PRIMARY SECURITY THREATS FOR SS7 CELLULAR NETWORKS

2016

POSITIVE TECHNOLOGIES

Contents

Introduction

SS7 exploits can turn a cell phone into an open book, allowing an attacker to read messages, track a subscriber's location, and eavesdrop on and redirect calls. This technique is now available not only to intelligence services, but to an average hacker as well. In 2014, we described in detail security issues in signaling networks[1]. This report contains a security analysis of SS7 networks for various operators with a subscriber base of 10 to 70 million.

Technology from the 1970s

The SS7 signaling system is often called the nervous system of a phone network. Before the invention of SS7, service commands for subscriber connection and data packet delivery were transferred via a speaking channel. This approach was upgraded and replaced with the global signaling system (SS7) over 30 years ago. Today the SS7 standard determines the procedures and data exchange protocols across network devices of telecom companies. SS7 serves as a base for a signaling infrastructure in local, national, international, and wireless networks.

The SS7 system CCS-7, which dates to the 1970's, is riddled with security vulnerabilities like the absence of encryption or service message validation. For a long time, it didn't pose any risk to subscribers or operators, as the SS7 network was a closed system available only to landline operators. The network evolved to meet new standards of mobile connection and service support and in the early 21st century, a set of signaling transport protocols called SIGTRAN was developed. SIGTRAN is an extension to SS7 that allows the use of IP networks to transfer messages, and with this innovation the signaling network stopped being isolated.

SS7 vulnerabilities were exposed in 2008, when German researcher Tobias Engel demonstrated a technique that allows mobile subscribers to be spied on[9]. In 2015, Berlin hackers from SR Lab were able to intercept SMS correspondence between Australian senator Nick Xenophon and a British journalist during a live TV broadcast of the Australian program "60 Minutes". They also managed to geo-track the politician during his business trip to Tokyo[6].

Experts discovered these flaws a number of years ago — Lennart Ostman reported SS7 issues in 2001[3], and the US government expressed their concern about the problem in 2000[4]. In 2013, Edward Snowden identified SS7 exploitation as one of the techniques used by the National Security Agency[8]. According to Bloomberg[5], several agencies like Defentek and Verint Systems offer spying services via SS7. The Italian spyware maker Hacking Team received similar offers from the Israeli startup CleverSig and the Bulgarian company Circles. Interestingly this only came to light after the cybergroup was hacked and 415GB of data from their servers leaked online[10]. The British company Cobham provides location discovery service with up to a meter precision to more than a dozen countries, says Bruce Schneier[7], indicating that the SS7-based spying market is rapidly growing.

What an Attacker Can Do

With access to SS7 and a victim's phone number, an attacker can listen to a conversation, pinpoint a person's location, intercept messages to gain access to mobile banking service, send a USSD command to a billable number, and conduct other attacks[1].

It's important to note that it is still impossible to penetrate the network directly —it must be accessed via an SS7 gateway. But getting access to an SS7 gateway is relatively easy. An attacker can obtain the operator's license in countries with lax laws or purchase access through the black market from a legal operator for several thousand dollars. If there is an engineer in a hacker group, they will be able to conduct a chain of attacks using legitimate commands or connect their equipment to SS7. There are several ways to get into a network using hacked carrier equipment, GGSN[2] or a femtocell.

SS7 attacks may be performed from anywhere and an attacker doesn't have to be in physical proximity to a subscriber, so it's almost impossible to pinpoint the attacker. Additionally, the hacker does not need to be a highly skilled professional either. There are many applications for SS7 on the internet, and cellular carriers are not able to block commands from separate hosts due to the negative impact this would have on service and the violation of roaming principles.

Signaling network vulnerabilities open up multiple opportunities for various attacks. For example, SS7 MAP commands allow cell phones to be blocked from a distance[11]. Issues with SS7 security threaten not only mobile subscribers but also a growing ecosystem of industrial and IoT devices — from ATMs to GSM gas pressure control systems, that are also considered mobile network subscribers.

Therefore SS7 security is one of the priorities when building a global cellular defense.

The research contains statistics collected by Positive Technologies specialists during their SS7 security analysis in 2015. We have examined existing threats and the current level of signaling network protection against outsider attacks.

1. Research Methodology

In 2015, Positive Technologies' experts conducted 16 sets of testing involving SS7 security analysis for leading mobile EMEA and APAC operators. The results of the top 8 projects are included in the statistics below.

We imitated outsider's actions both on a national and international level of a signaling network, and conducted tool scan of SS7 networks using special software in order to:

- Check signal messages filtering and analyze vulnerabilities related to them
- Investigate ways to attack signaling network nodes and mobile operator subscribers

The experts examined a scenario where an attacker acts from an external signaling network and conducts attacks based on application level messages (MAP, CAP).

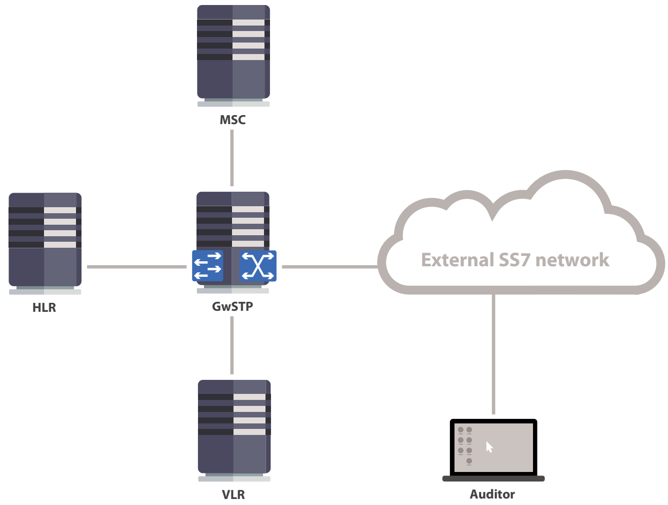

Figure 1. SS7 Security analysis procedure

The resulting information helps to improve the robustness of network security standards of mobile services and mitigate risks related to network integrity and fraudulent activity.

2. Summary

Key findings:

No SS7 network is safe

All SS7 networks examined could be exploited from the outside. For example, DoS attacks targeting an individual subscriber were successful in 80% of cases. Threats related to fraud, including theft of funds from user accounts, could be accomplished in 67% of cases.

Subscriber data is at risk

All SS7 networks had vulnerabilities that allowed data leaks and SMS interception. All attempts to discover subscriber location were successful except in one network.

EMEA networks are less secure

The majority of vulnerabilities were detected in cellular operator networks from EMEA. They allowed an attacker to cause service disruption, commit fraud, and steal sensitive data. Nevertheless, the selection was not representative enough to make general statements regarding the level of security of SS7 networks for specific geographic areas.

Large operators cannot guarantee security

As expected, small mobile operators are less protected against outsider threats. However, even the leading cellular carriers are not able to provide a sufficient level of security and the percentage of successful attacks was significant in all cases.

3. Participant Profile

25% of the investigated SS7 networks belong to large-scale mobile operators with a client base of 40 to 70 million subscribers. Relatively small companies are also included in the report (up to 10M subscribers) and constitute another quarter of all the cellular carriers.

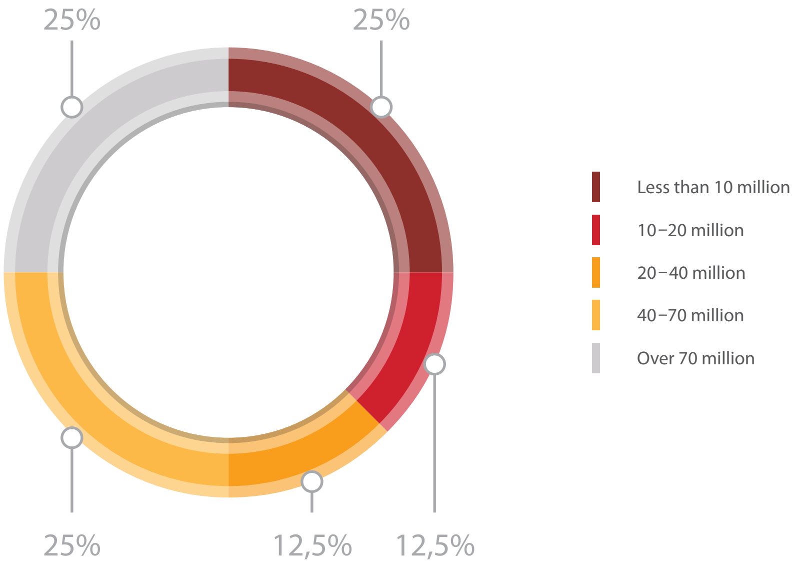

Figure 2. Operators distribution by subscriber database

The majority of SS7 networks belong to APAC (Asia, Pacific, Americas and the Caribbean), and only a quarter of them — to EMEA (Europe, Russia, the Middle East, and Africa).

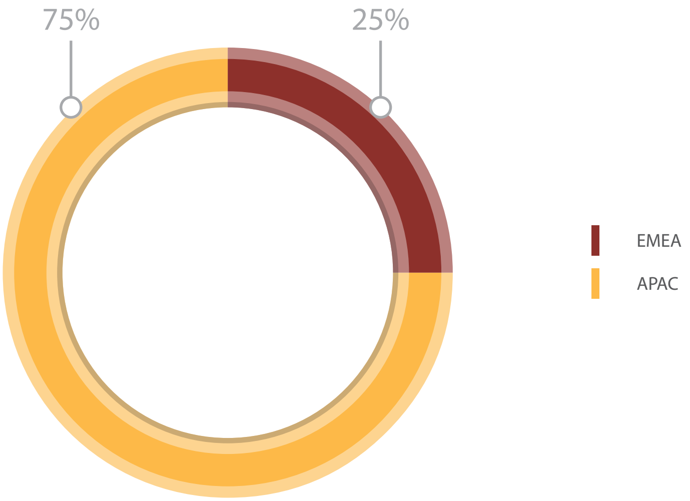

Figure 3. Systems distribution by region

Due to confidentiality agreements, we cannot disclose the names of companies that took part in the research.

4. Threat Success Rate

We divided threats against SS7 and mobile operator subscribers into three groups:

- Sensitive data leakage
- Fraud
- Operation disruption

All types of threats may cause reputational and financial loss to a mobile operator.

Data leakage implies disclosure, interception or theft of subscriber information or SS7 configuration details, including subscriber location, texts, and conversations.

We defined any unauthorized activity in the network as fraudulent, such as illegal money transfer from user accounts, calls redirection or modification of a subscriber's profile.

Operation disruption in the SS7 network or its services is caused by DoS attacks.

4.1. Most Common Threats

All the researched networks were exploitable. During the security analysis, experts managed to execute 80% of DoS attacks, 77% of leakage attacks, and 67% of fraudulent actions.

Multiple vulnerabilities and equipment configuration errors leave a wide surface for a potential attack.

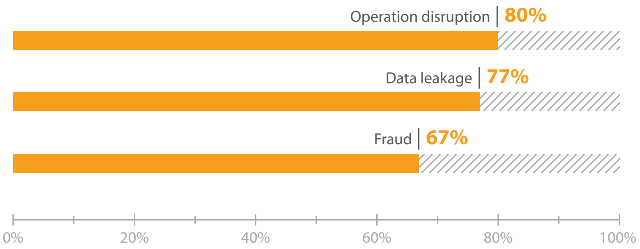

Figure 4. Percentage of successful attacks

There are four types of flaws:

- Lack of location verification
- No way to check whether a subscriber belongs to a network
- No filtering of unused signaling messages
- Configuration flaws in SMS Home Routing.

SMS Home Routing is a hardware and software solution that supports proxy functions of confidential subscriber identifiers and equipment addresses when receiving texts from external connections.

Vulnerability exploitation may lead to the realization of various attack scenarios. For example, if a bad actor conducts attacks related to lack of verification mechanisms, it is then possible for him to determine a current subscriber's location (data leakage) or to forward originating calls to a billable number (fraud).

Each SS7 network was susceptible to multiple attacks (nine on average) based on the lack of a location verification mechanism. More than three vulnerability exploitation attempts were possible due to inability to check whether a subscriber belongs to a network. In most cases such flaws are the critical to the system.

Risk levels are color-coded: red — high, orange — average. The Positive Technologies experts evaluated risks based on the impact and exploitation difficulty. There is no need for complex equipment to conduct an attack. We used a Linux-based host and a publicly available SDK for SS7 packets generation.

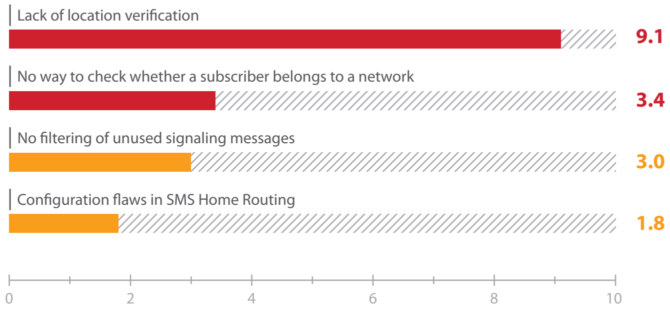

Figure 5. Average number of successful attacks per SS7 network by exploit type

The above vulnerabilities include configuration flaws (lack of filtering mechanism for signaling messages and Home Routing configuration errors), architecture issues of protocols and systems (no way to check if a subscriber belongs to a network and lack of location validation), and software flaws (error that causes software to produce an incorrect or unexpected result).

As shown on the graph below, the majority of successful attacks (61%) exploit architecture flaws and only 1% — software vulnerabilities.

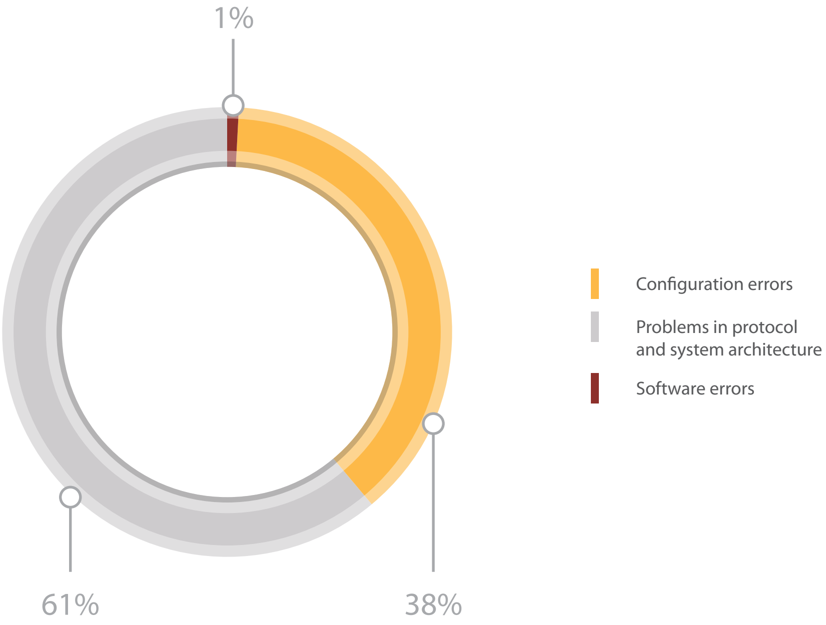

Figure 6. Percentage of successful attacks by type

In order to fix vulnerabilities, a system designer needs to employ an appropriate approach. This could be the use of additional technical and software security tools or changes in system settings. For more details, see Section 4.4.

4.1.1. Information Leakage

As mentioned above, data leakage implies subscriber information exposure. In general, realization of such threats doesn't cause any direct loss to operators. However, public disclosure of a data leak may lead to reputational loss, and ensuing economic loss as subscribers choose alternative carriers.

Key threats:

- Listening in to calls
- Getting subscriber balance information
- SMS interception
- Location disclosure
- Stealing of subscriber information.

According to the research, all SS7 networks are vulnerable to attacks aimed at subscriber data leakage and SMS interception. Only once did we fail to discover a subscriber's location. Not all tested hacking methods prove to be effective. For example, 90% of attempts to get subscriber balance or data were to be successful, while only 50% of call tapping attempts succeeded.

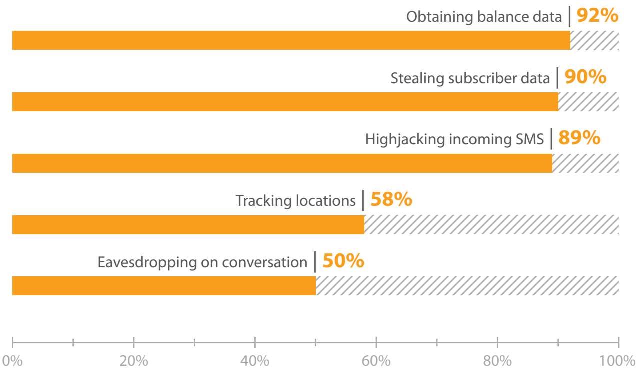

Figure 7. Percentage of successful attacks for sensitive data extraction

In particular, in order to obtain subscriber data from cellular carriers, we used specially crafted messages of the following types:

- SendRoutingInfo;
- SendRoutingInfoForSM;
- SendRoutingInfoForLCS;
- SendIMSI.

As shown in the diagram below, attacks were successful in 76% of cases when using the SendRoutingInfo method. It exploits the lack of filtering for unused signaling messages. SendRoutingInfo is a MAP message for terminating calls and inquiring routing information and normally, this message should pass only between network elements of a home network. The Positive Technologies experts classify this threat as medium because by using this method, an attacker may obtain subscriber data, and determine the user's current location.

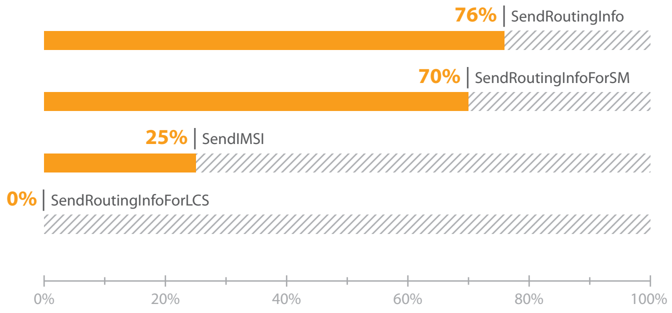

Figure 8. Percentage of successful attacks for sensitive data extraction by method

SendRoutingInfoForSM is a MAP message for incoming SMS used for inquiring routing information to determine a subscriber's location. This message should be routed to the SMS Home Routing equipment, if it's deployed in the operator's network. This method is effective in 70% of cases.

SendIMSI is a MAP message that is employed to determine a subscriber's IMSI by his phone number. It is used infrequently, however the equipment often processes it according to 3GPP specification and one in four attempts were successful.

SendRoutingInfoForLCS is a MAP message that is used to inquire routing information for location services. Normally, this message would be employed only among home network elements. According to the research, no SendRoutingInfoForLCS-based attack succeeded.

An adversary may use other methods to obtain a subscriber's location as shown on the diagram below.

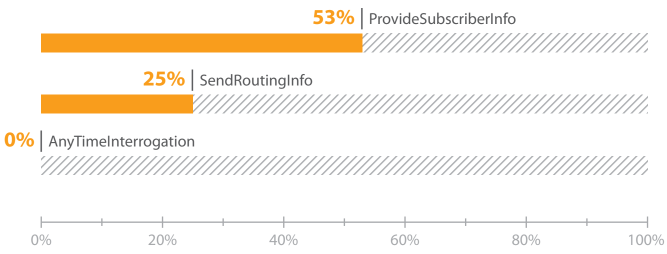

Figure 9. Percentage of successful attacks aimed to discover a subscriber's location by method

AnyTimeInterrogation is a MAP message used by nodes to determine a subscriber's location. This message is applied exclusively within the home network.

ProvideSubscriberInfo is a MAP message that is used by various services to derive location data. No external connections to home network subscribers are allowed.

All AnyTimeInterrogation attacks failed for all the projects in 2015, however 53% of attacks using ProvideSubscriberInfo resulted in discovery of a subscriber's location. We were able to accomplish the objective in all networks except for two.

As stated above, we succeeded in about half of the attacks designed to intercept originating and terminating calls. For terminating calls, we accomplished an attack based on roaming spoofing and traffic transferring to another switch. Listening in to originating calls was conducted using the InsertSubscriberData method with traffic transferring to another switch.

InsertSubscriberData is a MAP message that is used to change a subscriber's profile in the VLR database. Attackers can modify the platform value in the profile so that call billing would go through their equipment. A mobile switch would send a request to proceed with an originating call to the indicated address. An adversary needs to send a command to forward a call to a controlled PBX, and then transfer traffic to a destination user. Thus, a conversation between subscribers will be openly held via PBX under the complete control of the attacker.

We used the UpdateLocation method to intercept incoming SMS messages and 89% of the attacks were successful. UpdateLocation is a message that is used to request registration in the area of coverage of a new mobile switch. This message comes from the roaming partner network at a subscriber's registration attempt. An attacker may complete subscriber's registration in a false network, which means that all incoming texts will be transferred to the indicated address.

4.1.2. Fraud

According to the research results, each system had its own handicaps that allow an outsider to conduct fraudulent actions, such as:

- Call redirection
- Funds transfer from a subscriber's account
- Changing a subscriber's profile.

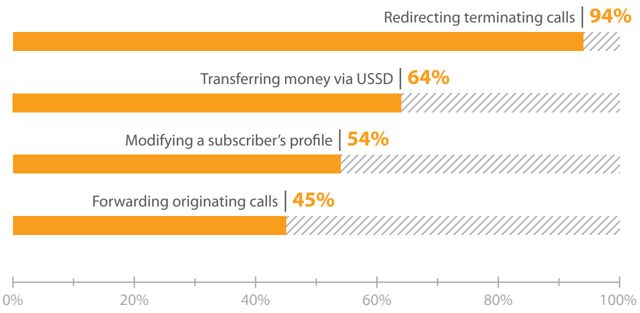

Figure 10. Percentage of successful attacks depending on a threat (fraud)

94% of the attacks aimed at terminating call forwarding were successful but the same was true only for 45% of originating calls. These numbers show that there are some serious issues in the system and protocol architecture of SS7 networks.

In order to redirect originating calls, we employed the InsertSubscriberData method. We based the attacks for terminating calls forwarding on the following two methods:

- Roaming number spoofing
- Redirection manipulations

Roaming number spoofing is conducted during a terminating call to a target subscriber. Beforehand, a victim must be registered in a false network. As a response to a roaming number inquiry, an attacker should send a number for call redirection. All the connections will be at the operator's expense.

Redirection manipulation includes unauthorized setting of unconditional forwarding. All terminating calls will be redirected to a given number and the subscriber will be the one to pay for all connections.

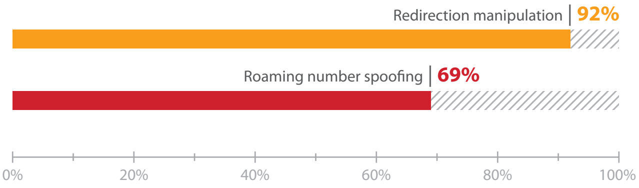

Figure 11. Percentage of successful attacks in order to redirect a terminating call by method

Each employed method was effective, and 92% of redirection manipulation attacks were successful. Threat realization is possible due to vulnerabilities related to the lack of location validation in a victim network. The Positive Technologies experts determined that this flaw is critical in the case of roaming number spoofing and medium in the case of redirection manipulation.

We were able to modify a subscriber's profile in half of the cases (54%) using the InsertSubscriberData message.

4.1.3. Operation Disruption

The research showed that the majority of the examined SS7 networks suffered from exploitable flaws that may lead to DoS. We attempted the UpdateLocation method in all of the testing and achieved an 80% success rate.

As a result, an attacker may cause disruption in network services for separate cell phone users without any impact — quality or access wise — for other subscribers. Thus, an adversary may conduct targeted attacks.

4.2. Common Threats for EMEA and APAC

We will not provide detailed statistics for both regions as this data may lead to reputational losses for some carriers and the sample is not large enough to make overall statements regarding the level of security of SS7 networks for specific areas. In this section, there are general results that demonstrate what attack types may be used against networks in both areas.

For example, DoS attacks had 100% success rate in EMEA and 71% in APAC countries.

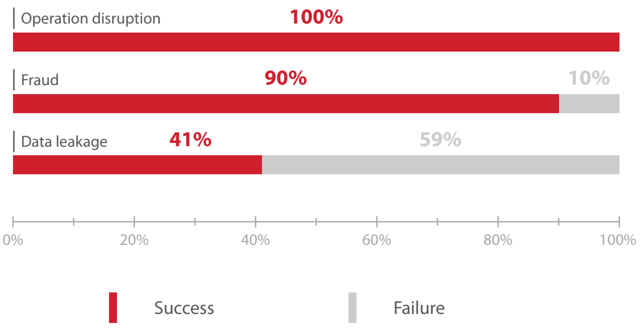

Figure 12. Percentage of successful attacks in EMEA

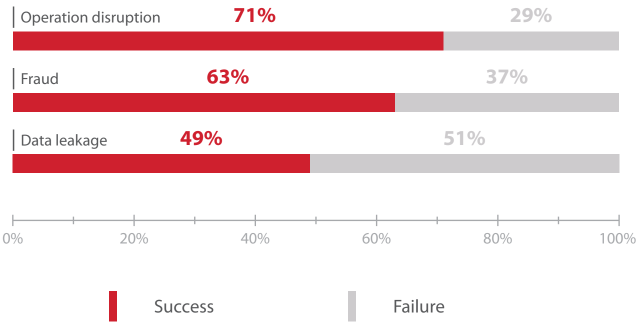

Figure 13. Percentage of successful attacks in APAC

This threat is critical for both regions, and may be exacerbated by the fact that carriers focus on building security against DoS targeting their SS7 networks and equipment, rather than the protection of individual subscribers.

The most critical threat here is fraud. Successful attack development may lead to reputational and financial losses, if, say, an attacker transfers money from a user's account. EMEA is especially vulnerable to almost every type of attack (90%).

Figure 14 demonstrates a percentage of successful attacks. An attack is considered successful if at least one attempt is achieved.

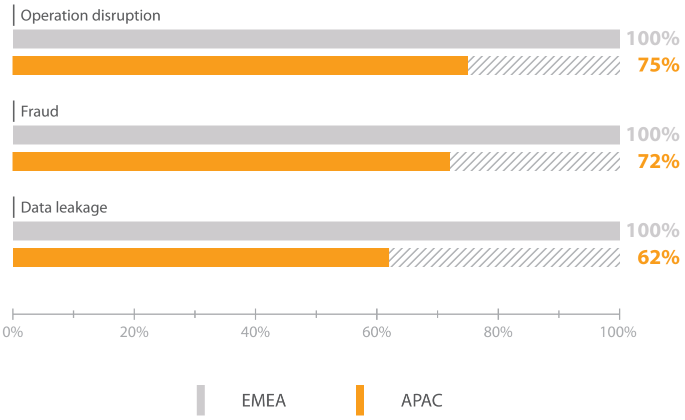

Figure 14. Percentage of successful attacks for each region

For example, data leakage attacks were successful in all EMEA networks for all subscribers, and for APAC, the rate is 75%.

This high rate might be biased by the smaller sample pool of EMEA networks. It is impossible to draw any general conclusions about all cellular carriers, however the research results confirm that a solution to SS7 security issues should be global to mitigate the existing risks. If an operator attempts to cover individual flaws, an attacker may use the combination of other methods to penetrate the network.

4.3. Threats for Operators by Subscriber Database

SS7 threat conclusions:

- Large operators pay more attention to network protection against all reviewed threat types.
- The larger subscriber database is, the less users are secured against fraud.
- The level of subscriber protection is insufficient in all the networks.

The results below might be driven by the ability of larger cellular carriers to fund and implement various mechanisms and systems that are dedicated to SS7 protection. The costs of such security measures are not always feasible for small operators. However, the percentage of successful attacks is so high that even market leaders cannot be considered safe.

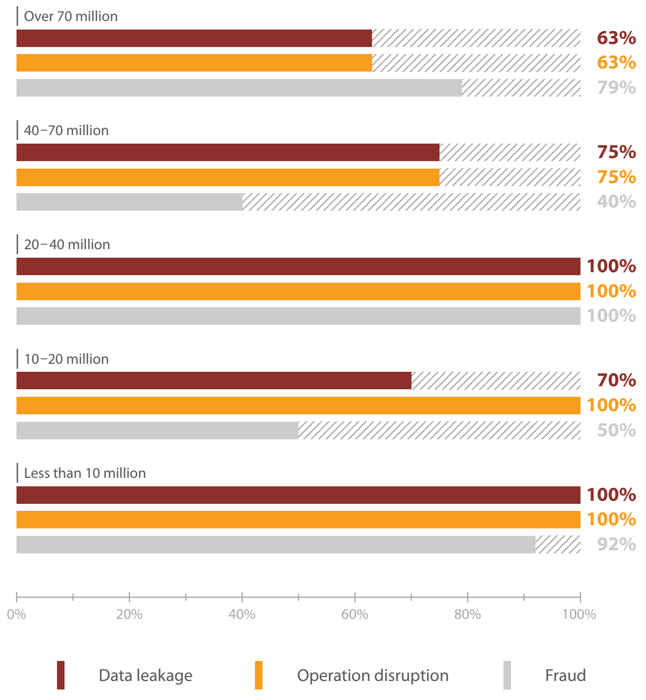

Figure 15. Percentage of successful attacks by carriers

4.4. Recommendations

Main protection mechanisms:

- Configuration settings
- Implementation of additional security means
- Combination of the two

The majority of flaws that allow an attacker to track a subscriber's location and steal data could be eliminated if we change network equipment configuration, and prohibit the processing of AnyTimeInterrogation and SendIMSI messages via HLR.

The way to fix architecture flaws in protocols and systems is to block undesired messages. A system must consider the filtering of SendRoutingInfoForSM, SendIMSI, SendRoutungInfoForLCS, and SendRoutingInfo. Filtering will help to avoid the risks of DoS, SMS interception, calls forwarding, subscriber's profile modification. Not all indicated SS7 messages are dangerous. Systems need to configure filtering to cut off only undesired messages used in attacks, and implement additional security tools, for example, intrusion detection systems. These systems do not interfere with network traffic and are capable of detecting malicious activity and its source as well as determining necessary configuration for message filtering.

The most effective way to counteract all of the identified types of attacks (including the ones that exploit software errors) is a combination of these methods.

The described options are most effective in cases where the mobile operator company has a regular and reliable set of procedures for the inner SS7 security audit. However most cellular carriers, especially small ones, struggle to support regular audit procedures. In such cases operators should use outsourcing options as this will help to determine the current level of their protection, uncover existing security threats, and minimize risks at hand by taking necessary actions to fix detected vulnerabilities.

Conclusion

The overall security level of the SS7 networks examined was below average. Every single network fell victim to attacks aimed at data leakage, network disruption, and fraudulent actions.

The research demonstrated that telecom companies employ various measures of protection but these are not enough to counteract all possible ways for attackers to penetrate the network. Even large operators are not protected against conversation tapping, messages monitoring, and fraudulent activity such as calls redirection and stealing. Additionally, hackers can pinpoint a subscriber's location at any given moment.

In order to reduce risks, operators should employ a global approach to SS7 protection. They should conduct regular security audits of the signaling network and develop appropriate measures to mitigate risk based on vulnerabilities as they evolve. Clearly all operators need to employ additional security measures to better address threats.

Abbreviations

GwSTP (Gateway Signaling Transfer Point) is a gateway host that routes signal messages.

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

MSC (Mobile Switching Center) is a specialized automatic telephone exchange.

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

SDK (Software Development Kit) a set of software development tools that allows the creation of applications.

VLR (Visitor Location Register) is a database that contains information about visiting subscribers.

Sources

1. Kurbatov, D., and S. Puzankov. 2014. Vulnerabilities of Mobile Networks Based on SS7 Protocols. http://www.ptsecurity.com/upload/ptcom/SS7_WP_A4.ENG.0036.01.DEC.28.2014.pdf

2. Kurbatov, D., S. Puzankov, and P. Novikov. 2014. Mobile Internet Vulnerabilities (GPRS). http://www.ptsecurity.com/upload/ptcom/Vulnerabilities_of_Mobile_Internet.pdf

3. Ostman, L. CellPoint Systems. 2001. A Study of Location-Based Services. http://epubl.ltu.se/1402-1617/2001/254/LTU-EX-01254-SE.pdf

4. Porter, T., and M. Gough. 2007. How to Cheat at VoIP Security. https://goo.gl/dxQfgs

5. Kolker, R. Bloomberg Businessweek. 2016. What Happens When the Surveillance State Becomes an Affordable Gadget? http://goo.gl/weqptW

6. Coulthart, R. 2015. Special Investigation: Bugged, Tracked, Hacked. http://www.9jumpin.com.au/show/60minutes/stories/2015/august/phone-hacking/

7. Schneier, B. Schneier on Security. 2015. SS7 Phone-Switch Flaw Enabled Surveillance. https://www.schneier.com/blog/archives/2015/08/ss7_phone-switc.html

8. Soltani, A., and B. Gellman. The Washington Post. 2013. New Documents Show How the NSA Infers Relationships Based on Mobile Location Data. https://goo.gl/cCmlzn

9. Engel, T. Locating Mobile Phones Using Signalling System #7. https://events.ccc.de/congress/2008/Fahrplan/attachments/1262_25c3-locating-mobile-phones.pdf

10. McDaid, C. 2015. Can They Hear You Now? Hacking Team & SS7. http://www.adaptivemobile.com/blog/can-they-hear-you-now-hacking-team-ss7

11. Unblocking Stolen Mobile Devices Using SS7-MAP Vulnerabilities. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7345408

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

pt@ptsecurity.com ptsecurity.com