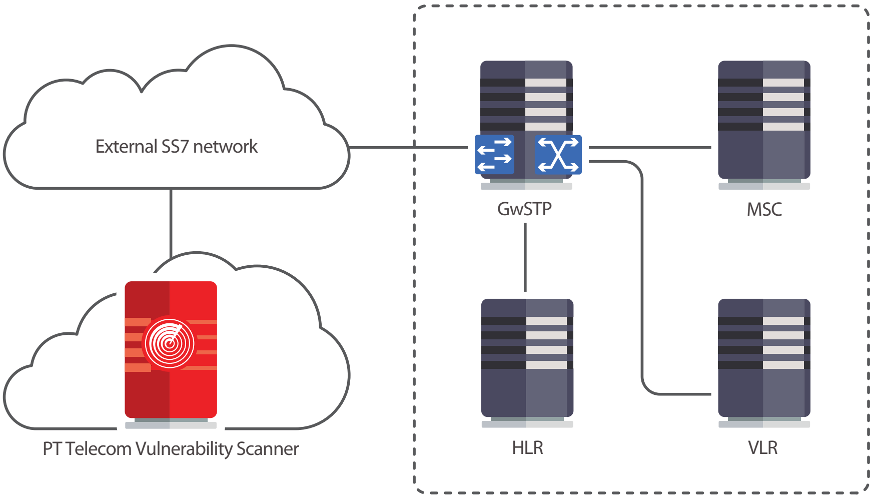


Figure 1. Workflow: SS7 networks security analysis

Participant portrait

Mobile operators from Europe and the Middle East took part in the 2016–2017 research.

Half of the operators had a subscriber base of more than 40 million. Most small companies (no more than 10 million customers) were mobile virtual network operators based on larger telecommunications corporations.

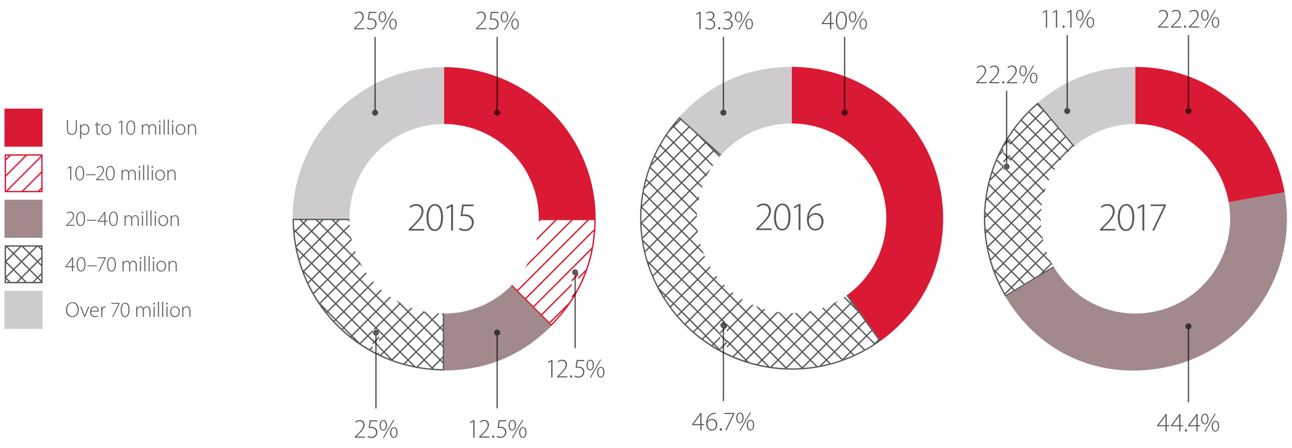


Figure 2. Operators by subscriber base size

Statistics on basic threats

We highlight the following threats that can be posed by attackers exploiting security flaws in mobile networks:

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

Each listed threat represents reputational and financial risks for the operator. Fraud, traffic interception, and denial of service affect subscribers directly and may lead to significant financial losses, privacy violation, and availability disruption.

Subscriber information disclosure means leakage of IMSI, disclosure of location or other data, such as account balance or profile details. Network information disclosure is fraught with leakage of SS7 network configuration data.

Certain methods of subscriber traffic interception allow an intruder to tap or redirect terminating and originating calls and intercept user SMS messages.

Fraud attacks can be performed against both operators and subscribers. For example, if an intruder changes a payment plan for roamers or bypasses the billing system, it will cause damage to the operator. While transferring money from a subscriber's account and redirecting calls to premium rate numbers or upgrading to a paid subscription will most certainly harm subscribers.

In our research, we consider a denial of service against individual subscribers only, because few operators would allow testing of network elements that lead to mobile network malfunctioning. Malfunction can spread if intruders have a subscriber base or the resources to bruteforce IMSIs.

The level of awareness of operators about SS7 security is growing, which is why they have started to implement protection techniques. In 2015, each network was prone to every type of threat. But in the last two years, positive trends have been seen in network security.

Mobile operators now take SS7 security issues more seriously and implement protection techniques

Table 1. Vulnerable networks by threat type

	2015	2016	2017
Subscriber information disclosure	100%	100%	100%
Network information disclosure	100%	92%	63%
Subscriber traffic interception	100%	100%	89%
Fraud	100%	85%	78%
Subscriber denial of service	100%	100%	100%

The risk of network information leakage, fraud, and subscriber traffic interception has dropped. However, each network was still prone to vulnerabilities that allow access to information about subscribers or denial of service.

Below are successful attack attempts performed by our specialists during security analysis.

As seen from the figure, operators prioritize measures that decrease the risk of network and subscriber information disclosure, because these data are the basis for a number of further attacks. As compared to 2015, the number of successful attacks aimed at network information disclosure decreased almost threefold. As for subscriber data, successful attacks halved. Actually, it is not that hard to defend against such attacks, and the information security market offers ready-made protection solutions. Still, 100 percent of networks are vulnerable to them, which points to the inefficiency of current solutions.

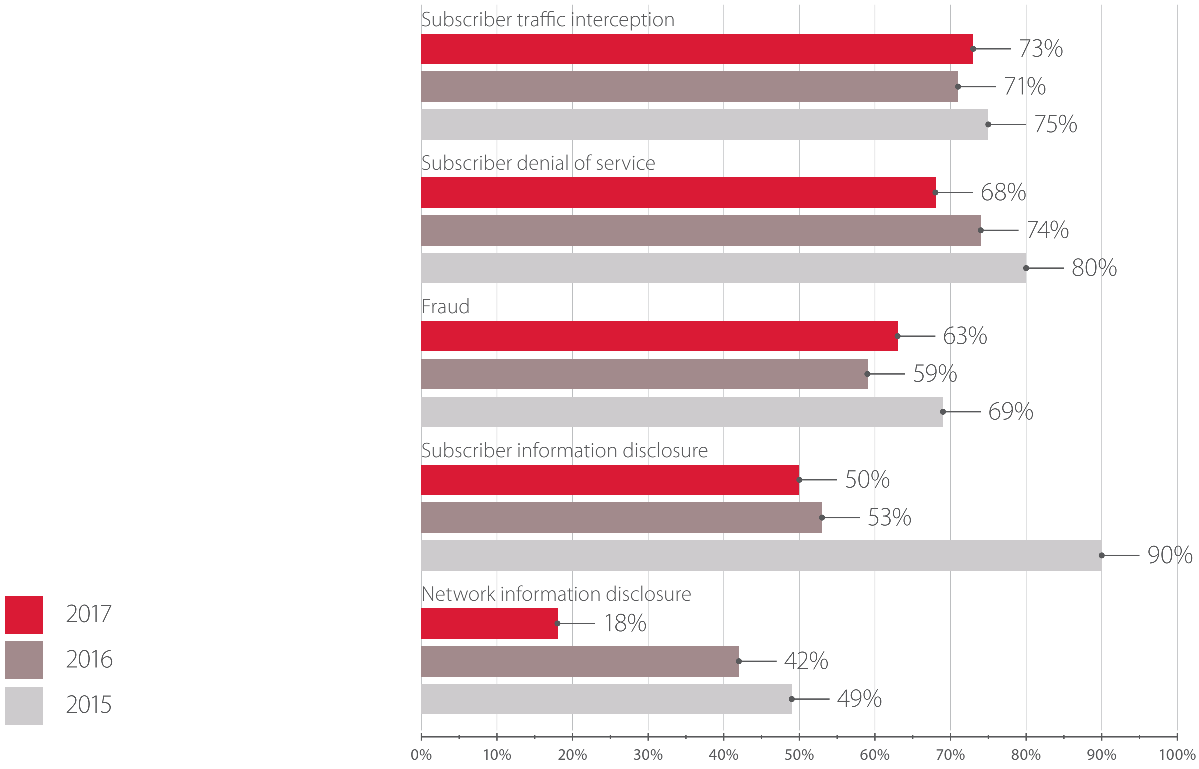


Figure 3. Successful attacks by threat types

SS7 architecture problems cannot be solved by current traffic filtering tools

The number of successful attacks using other types of threats are changed insignificantly. The reason is that implementation of traffic filtering and blocking systems cannot compensate for SS7 architecture flaws. To minimize them, another approach is required.

The following flaws allow various attacks:

- Lack of subscriber actual location check
- Inability to verify a subscriber's belonging to the network
- SMS Home Routing configuration flaws
- Lack of message filtering

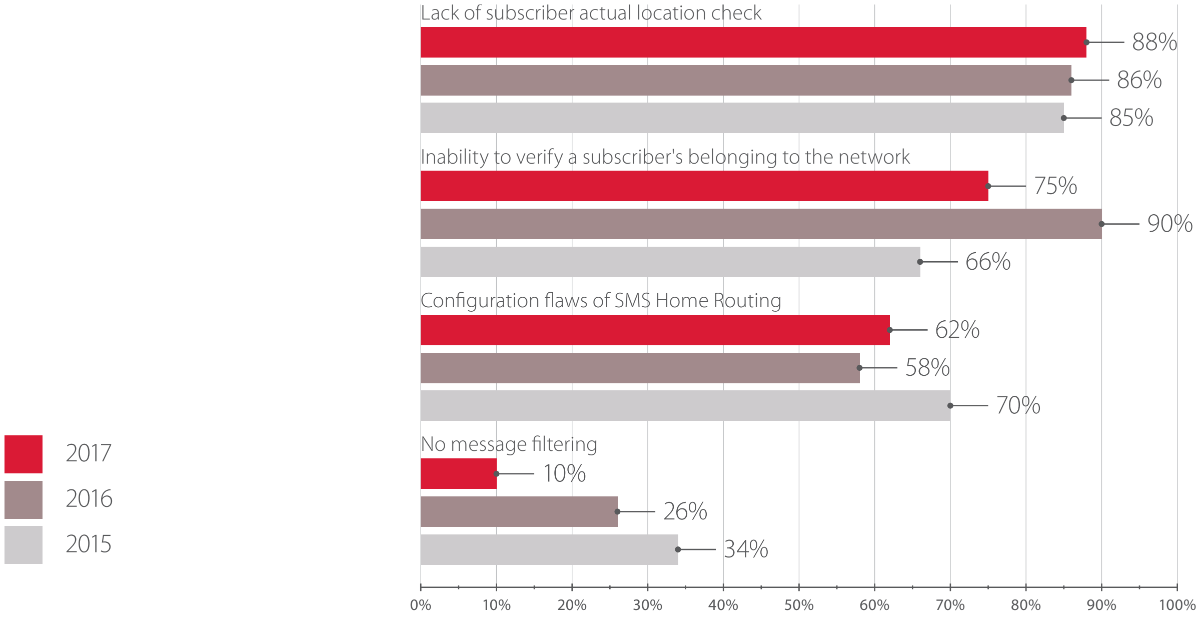


Figure 4. Vulnerabilities (successful attacks)

According to the results, most attacks can be conducted by exploiting the lack of such checks as a subscriber's actual location and a subscriber's belonging to the operator network. Among the possible attacks are ones aimed at subscriber location disclosure, call interception or redirection, SMS interception, subscriber profile or payment plan altering. Lack of a location check is related to signaling messages sent from a visited network where a roaming subscriber is registered to the subscriber's home network. If the signaling message is correct, it cannot be verified by using received parameters only. It is necessary to perform an additional check on whether the subscriber is located in the network from which the signaling traffic originated.

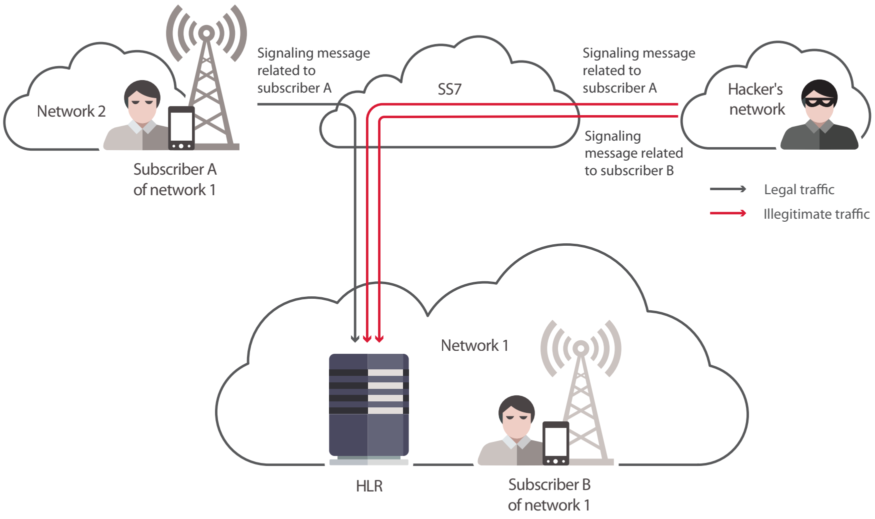
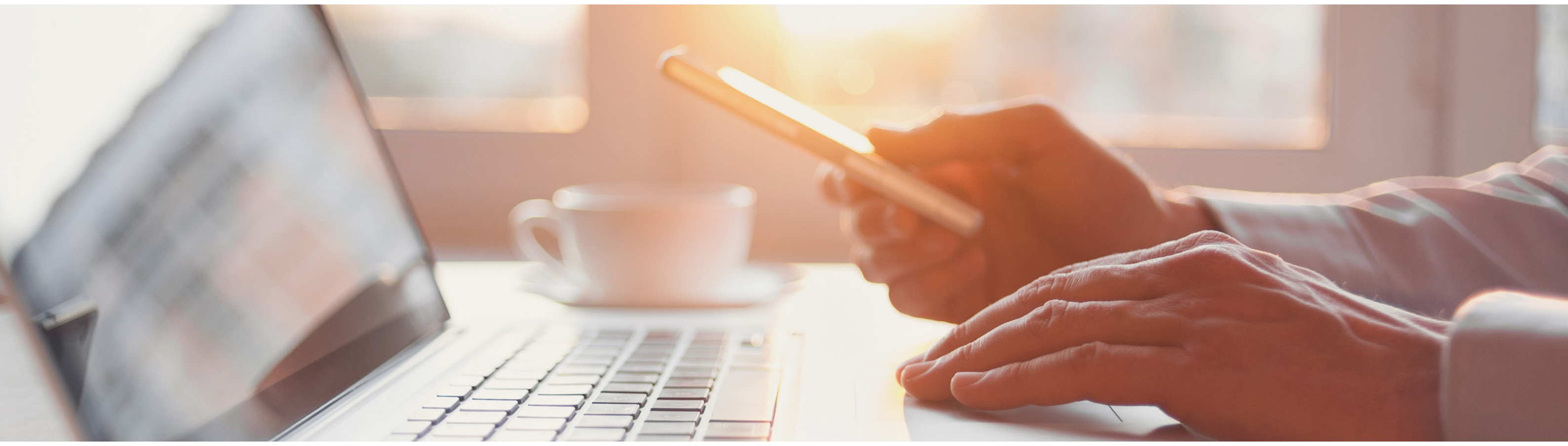


Figure 5. A subscriber's actual location is not checked

Inability to verify a subscriber's belonging to the network is related to signaling messages that are sent from the operator and directed at roaming subscribers to another network where those subscribers are registered at that particular moment. To detect illegitimate traffic it is necessary to check whether the message source corresponds with the subscriber's IMSI. If the source address and IMSI correspond to one operator, the message is valid. However, if there is no correspondence, it does not mean the message is fake (for example, a transit operator can alter the address). Signaling traffic is most likely illegitimate if it goes from external networks and it is related to subscribers of the home network.

SMS Home Routing is a hardware and software package that conceals real IMSIs and equipment addresses. It is used in 85 percent of analyzed networks, but in case of incorrect network element configuration it was possible to bypass protection mechanisms. Without SMS Home Routing, all attempts to get IMSIs and network data were successful.



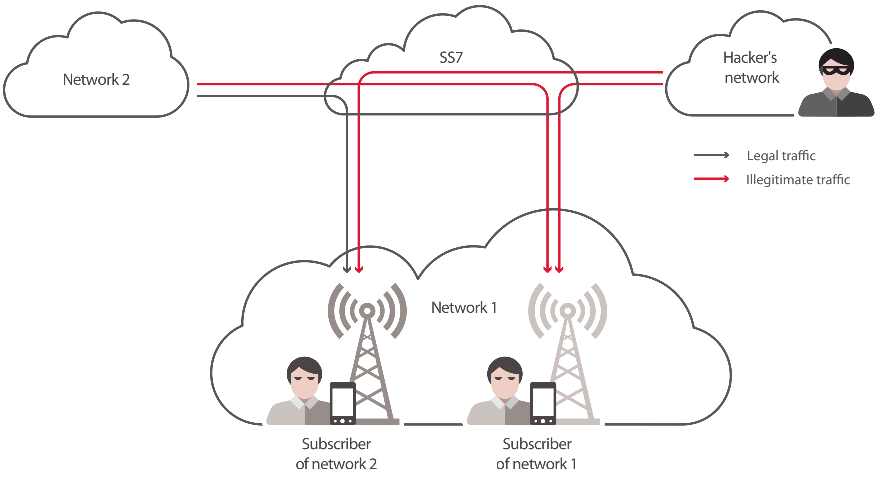


Figure 6. A subscriber's belonging to the network is not checked

Operators take active measures to implement signaling traffic filtering and blocking systems: it has already been implemented implemented in one third of the networks in 2017. As a result, attacks related to the lack of message filtering are now successful in only 10 percent of cases: that's three times better than in the previous years.

To conduct an attack, standard service messages are used. These messages should be checked at the network border or in the operator's network in order to block illegitimate requests. One and the same attack can be conducted by using several different messages (methods), the efficiency of which may vary. We will take a closer look at methods that attackers use to implement the listed threats.

Subscriber information disclosure

As it was mentioned above, the first step in reducing the possibility of attacks is to minimize the risk of IMSI disclosure. The number of successful attempts to obtain IMSI decreased fourfold in 2017 (as compared to 2015).

In 75 percent of networks, it is possible to discover a subscriber's location. The share of successful attacks using different methods is 33 percent, which is also better than in previous years.

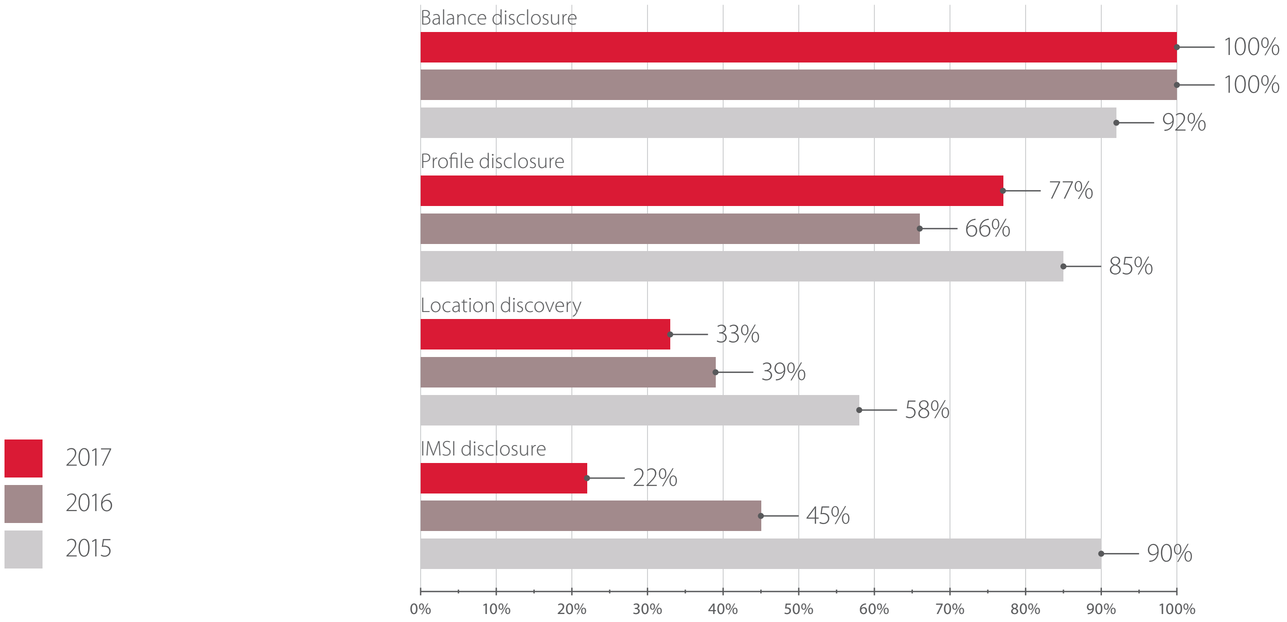


Figure 7. Percentage of successful attacks by type of threat related to obtaining subscriber data

There are four methods that allow disclosure of IMSI; successful attempts are shown in Figure 8.

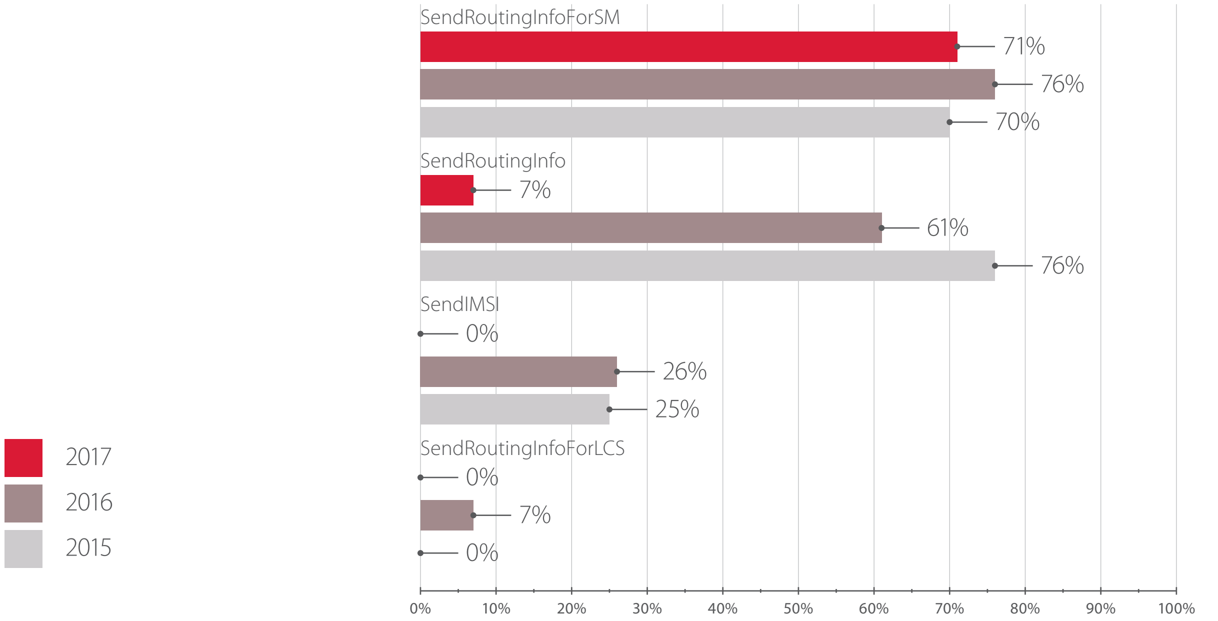


Figure 8. Methods for obtaining a subscriber's IMSI (percentage of successful attacks)

The number of successful attacks by SendRoutingInfo and SendIMSI decreased due to the implementation of filtering tools. The message SendRoutingInfo is used to obtain routing information about a subscriber during an incoming voice call and must be transmitted only within the operator's home network. Today, the message SendIMSI is not used to implement mobile services; however, the message is processed in mobile communication networks as it is required by certain standards.

SendRoutingInfoForLCS was successfully exploited in two networks only due to the efficiency of message filtering. The method is used by services that need subscriber location data.

The message SendRoutingInfoForSM is sent to obtain routing information that is required to deliver an incoming SMS message. In order not to disclose actual IMSIs and addresses of network elements, a message from the external network should be forwarded to SMS Home Routing and return virtual data. Although most networks use SMS Home Routing, incorrect configuration of boundary network equipment (STP/FW) is not uncommon. As a result the request is sent to HLR and bypasses SMS Router and returns actual IMSIs and network configuration data.

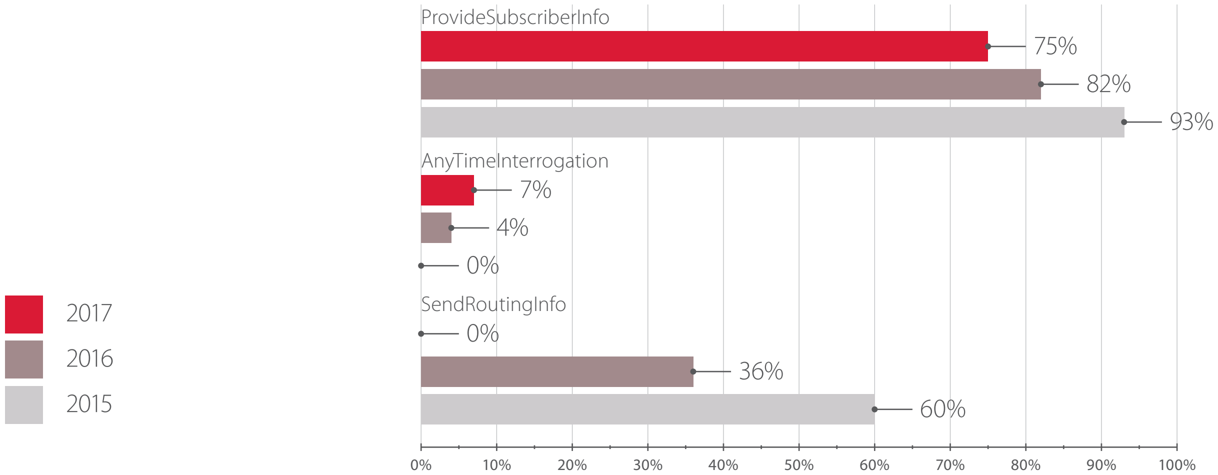


Figure 9. Location tracking methods (percentage of successful attacks)

ProvideSubscriberInfo was used to determine subscriber location due to SS7 architecture flaws. The message ProvideSubscriberInfo should be processed only in case the message source and IMSI corresponds to the same operator. But due to SS7 architectural features, it is not possible to determine a subscriber's belonging to the network without additional tools. To protect against such attacks, traffic filtering systems are required.

In 2015, we assumed that operators are well aware of attacks that use AnyTimeInterrogation allowing disclosure of a subscriber's location using the phone number, and about protection methods, as none of our attempts was successful. However, in the next two years we detected networks without filtering for this message.

Balance or profile disclosure does not pose an immediate serious threat, so protection of these data is not of high priority. Moreover, only constant monitoring and filtering of signaling traffic helps to protect against most attack methods. Each analyzed network allowed attacks to be conducted by using the following methods:

- RestoreData
- InterrogateSS
- ProcessUnstructuredSS
- UpdateLocation
- AnyTimeSubscriptionInterrogation

During security analysis performed in 2017, all these methods (except AnyTimeSubscriptionInterrogation) led to successful attacks.

Operator information leakage

During analysis, more than half of the attacks related to SMS Home Routing configuration flaws (which allow retrieval of network configuration data) were successful. However, operators significantly reduced the possibility of disclosure of such information.

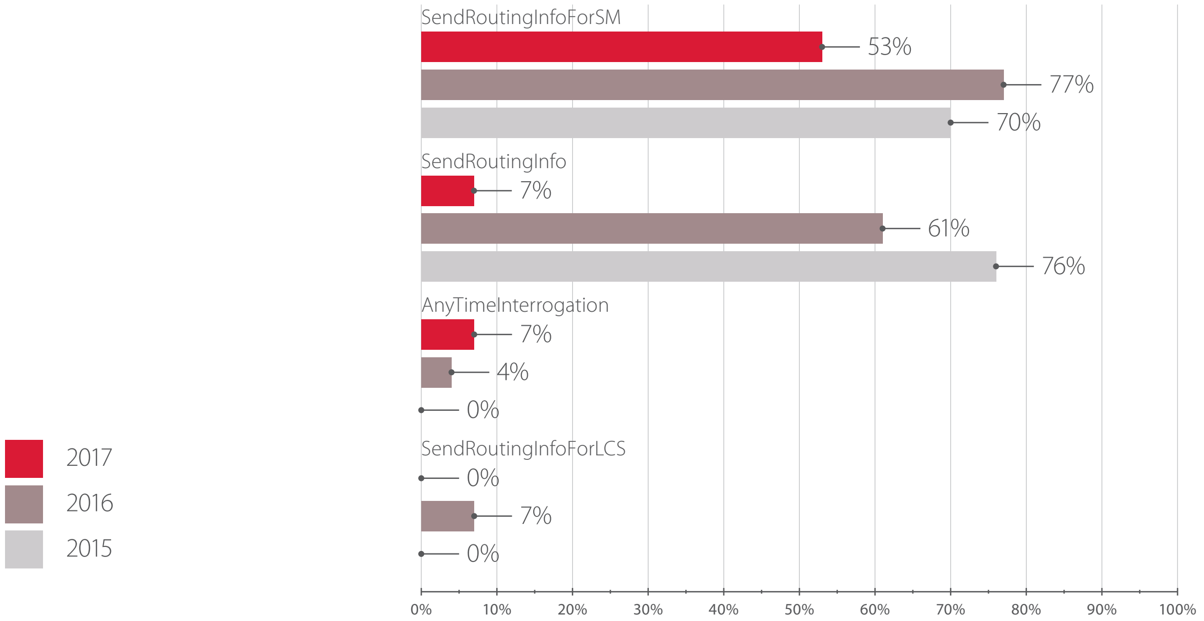


Figure 10. Methods for obtaining SS7 configuration data (percentage of successful attacks)

The number of successful attacks using SendRoutingInfoForSM in 2016 increased because we analyzed several networks without SMS Home Routing.

Nine out of ten SMS messages can be intercepted

Subscriber traffic interception

The risk of subscriber traffic interception is still high. The vast majority of attempts to intercept subscriber SMSs was successful. Today, extremely important data are transmitted via SMS messages: passwords for two-factor authentication sent by e-banking and internet payment systems. Leakage of such information affects the operator's reputation, and might result in contract termination by customers, including companies with a large volume of traffic.

Attempts to tap or redirect terminating and originating calls were successful in more than half of all cases.

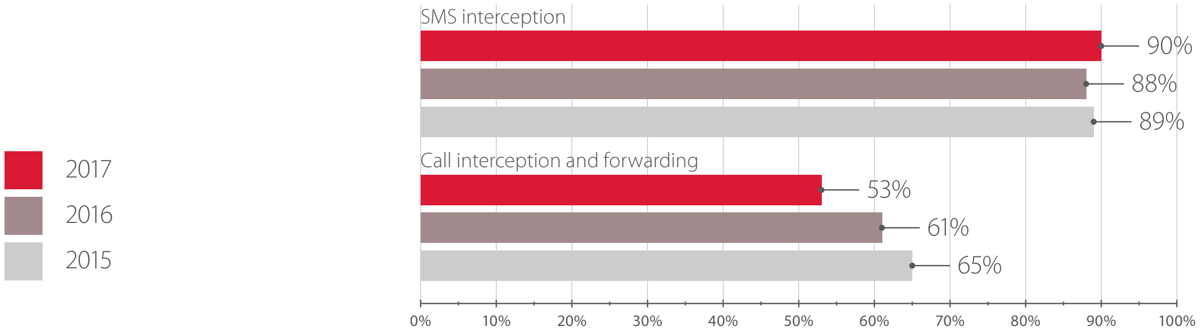


Figure 11. Methods for intercepting and forwarding subscriber traffic (percentage of successful attacks)

Redirection means transferring a call to a third-party number. Further development of this attack establishes a connection so that an attacker could tap a subscriber's conversation.

The message UpdateLocation is used to inform the HLR about a change a mobile switch. Terminating SMSs or calls are intercepted by sending a fake request to register a subscriber in an intruder's network. When a terminating call is received, the operator's network sends a request to a fake network to obtain the subscriber's roaming number. An attacker can send the number of his or her telephone exchange in response, and the incoming traffic will be transmitted to the attacker's equipment. After sending another request to register the subscriber in the real network, the attacker can redirect the call to the subscriber's number. As a result, the conversation will pass through the equipment controlled by the attacker. The same principle is used for interception of terminating calls via RegisterSS, but in this case terminating calls are unconditionally redirected to the intruder's telephone exchange.

The percentage of successful attacks is high due to the lack of a subscriber actual location check. To reduce the possibility of attacks using these methods, continuous monitoring of signaling traffic and illegitimate activity is required to identify suspicious hosts, build lists of trusted networks, and immediately block requests from banned sources.

Originating calls are tapped by using a similar pattern: the message InsertSubscriberData replaces the address of the billing platform in the subscriber's profile stored in the VLR database. When a request is sent to the changed address, the attacker first redirects the originating call to his or her equipment, and then redirects it to the called subscriber. So the attacker can tap any conversation of the subscriber.

78 percent of networks
are vulnerable to fraud

Fraud

There is a wide range of methods that can be used by criminals to gain financial benefit from the operator or subscribers. These methods can be divided into four categories:

- Illegitimate redirection of terminating or originating calls
- USSD request manipulation
- SMS message manipulation
- Subscriber profile changing

Illegitimate redirection of terminating or originating calls

An attacker can redirect voice calls of subscribers to premium-rate numbers or to a third-party number. The call will be paid by the subscriber in case of establishing unconditional redirection, or by the operator in case the subscriber is registered in a fake network and his or her roaming number is spoofed.

Call redirection also helps to implement other fraudulent schemes. For example, if a subscriber makes a call to a bank, an intruder can redirect it to his or her own number impersonating a bank employee, and thus obtain confidential information, such as passport data and a codeword. Another method is redirecting terminating calls and impersonating a subscriber to confirm banking transactions.

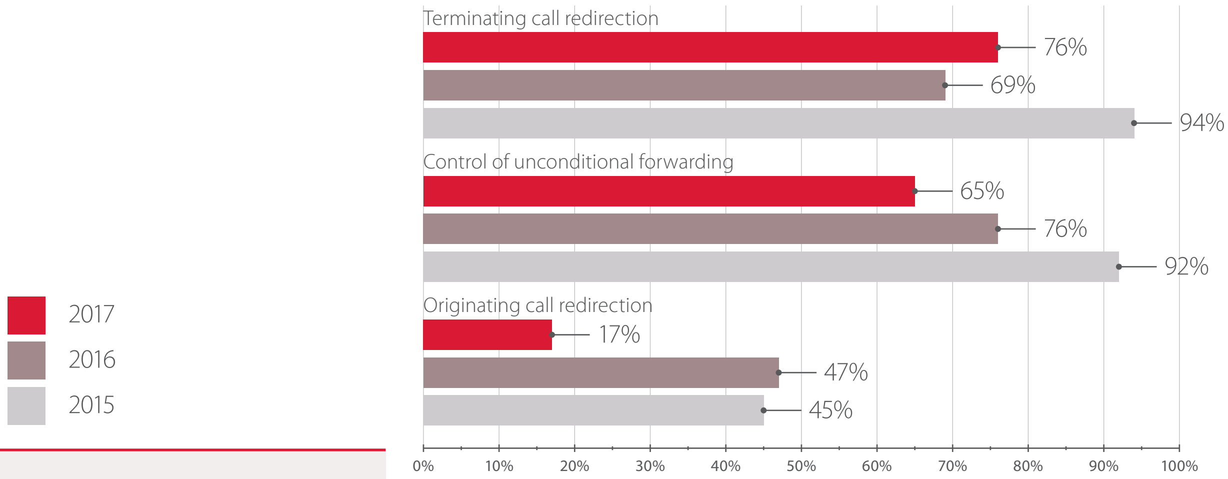


Figure 12. Forwarding a subscriber's voice calls (percentage of successful attacks)

Attacker can obtain passport data and a codeword impersonating a bank employee

Calls are redirected by using UpdateLocation, RegisterSS, InsertSubscriberData listed above, as well as by using AnyTimeModification that allows making changes to a subscriber's profile (note that no attack attempt using the AnyTimeModification was successful).

USSD request manipulation

An attacker can transfer money from the account of a subscriber or an operator's partners by sending fake USSD requests using the ProcessUnstructuredSSRequest method. UnstructedSSNotify is used to send notifications to subscribers from various services and the operator. An attacker can send a fake notification on behalf of a trusted service containing instructions for the subscriber: send an SMS message to a paid number to subscribe to a service, call a fake bank number because of suspicious transactions, or follow a link to update an application.

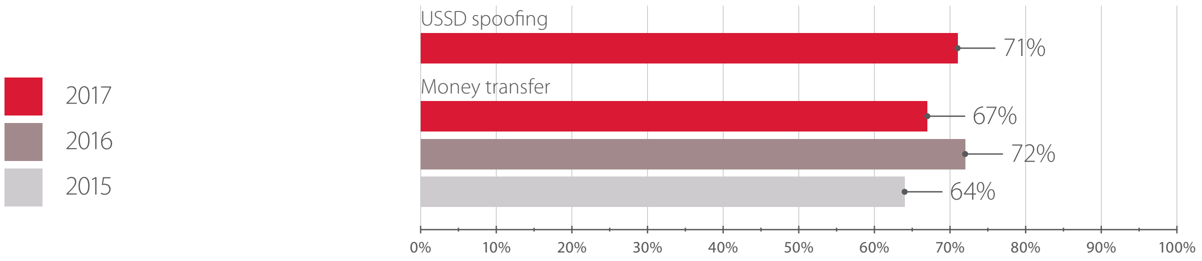


Figure 13. Forged USSD requests (percentage of successful attacks)

SMS message manipulation

Phishing or ad messages can be sent on behalf of arbitrary subscribers or services using MT-ForwardSM and MO-ForwardSM methods. MT-ForwardSM is designed for delivering incoming messages and can be used by attackers to generate forged incoming SMS messages. Unauthorized usage of MO-ForwardSM allows sending messages from subscribers and at their expense. In 2017, all networks under security analysis were exposed to vulnerabilities related to insufficient monitoring of signaling traffic and allowing fake messages to be sent.

All networks allow sending fake SMS messages on behalf of subscribers or trusted services

Subscriber profile changing

A subscriber's profile stores data about the billing platform and service subscriptions. To bypass a billing system in real time, it is necessary to delete the subscriber's O-CSI subscription, which is used to make originating calls, or to substitute the billing system address. In order to prevent non-fare calls, O-CSI parameters imply that the call must be terminated if the billing platform is unavailable. However, this parameter can be changed so that the call continues without addressing the platform. As a result, the legitimate platform does not receive information about calls and they are not billed.

Attacks using InsertSubscriberData and DeleteSubscriberData were successful in more than 80 percent of cases, while attacks using AnyTimeModification failed.

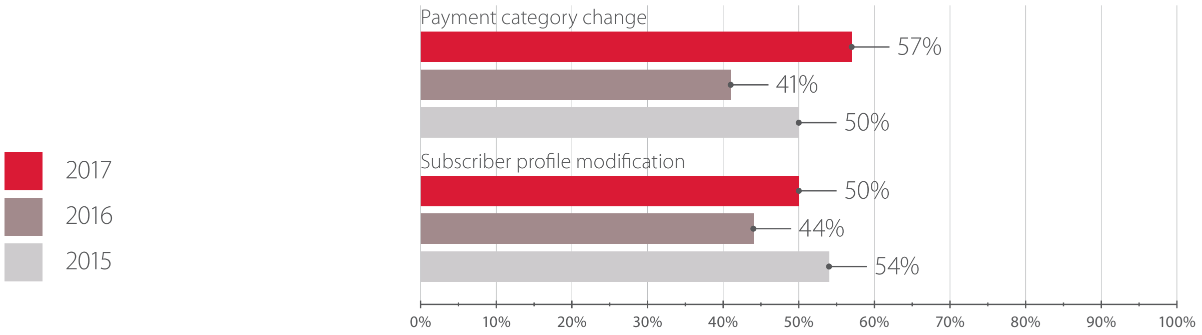


Figure 14. Subscriber profile modification (percentage of successful attacks)

All networks are exposed to a subscriber denial of service

Denial of service

Denial of service attacks against individual subscribers were possible in each network. Detected vulnerabilities are related to protocol architecture (the lack of such checks as a subscriber's belonging to the network and actual location) and allow attacks via the following methods:

- UpdateLocation
- RegisterSS
- InsertSubscriberData
- PurgeMS

All attempts resulted in a denial of service for subscribers, except using InsertSubscriberData, which allowed 83 percent of successful attacks. AnyTimeModification can be used for this purpose as well; however, the security settings of all analyzed networks blocked these requests.

Apart from the inability to make voice calls and send and receive SMS messages, an attack via InsertSubscriberData can cause internet access denial.

Although such disruption of network functioning is targeted and affects an individual subscriber, an attacker can cause a massive service denial if he or she has access to an IMSI database or is able to bruteforce IMSIs.

3 hours: average subscriber down-time

A denial of service can be critical for IoT devices. IoT is spreading rapidly, connecting billions of devices that require access to telecommunications networks. The disruption of smart home or surveillance systems, or devices that track car location, or the shutdown of industrial processes can lead to a significant subscriber churn.

The research revealed that the average subscriber down-time after a DoS attack is more than three hours. In some cases, a subscriber's profile in a database is changed after that and the equipment cannot restore the profile even when the subscriber reboots the device. This happened after DoS attacks via the PurgeMS and InsertSubscriberData methods.

If the VLR address where the subscriber is currently registered is removed from the HLR via PurgeMS initiated by a certain third-party host, terminating calls cannot be routed to the subscriber's VLR/MSC, because there is no registration address in the HLR. In this case, originating calls are available for the subscriber, because the registration record in the VLR is not changed.

Rebooting the device does not help to restore the record in the HLR, because the VLR does not initiate the UpdateLocation procedure, assuming that there are no changes in the subscriber's registration data.

It is possible to restore the registration record and therefore the subscriber's availability only by registering in the coverage area of another serving MSC (for example, by first manually selecting the network of another operator, and then selecting the home network again). Another method is to move to another MSC of the home network.

Smart devices malfunction can lead to subscriber churn

Protection measures and their efficiency

Detected vulnerabilities are caused by incorrect configuration of network equipment or protection tools, as well as by fundamental SS7 vulnerabilities. In the former case, changing equipment configuration will solve the problem. However, architecture flaws can be mitigated only by monitoring and filtering signaling traffic. To ensure analysis and blocking of incoming messages without network disruption, additional equipment is required. Let us look at some protection methods applied in analyzed networks, and assess their efficiency.

SMS Home Routing was enabled in almost every network. In 2016, operators started to implement signaling traffic blocking and filtering systems. In 2017 these systems were present in every third network.

Table 2. Installed protection tools (percentage of networks)

Protection mechanisms in place	2015	2016	2017
SMS Home Routing in place	100%	67%	100%
Signaling traffic filtering and blocking system in place	0%	7%	33%

SMS Home Routing prevents IMSI and network configuration disclosure via SendRoutingInfoForSM. The number of successful attacks is decreased by one third in case of enabling SMS Home Routing. However, in respect of incorrect equipment configuration, actual data can be obtained in 67 percent of cases.

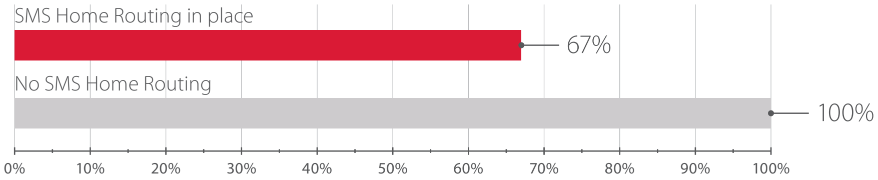


Figure 15. Obtaining IMSI with the SendRoutingInfoForSM method,
depending on the presence of SMS Home Routing (percentage of successful attacks)

SMS Home Routing cannot be used as a protection mechanism against other attacks. Moreover, it is not intended to protect a network. It is devised for correct routing of incoming SMS messages. Research results show that networks with SMS Home Routing are not more secure than others, perhaps because operators often rely solely on SMS Home Routing, neglecting additional security measures.

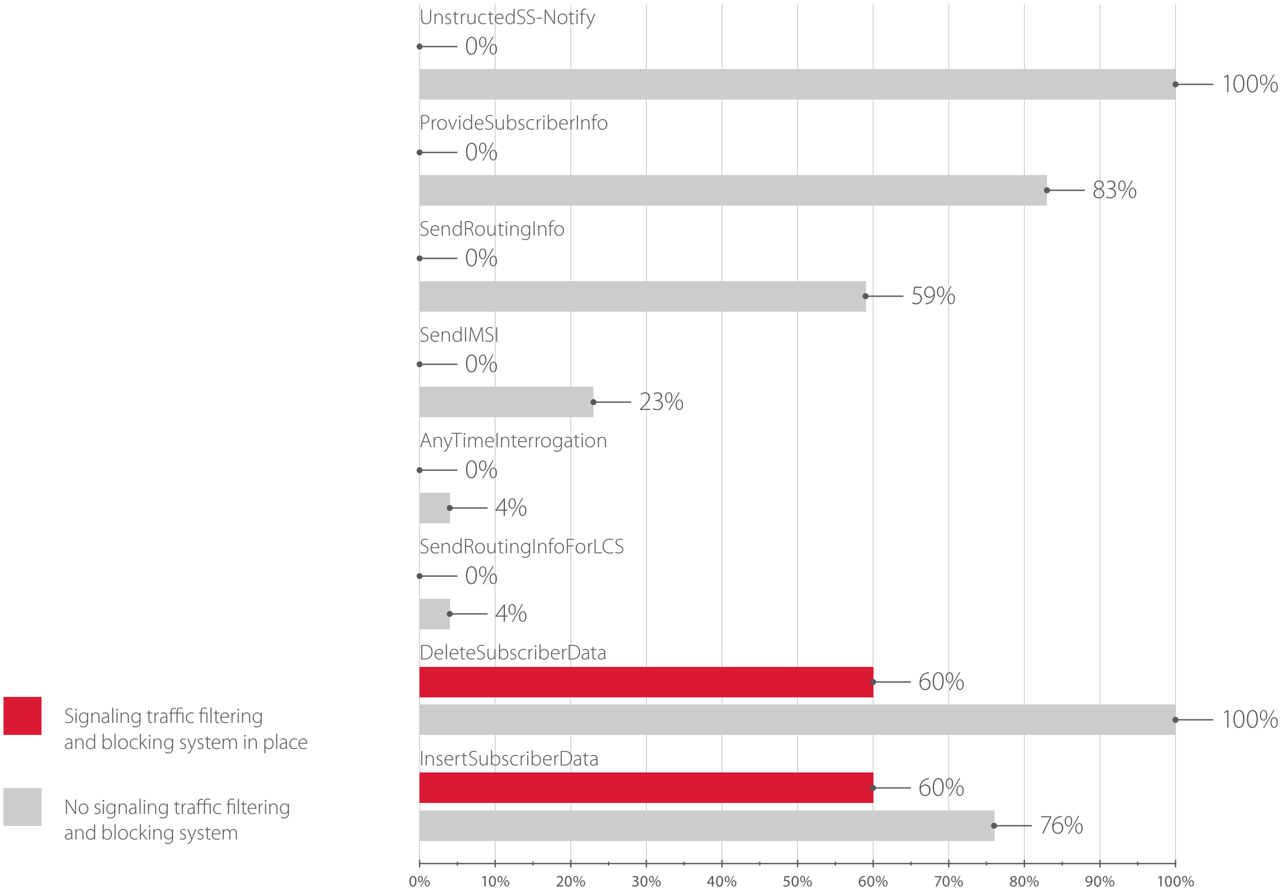


Figure 16. Percentage of successful attacks, depending on the presence
of a signaling traffic filtering and blocking system

Traffic filtering does not ensure overall security

Let us compare the results of attack attempts against which signaling traffic filtering and blocking systems are recommended as countermeasures.

Correct signaling traffic filtering reduces the risks of passing unauthorized requests. This is partly confirmed by the following diagram, which compares the possibility of each threat being implemented. It is noteworthy that there were no successful attempts to track the location of a subscriber in networks with a traffic filtering and blocking system. In 40 percent of cases, such attack attempts were successful in other networks.

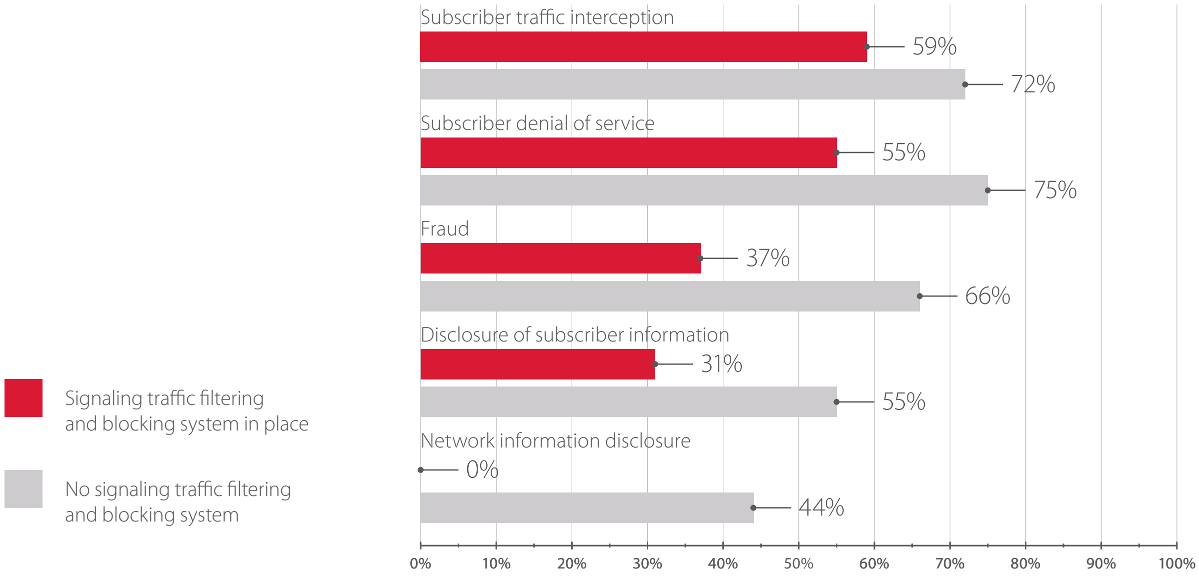


Figure 17. Percentage of successful attacks, depending on the presence of a signaling traffic filtering and blocking system

Obviously, a filtering system alone cannot protect the network thoroughly. Let us look into why this is so.

All messages listed in this report are divided into three categories as defined in GSMA IR.82.

1) The first category includes messages sent solely between home network elements.
2) The second category includes messages sent from the operator home network to the visited network where the subscriber is registered.
3) The third category includes messages sent from the visited network to the home network.

Category 1

SendRoutingInfo
SendRoutingInfoForLCS
SendIMSI
AnyTimeInterrogation
AnyTimeSubscriptionInterrogation
AnyTimeModification

Category 2

ProvideSubscriberInfo
InsertSubscriberData
DeleteSubscriberData
UnstructedSS-Notify

Category 3

SendRoutingInfoForSM
UpdateLocation
RestoreData
ProcessUnstructuredSS-Request
InterrogateSS
RegisterSS
EraseSS
PurgeMS
Mt-ForwardSM
Mo-ForwardSM

List of messages covered in this report

It is most simple to protect against attacks that use messages of the first and second categories. For this, network equipment and signaling traffic filtering need to be set up for correct analysis of incoming messages. The risk of attacks that use first category messages was minimized in 2017.

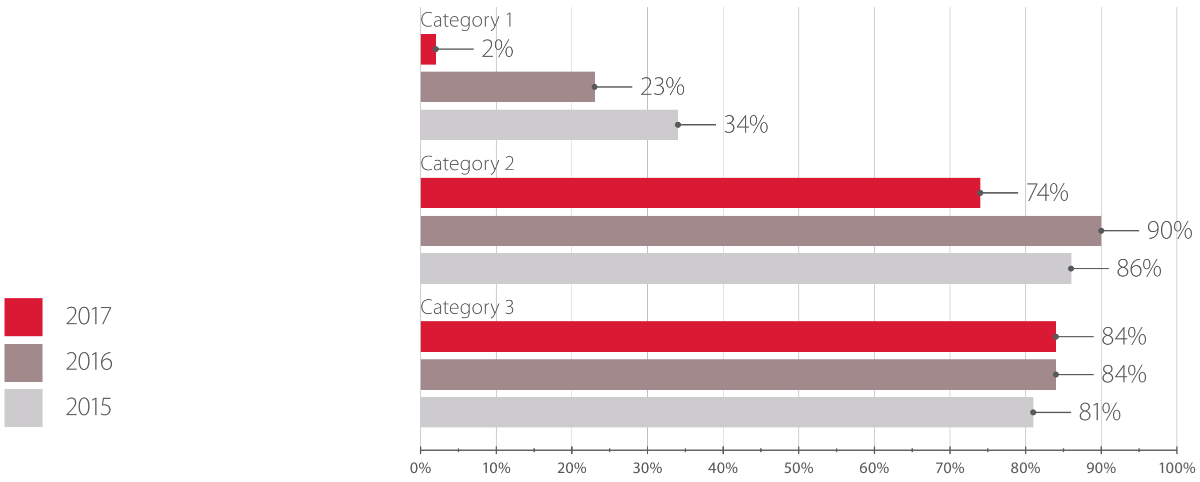


Figure 18. Percentage of successful attacks by message category

Traffic filtering systems provide thorough protection against attacks that use first category messages. As for second category messages, the risk of such attacks is twice as low.

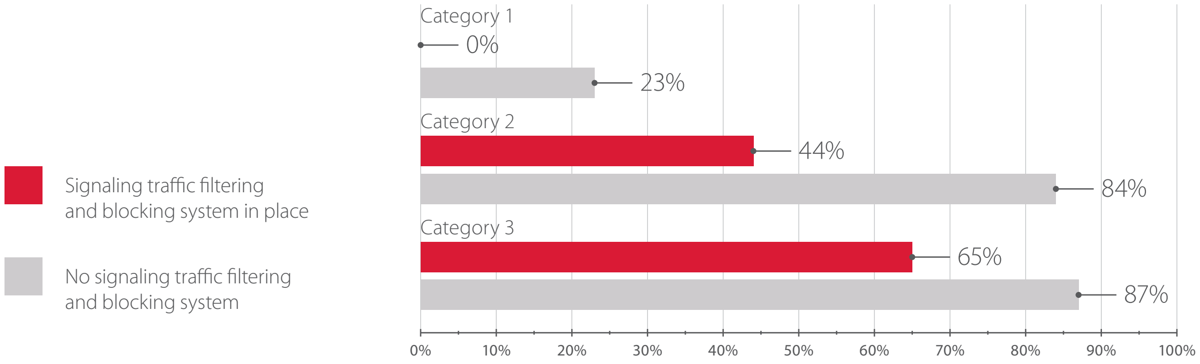


Figure 19. Percentage of successful attacks by message categories,
depending on the presence of a signaling traffic filtering and blocking system

The situation with the third category is different. Unfounded blocking of such messages can affect the service for a subscriber in roaming. For example, blocking the legitimate registration of a subscriber in the visited network by mistake can leave him or her without a phone connection in roaming; this means less profit and probably even customer loss. Detecting illegitimate requests is a challenge. It is recommended to filter messages using lists of trusted and prohibited sources provided by roaming partners, though it is not easy to put it in practice because of the necessity to constantly update such lists. Operators take a cautious approach to blocking such messages, as they fear causing network disruption. However, messages of this category allow intruders to implement all types of threats, from network and subscriber data disclosure through to subscriber traffic interception, fraud, and subscriber availability disruption.

To ensure a higher level of protection against all messages covered in this report, a comprehensive approach to information security is required. First of all it is important to analyze the security of a signaling network, for it allows detecting current vulnerabilities caused by changes in the network and equipment configuration and assessing information security risks.

Moreover, to keep security configurations up-to-date, detect threats in good time, and take appropriate measures, it is recommended to ensure continuous monitoring and analysis of messages that cross the network border. GSMA recommendations specify the use of a monitoring and attack counteraction system.[1] Special threat detection systems, which can perform intellectual analysis in real time, help to meet this requirement. This enables detecting illegitimate activity on external hosts at an early stage and sending this information to the traffic filtering system to increase its efficiency (for example, to update the list of prohibited hosts). It also allows detecting network equipment configuration errors and notifying the operator's employees of the need to modify the configuration.

Ensuring security is a process that is not limited to one-time measures (audits or protection tool implementation): Positive Technologies specialists use this motto in protecting signaling networks of their clients. For more information, visit the company's website, leave your question in the contact form, or send an email to info@ptsecurity.com.

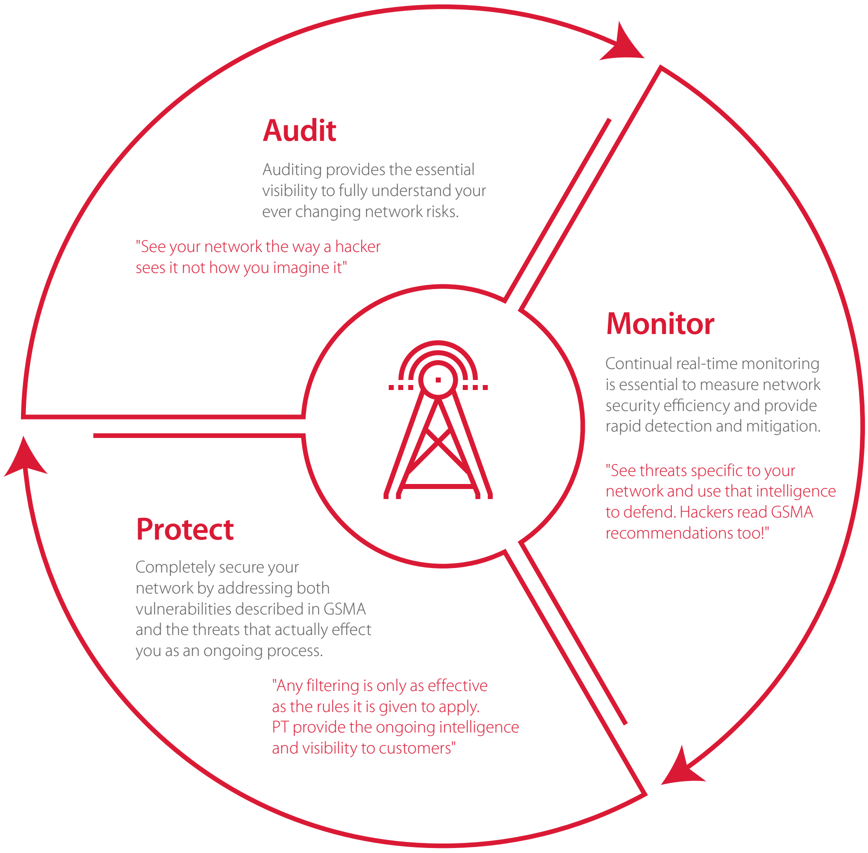

Audit
Auditing provides the essential visibility to fully understand your ever changing network risks.
"See your network the way a hacker sees it not how you imagine it"
Monitor
Continual real-time monitoring is essential to measure network security efficiency and provide rapid detection and mitigation.
"See threats specific to your network and use that intelligence to defend. Hackers read GSMA recommendations too!"
Protect
Completely secure your network by addressing both vulnerabilities described in GSMA and the threats that actually effect you as an ongoing process.
"Any filtering is only as effective as the rules it is given to apply. PT provide the ongoing intelligence and visibility to customers"

Figure 20. Recommended approach to signaling network security

In the next section, we will look at the results of using the threat detection and response system in mobile operator networks, try to find out whether existing security measures are sufficient to counteract intruders in real-time conditions, and how the use of the threat detection and response system can ensure network security.

[1] SG.11. SS7 Interconnect Security Monitoring Guidelines.

ATTACKS ON SS7 NETWORKS

We have examined vulnerabilities in SS7 networks and potential threats related to their exploitation. One question remains open: how do security research results compare with the capabilities of real-life criminals? In this section, we will share the results of security monitoring projects in SS7 networks, and see what kind of attacks mobile operators actually face and whether existing security measures are effective in practice.

Methodology

Security monitoring projects in SS7 networks were carried out for large telecom operators in Europe and the Middle East. They were aimed at demonstrating the capabilities of the PT Telecom Attack Discovery (PT TAD) system, which is designed to analyze signaling traffic in real time and detect illegitimate activity with the possibility of blocking unauthorized messages and notifying third-party systems for traffic filtering and blocking. This approach allows potential threats to be identified in a timely manner and to react without adversely affecting the network functioning.

PT TAD can also be used as a passive system for detecting illegitimate activity. In this case, the system allows analysis to be carried out, but does not affect the traffic flow. This study presents the results of traffic monitoring in passive mode.

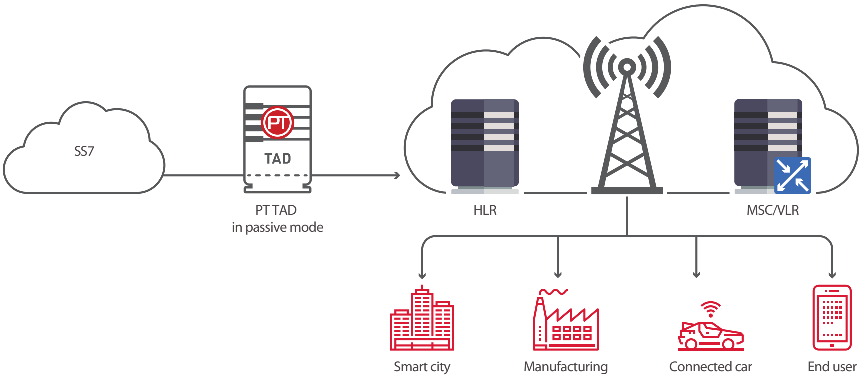


Figure 21. Diagram of hardware connection for analyzing signaling traffic with PT TAD in passive mode

Statistics on attacks detected

In all networks where works were carried out to monitor security events, SMS Home Routing was used while a filtering and blocking system for signaling traffic was installed in every third network.

During the monitoring, we obtained results indicating that attackers are not only well aware of security problems in signaling networks but also actively exploit these vulnerabilities.

In the table, the vertical axis shows the distribution of all attack attempts broken down by method. The percentage of successful attacks is given for each threat and separately for each method. An empty cell means that the message does not lead to threat realization.

For example, in 79.9 percent of cases an attempt to get a subscriber's IMSI is performed by attackers using the SendRoutingInfo method. Overall, in 34.5 percent of cases attackers successfully managed to obtain IMSI with that method or another. As for SendRoutingInfo, the method was successful in 22.6 percent of attack attempts.

Table 3. Distribution of attacks by threat types

	Subscriber information disclosure				Fraud					
	IMSI disclosure	Subscriber location disclosure	Subscriber profile information disclosure	Network information disclosure	Call redirection	Exploitation of USSD request manipulation	Real-time billing evasion	SMS interception	Disruption of service availability for subscribers	**Percentage of successful attacks**
SendRoutingInfoForSM	15.7%			5.2%						87.2%
SendRoutingInfoForLCS	3.3%			1.1%						1.1%
SendRoutingInfo	79.9%	27%		26.3%						22.6%
SendIMSI	1.1%									65.6%
AnyTimeInterrogation		69.3%		67.4%						13.3%
ProvideSubscriberInfo		3.7%								58.6%
RestoreData			84%							0.5%
UpdateLocation			0.9%		4.7%			100%	4.6%	100%
AnyTimeSubscriptionInterrogation			14.8%							0%
InterrogateSS			0.3%							58.8%
AnyTimeModification					0.6%		0.5%		0.6%	0.1%
InsertSubscriberData					93.2%		86.7%		90.6%	1.5%
RegisterSS					1.5%				1.4%	26.7%
ProcessUnstructuredSS						0.6%				53.3%
UnstructuredSSNotify						99.4%				31.1%
DeleteSubscriberData							12.8%			2.1%
PurgeMS									2.8%	53.3%
Percentage of successful attacks	34.5%	17.5%	1.5%	20.1%	6.5%	31.2%	1.5%	100%	7.8%	

As we found out, the source of most attacks is not national telecom operators of the country where security monitoring was carried out, but rather global telecom operators. Meanwhile, suspicious requests come mainly from countries of Asia and Africa. This may be because in these countries attackers consider it easier and cheaper to buy access to the SS7 network. It is noteworthy that there is no need for physical access to equipment of the operator that provided connection to SS7—an intruder can attack from any point of the globe.

To demonstrate the average number of attacks per day, we selected a large operator with a subscriber base of over 40 million people. The operator gave consent to publishing the data without specifying the company name.

Table 4. Average number of attacks per day by threat types

Threat	Average number of attacks per day
Subscriber information disclosure	4,827
IMSI disclosure	3,087
Subscriber location disclosure	3,718
Subscriber profile disclosure	47
Network information disclosure	4,294
Fraud	62
Call redirection	2
USSD request manipulation	59
Real-time billing evasion	2
SMS interception	1
Disruption of service availability for subscribers	4

Information leakage

Almost all the attacks were aimed at disclosing information about the subscriber and the operator's network. Fraud, subscriber traffic interception, and disruption of service availability for subscribers totaled less than 2 percent.[2]

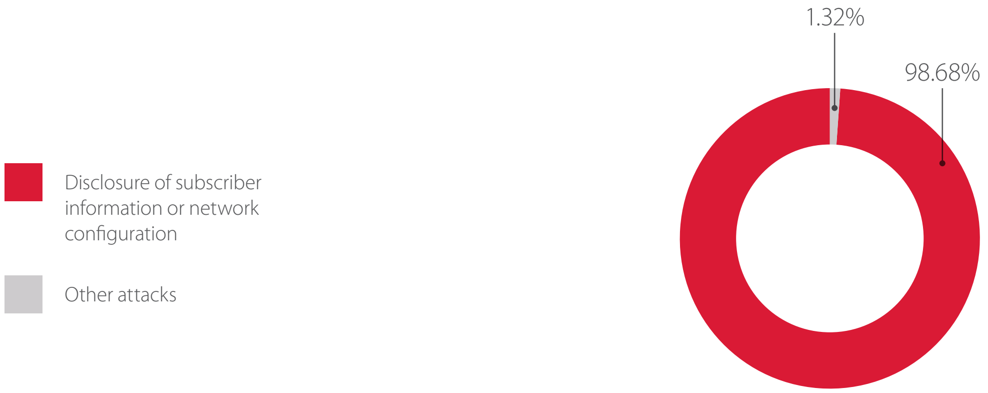


Figure 22. Distribution of attacks by threat types

Such distribution is due to the fact that an intruder first needs to obtain subscriber identifiers and host addresses of the operator's network. Further attacks are subject to obtaining all the necessary data at the first stage. Still, data mining does not necessarily mean an imminent targeted attack on the subscriber. Instead of carrying out technically complicated attacks, there is an easier way to make a profit by selling information to other criminal groups. Mass single-type requests may indicate that attackers are building subscriber data bases, in which telephone numbers are matched against user identifiers, and collecting the operator's data for a subsequent sale of obtained information on the black market.

Every third attack aimed to get a user IMSI, and every fifth attack aimed at disclosing network configuration helped attackers obtain information they were looking for.

To obtain information, mainly two methods were used: AnyTimeInterrogation and SendRoutingInfo. Both of them allow network information disclosure, and SendRoutingInfo alone returns a subscriber IMSI; in addition to that, these messages allow subscriber location to be detected. As our results show, in 17.5 percent of cases network responses to such requests contained data regarding subscriber location.

In 87 percent of systems suspicious requests managed to bypass SMS Home Routing

Filtering settings on network equipment (STP, HLR) or a correctly configured filtering system for signaling traffic would completely eliminate the possibility of attacks using these messages and, therefore, mitigate the risk of other threats. However, in practice, message filtering options are not always set correctly. For instance, the percentage of responses to suspicious requests aimed at detecting user location was half as high in networks protected with a signaling traffic blocking system than in other networks. Approximately the same results were obtained for attacks aimed at disclosing network configuration and subscriber identifiers. Overall, these are good indicators. They point to effective protection measures. Still, if the configuration was correct, the proportion of successful attacks would be reduced to zero.

It is noteworthy that all networks used the SMS Home Routing system to counteract attacks based on the SendRoutingInfoForSM method. The SendRoutingInfoForSM message requests information needed to deliver the incoming SMS: the subscriber identifier and the serving hosts address. In normal operating mode, an incoming SMS should follow this message, otherwise the requests are considered illegitimate.

[2] The UpdateLocation procedure returns information about the subscriber's profile. However, we suppose that by registering a subscriber in a fake network an intruder primarily pursues other goals: interception of terminating calls or SMSs, or subscriber denial of service.

Each request should be sent to the SMS Home Routing system, which returns virtual identifiers and addresses. However, due to the seemingly incorrect configuration of network equipment, this method of protection turned out to be not efficient enough: in 87 percent of cases, suspicious requests managed to bypass SMS Home Routing. We observed similar results in the course of SS7 network security assessment.

Intruders successfully carry out 23 percent attacks for the purpose of fraud

Fraud

Fraud-related attacks targeted at both operators and subscribers totaled only 1.32 percent, most of which exploited USSD requests. Unauthorized sending of USSD requests allows attackers to transfer money from a subscriber's account, subscribe a user to an expensive service, or send a phishing message under the guise of a trusted service.

About a quarter of all attempts were successful—the messages were accepted by the operator's network as legitimate, even though traffic filtering tools were in place.

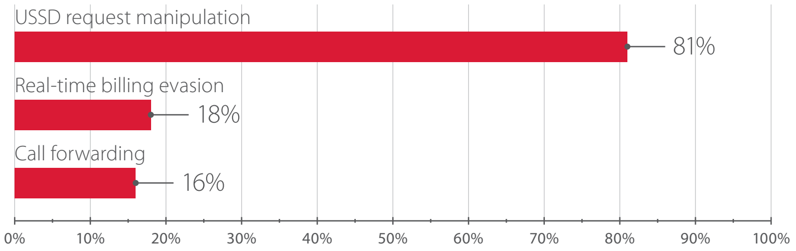


Figure 23. Attacks for fraudulent purposes

100 percent of attacks aimed at SMS interception are successful

Traffic interception

In the course of the works, we found UpdateLocation requests for subscriber registration in a new network. The requests were coming from suspicious sources. Meanwhile, no fake registration attempt was rejected by the operator's network. According to the security assessment results and data obtained from security monitoring projects, the use of filtering and traffic blocking systems does not provide significant advantages in this case—comprehensive security measures must be taken to stay protected from such attacks.

Illegitimate UpdateLocation requests amounted to only 0.01 percent of the total number of attacks, but this vector has a particularly high severity since it allows criminals to intercept a subscriber's SMS containing confidential information and redirect calls to intruders' phone numbers—this can be used by criminals for fraudulent purposes.

In 2017, a vivid example of an attack using SS7 network vulnerabilities was an SMS interception targeting a German mobile operator's subscribers, in which the attackers managed to steal money from users' bank accounts. The attack was carried out in two stages. At the first stage, the criminals sent users messages containing a link to a phishing web site disguised as an official bank site and stole logins and passwords for bank accounts. To pass the two-factor authentication and confirm further operations, they needed access to one-time codes that the bank sends users in SMS. It is assumed that the criminals bought access to the SS7 network on the black market in advance. At the second stage of the attack, they registered subscribers in the fake network, pretending to be a roaming partner—a foreign mobile operator. Afterwards, incoming SMSs containing one-time codes and transaction notifications were sent to the intruders' phone numbers. According to experts, the criminals attacked mainly during the night time to mitigate the risk of being caught.

Denial of service is crucial for the internet of things

Denial of service

Attacks aimed at denial of service were not numerous either, with only 7.8 percent of such attacks being successful. The InsertSubscriberData method was mainly used, but 99 percent of these messages remained unanswered—they were ignored by the operator's network. Filtering and traffic blocking systems had a significant impact on the final results—the percentage of successful requests in these networks was four times lower than in the rest, but it was not possible to stay completely protected from such attacks.

Denial of service is a serious danger for IoT electronic devices. Today, not only individual user devices are connected to communication networks, but also smart city infrastructure elements, modern industrial enterprises, transport, energy, and other companies.

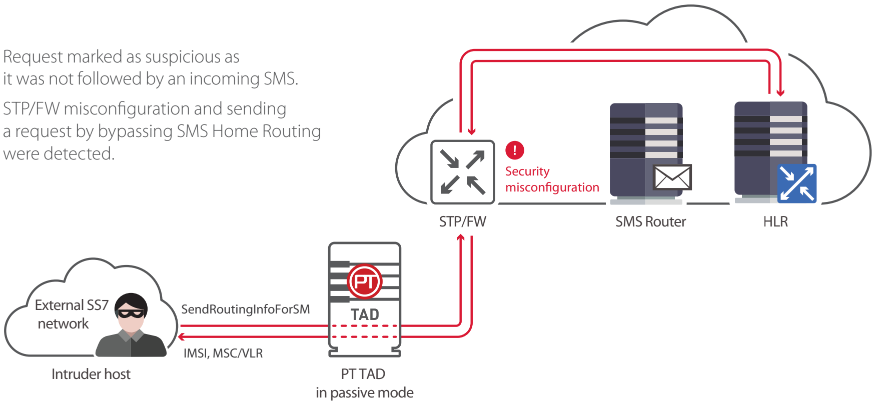
As we have already mentioned, an attacker can conduct an attack on subscriber availability in such a way that communication cannot be restored without contacting technical support, while the down time exceeds three hours on average. Losing its reputation as a reliable telecom supplier can deprive the operator of a significant clientele base—they will simply switch supplier.

Attack example

As noted above, implementing single security measures without applying an integrated approach to security is not enough to counteract all attacks exploiting vulnerabilities, the causes of which lie in the very architecture of SS7 networks.

Let us review a real example found by our experts. The attack was a series of successive steps that the attack detection system was able to combine into a logical chain, while existing security systems failed to recognize single requests as illegitimate. First of all, the attackers made a successful attempt to detect a subscriber IMSI by the phone number. Having obtained the necessary information for further actions, they tried to locate the subscriber. However, that stage of the attack failed. A day later, the attackers sent a request for subscriber registration in a fake network. The request was accepted by the operator's network. So they were able to intercept the subscriber's incoming calls and SMSs, which was probably their goal. Let us review each step in detail.

The PT TAD threat detection and response system identified SendRoutingInfoForSM messages sent from an external host to a subscriber of the operator's home network. The messages were marked as suspicious because they were not followed by an SMS, as expected in the case of legitimate activity. Each message was followed by an attempt to attack via ProvideSubscriberInfo, which was blocked by the network. The PT TAD system detected a sequential combination of SendRoutingInfoForSM and ProvideSubscriberInfo attacks with an interval of 1–2 seconds, which indicates that locating a subscriber is performed automatically.

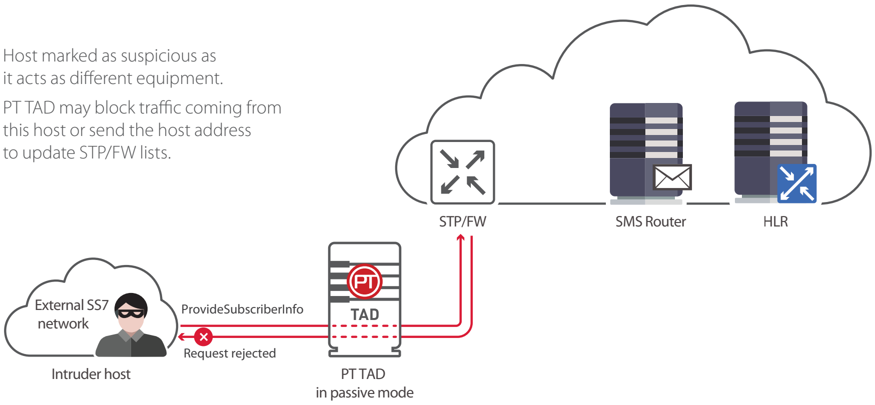


Request marked as suspicious as it was not followed by an incoming SMS.

STP/FW misconfiguration and sending a request by bypassing SMS Home Routing were detected.

Figure 24. Processing a suspicious SendRoutingInfoForSM request

As the SMS Home Routing system was used in the operator's network, the response to the SendRoutingInfoForSM message should not have contained the real IMSI, nor the real MSC/VLR address. However, the generated package somehow allowed bypassing the SMS Home Routing operating mechanism containing configuration flaws. The boundary STP must send SendRoutingInfoForSM messages received from the outside to the SMS Router. However, if address routing has a higher priority than operation code checking in the STP configuration, an intruder can send a SendRoutingInfoForSM message addressing it in the numbering plan (E.214) for subscriber registration in a roaming network (UpdateLocation), so STP will route the signaling message without checking the operation code. As a result of the attack, the intruders obtained neither the platform address nor the virtual IMSI, but rather the subscriber's actual MSC/VLR address and the real IMSI. The obtained data were used for another ProvideSubscriberInfo attack attempt aimed at locating the subscriber.



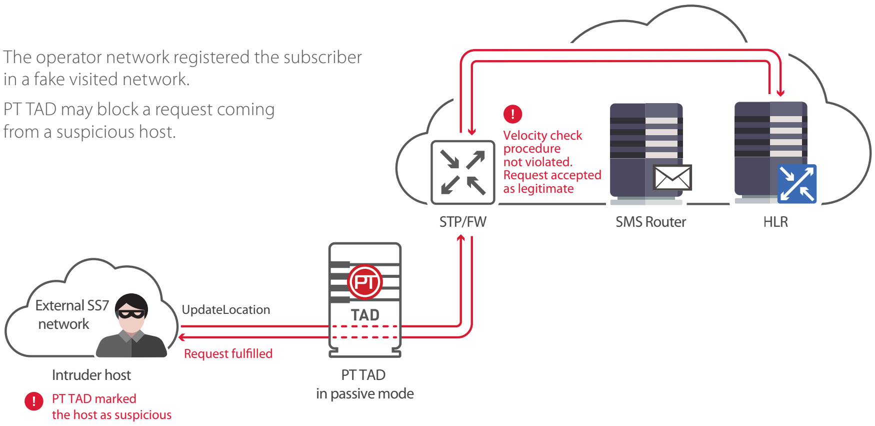
Host marked as suspicious as it acts as different equipment.

PT TAD may block traffic coming from this host or send the host address to update STP/FW lists.

Figure 25. Attempt to locate the user

After detecting attempts to attack from a host acting as different equipment (MSC and HLR in this case), the host was marked as suspicious. The following day, the host sent an UpdateLocation request to update the same subscriber's registration. The request did not violate the subscriber's velocity check procedure, since the previous UpdateLocation message was received six hours earlier and was passed by the signaling filtering system as legitimate.

If the network applied an integrated security approach, namely, security monitoring with an integrated blocking system, right after a successful SendRoutingInfoForSM attack and an unsuccessful ProvideSubscriberInfo attack, the monitoring system would immediately notify the filtering module that it is required to update the list of blocked hosts to block any traffic coming from this host.



The operator network registered the subscriber in a fake visited network.

PT TAD may block a request coming from a suspicious host.

Figure 26. Subscriber registration in a fake network

CONCLUSION

The research has shown that the level of security of mobile communication networks is still low. The overwhelming majority of networks remain vulnerable, which allows criminals to intercept subscribers' voice calls and messages, perform fraudulent operations, and disrupt service availability for subscribers.

Intruders are well aware of the existing vulnerabilities and we have already seen consequences of their attacks, as exemplified in the recent incident that affected subscribers of a German telecom operator, which resulted in money theft from user bank accounts. Given the level of illegitimate activity detected by the PT TAD threat detection and response system, we can expect new similar examples in the near future.

We noted that operators are aware of security flaws in signaling networks and that they are starting to implement additional security measures to eliminate vulnerabilities, including filtering and blocking of signaling traffic. However, these systems cannot completely solve problems associated with specific features of the SS7 network architecture.

To counteract criminals, an integrated approach to security is required. Regular security assessment of signaling networks is required to identify existing vulnerabilities and develop measures to mitigate threat realization risks, and then—to keep security settings up-to-date. Alongside with that, it is important to continuously monitor and analyze messages that cross network boundaries to detect potential attacks. This task can be performed by an attack detection and response system that detects illegitimate activity at an early stage and blocks suspicious requests, or passes information about unauthorized connections to third-party systems, thus increasing the efficiency of existing security measures. This approach ensures high-level protection without disrupting the normal operation of mobile networks.

For more information, visit the company's website, leave your question in the contact form, or send an email to info@ptsecurity.com.

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.

© 2018 Positive Technologies. No part of this document may be used, reprinted, or cited without mentioning the authors and the rightholder. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com