Stealthy SS7 Attacks

Sergey Puzankov

Positive Technologies, Russia
E-mail: spuzankov@ptsecurity.com

Received 8 September 2017;
Accepted 10 October 2017

Abstract

As we can see, most mobile operators defend their SS7 perimeter by reconfiguring network equipment and implementing SMS Home Routing solutions. This is the right way to withstand basic SS7 attacks, but it is not enough to protect the network. Our research and security audit practice proves that there are possibilities to perform SS7 attacks that bypass this kind of security mechanisms. Moreover, real attacks tend to be more stealthy and difficult to detect at an early stage. That is why we reckon mobile operators should engage continuous security monitoring of external SS7 connections supported by up-to-date vulnerability base. In this talk, I will describe the most interesting attacks on SS7 networks that have never been published before.

Keywords: SS7, Security, Location tracking, SMS interception.

1 Introduction

The "walled garden" paradigm is outdated. Nearly all operators now admit that attackers have penetrated SS7 (Signaling System 7) networks by exploiting a whole range of signaling network vulnerabilities.

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

Journal of ICT, Vol. 5_1, 39–52.
doi: 10.13052/jicts2245-800X.512

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 (Common Channel Signaling System 7), which dates to the 1970s, is riddled with security vulnerabilities like the absence of encryption or service message validation. For a long time, it did not 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 [7]. In 2015, Berlin hackers from SR Lab were able to intercept SMS (Short Message Service) 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 [4].

Experts discovered these flaws a number of years ago—Lennart Ostman reported SS7 issues in 2001 [1], and the US government expressed their concern about the problem in 2000 [2]. In 2013, Edward Snowden identified SS7 exploitation as one of the techniques used by the National Security Agency [6]. According to Bloomberg [3], 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 415 GB of data from their servers leaked online [8]. The British company Cobham provides location discovery service with up to a meter precision to more than a dozen countries, says Bruce Schneier [5], indicating that the SS7-based spying market is rapidly growing.

Tracking subscriber location, obtaining call details, tapping, intercepting text messages that contain security codes are the harsh reality we live in. However, mobile operators do not sit back. They address these threats by configuring hardware in the best possible way, deploying SMS Home Routing solutions to protect confidential data and fight SMS spam and SS7 firewalls, which currently offer the highest level of network protection against attackers.

2 Old Technology, New Vulnerabilities

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 services, send a USSD (Unstructured Supplementary Service Data) command to a billable number, and conduct other attacks.

It is 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 (Gateway GPRS (General Packet Service Radio) Support Node), or a femtocell.

SS7 attacks may be performed from anywhere and an attacker does not have to be in physical proximity to a subscriber, so it is 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 (Mobile Application Part) commands allow cell phones to be blocked from a distance [9]. Issues with SS7 security threaten not only mobile subscribers but also a growing ecosystem of industrial and IoT (Internet of Things) devices—from ATMs (Automated Teller Machine) to GSM (Global System for Mobile communications) 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.

Protection of the SS7 perimeter against attacks has become a security trend among mobile operators in the past few years. Many mobile operators reconfigure network equipment with security in mind and implement SMS Home Routing solutions, some of them implement SS7 firewalls. This is the right way to withstand basic SS7 attacks, but it is not enough to protect the network in full. Our research and security assessments show that there are possibilities to perform SS7 attacks that bypass this kind of security mechanisms. Real attacks tend to be quieter and stealthier, so it is difficult

to notice them at an early stage. That is why we believe that mobile operators should engage continuous security monitoring of external SS7 connections supported by an up-to-date vulnerability base.

3 Description of Stealthy SS7 Attacks

3.1 SMS Home Routing Bypass

A malefactor can easily bypass most security systems if they have configuration mistakes that are not evident at first sight.

Some operators believe that if they have implemented SMS Home Routing solution and configured core equipment to block Category 1 messages, it would be impossible for an intruder to obtain IMSI (International Mobile Subscriber Identity) and perform more dangerous attacks from the SS7 network. 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. Category 1 contains all the SS7 messages, which should normally only be received from within the same network and not on interconnect links from other networks, unless there is an explicit agreement to do so.

IMSI is considered confidential data because it is used to address subscribers in a majority of operations. An attacker can conduct more sophisticated attacks exploiting a retrieved IMSI. Sometimes, the IMSI is the attacker's final target. For example, banks use IMSIs to authenticate SIM (Subscriber Identity Module) cards. They can buy information about IMSIs either from operators or from third-party service providers that disclose IMSI values via SS7 vulnerabilities.

However, we should remember about the STP (Signaling Transfer Point) node that receives external signaling traffic. The STP contains many routing rules for signaling traffic, for example, routing a SendRoutingInfoForSM message to an SMS Router. Apart from that, the STP should process addresses of different numbering plans. For example, an UpdateLocation message should be routed to the appropriate HLR (Home Location Register) based on the address in the E.214 numbering plan.

Telecom standards have several numbering plans for signaling messages routing. The most frequently used of them have codes: E.164, E.212, E.214.

The E.164 is an ITU-T recommendation, which defines the international public telecommunication numbering plan used in the PSTN (Public Switched Telephone Network) and some other data networks. It also defines the format

of telephone numbers. E.164 numbers can have a maximum of 15 digits. All the global title addresses and mobile numbers that we use for calling are in this format.

The format of the E.164 address is as the following:

CC (Country Code) + NDC (Network Destination Code) + SN (Subscriber Number).

For example, CC of Finland is 358, NDC of a Finish operator is 98. SN can be any unique number, here I used some random digits 1234567.

So the number is 358 98 1234567.

IMSI stands for International Mobile Subscriber Identity. It conforms to the ITU (International Telecommunication Union) E.212 numbering standard and is a unique identification associated with all GSM, UMTS (Universal Mobile Telecommunications System), and LTE (Long Term Evolution) network users. It is stored on the SIM card and is sent to the network for a mobile equipment identification. The IMSI identifier helps the network to identify the subscriber and provide all the required services. The E.212 number can have a maximum of 15 digits.

The format of the E.212 address is as the following:

MCC (Mobile Country Code) + MNC (Mobile Network Node) + MSIN (Mobile Station Identification Number).

For example, MCC of Finland is 244, MNC of a Finish operator is 20. MSIN can be any unique number, here I also used random digits 3344556677.

Therefore, the IMSI is 244203344556677.

The E.214 is a numbering plan used for delivering mobility management related messages in GSM and UMTS networks. The E.214 number is derived from the IMSI. The E.214 number is composed of two parts. The first part is the combination of CC and NDC of a destination network. The second part of the number is the MSIN of the IMSI, which identifies an individual subscriber.

For example, for the IMSI 244203344556677, the corresponding E.214 number is formed by replacing MCC (244) with CC (358) and MNC (20) with NDC (98), and keeping MSIN as it is. The IMSI 244203344556677 translated to the E.214 numbering plan becomes 358983344556677.

The SS7 network uses the new prefix 35898 to enable the signaling message to reach the destination network. The destination network uses the MSIN 3344556677 to enable the signaling message to reach the appropriate HLR.

The E.214 numbering plan is usually used at subscriber authentication and registration under a new MSC (Mobile Switching Centre). Commonly, the new MSC does not usually have information about the new subscriber. Since the

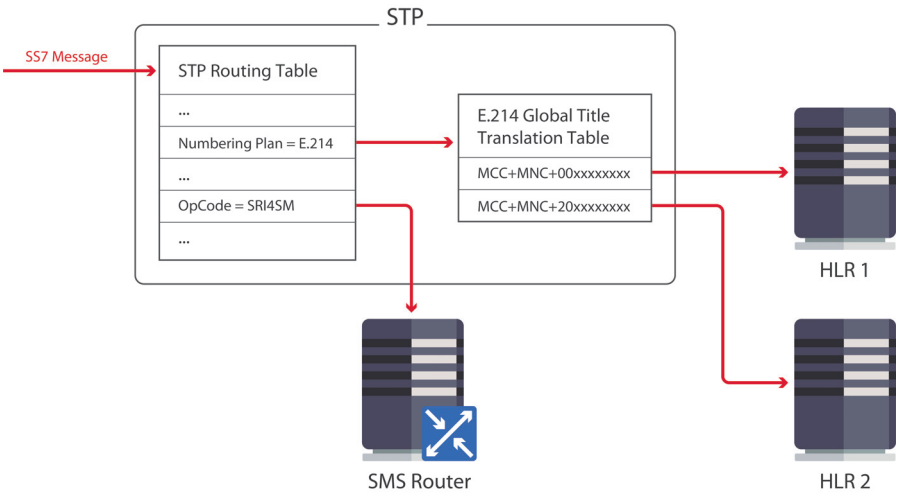

Figure 1 STP Routing misconfiguration.

IMSI identifier is located on the SIM card, the mobile phone sends the IMSI to the network via radio interface. Then the network transforms the IMSI of the E.212 numbering plan to the E.214 numbering plan and uses the new compiled number for routing SS7 messages of authentication and registration, such as SendAuthenticationInfo and UpdateLocation, to the destination network.

If the routing rule in the STP disregards an operation code for messages processed under the E.214, a malefactor could benefit from this misconfiguration and send the SendRoutingInfoForSM message addressing it in the E.214 (see Figure 1). Although digits of the E.214 must correlate with the IMSI, they can be bruteforced easily: any IMSI stored in the same HLR is enough.

As we can see, the SMS Home Routing solution may be useless if there are errors in the border STP configuration.

3.2 Positioning Enhancement During Location Tracking

One of the most popular attacks on SS7 networks is location tracking. A request for subscriber location is sent via SS7 networks, the response includes the base station identity. Each base station has specific geographic coordinates and covers a particular area. Because of urban density, the coverage area in a city ranges from tens to hundreds of meters.

An attacker can make use of these mobile network peculiarities to generate location requests, as well as to locate the base station by its identity using

a variety of publicly available Internet resources. Accuracy of the location discovery depends on the base station coverage area. Actually, the malefactor determines the position of the base station that serves the subscriber at the moment. However, our investigations show that intruders have learned to determine the subscriber location with better accuracy.

A mobile device usually receives signals from several base stations. If the malefactor determines coordinates of two or three base stations nearest to the subscriber, the subscriber location can be narrowed down.

Normally, a mobile device chooses a base station with the best radio conditions during a transaction. Therefore, the mobile device should interchange signals with the network. The malefactor can use a so-called silent SMS to initiate a hidden transaction with the target subscriber. However, the information about these messages is available in the subscriber's account. A more effective way to hide a transaction is to use silent USSD notifications. Although such transactions are not registered by the billing system, they initiate signal exchange between the mobile device and network. The malefactor can improve location accuracy manipulating base station identifications and silent USSD notifications (see Figure 2).

First, the intruder requests the identifier of the current base station (see Step 1 in Figure 2). Then the intruder sends a silent USSD notification (see Step 2 in Figure 2) in order to force the subscriber's equipment to carry out a transaction via radio interface (see Step 3 in Figure 2). If the malefactor gets

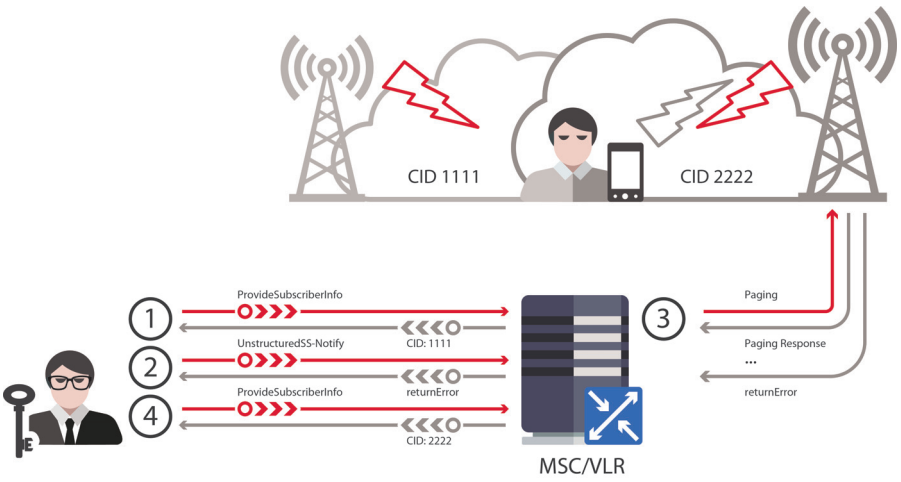

Figure 2 Positioning enhancement.

lucky, the network may choose a new base station for this transaction, and the VLR (Visitor Location Register) database updates the subscriber location. After that, the intruder requests the subscriber location once again and receives the identifier of the new base station (see Step 4 in Figure 2). Thus, the intruder can narrow down the area where the subscriber is located at the moment.

3.3 Invisible Interception of Short Messages

Short message interception is one of the most dangerous attacks on SS7 networks. Many services still use SMS as a trusted channel. For example, banks use SMS for OTP (One Time Password) delivery, social networks—for password recovery, messengers—for access to the application.

In order to intercept an incoming SMS, the intruder must register a subscriber in a "fake" network using the necessary equipment. The attack simulates a subscriber being in roaming in a visited network. The HLR gets a record of the subscriber's new location where terminating calls and SMS messages are routed. In case of an originating call, the first attempt fails, as the network registers the subscriber back in its home network. The attacker sees it and can repeat the attack to make the next call attempt fail.

Moreover, if the attackers control the network element, which is indicated as a new MSC, they can intercept terminating SMS messages and redirect terminating voice calls.

As soon as the registration is finished, all incoming SMSs are routed to the network element indicated as MSC and VLR in the UpdateLocation signaling message. The attacked subscriber may return to the home network as soon as one of following events is triggered:

- Outgoing call;
- Outgoing SMS;
- Moving to the area covered by another mobile switch;
- Mobile phone restart.

From the attacker's point of view, keeping the subscriber registered in the "fake" network is unreliable because it is impossible to predict all actions of the subscriber.

The malefactor can register the subscriber in the "fake" network spoofing the MSC address only, keeping the real VLR address (see Step 1 in Figure 3). The attack simulates a subscriber registered in another network so that the current MSC/VLR is used for voice calls and originating SMS messages

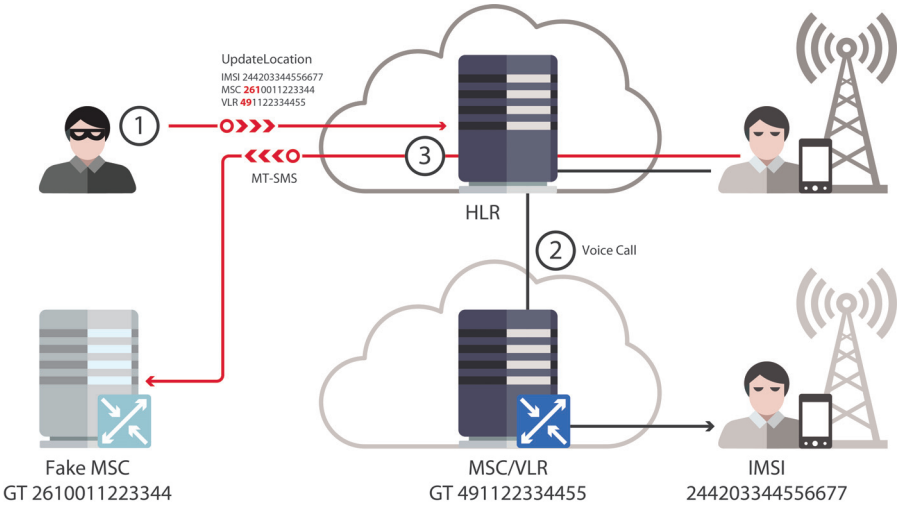

Figure 3 SMS interception attack.

(see Step 2 in Figure 3), and a fake MSC is used to receive terminating SMS messages (see Step 3 in Figure 3).

The attackers can use this to attack services of other companies (for example, bank accounts) that use SMS as a channel to inform clients of any changes. If the intruder controls the network element, which is indicated as a new MSC, they can intercept terminating SMS messages sent by services like mobile banking, password recovery for Internet services, getting access codes for messengers, etc.

These manipulations do not prevent the attacked subscriber from making originating calls and sending SMSs, but incoming SMSs go to the spoofed MSC address.

Moreover, this vulnerability is well known, and all SS7 firewall vendors try blocking registration in "fake" networks. Usually, the blocking mechanism in an SS7 firewall relies on its own database that contains current subscribers' locations. Apart from that, an SS7 firewall should have a velocity table reflecting approximate time to reach any country. For example, the velocity between two German networks is zero; the velocity between Germany and Madagascar is 8, which is the approximate duration of a direct flight, and so on.

When an UpdateLocation message is received by the network, the SS7 firewall extracts the following information from it: the subscriber's identifier IMSI (see Step 1 in Figure 4) and the address of a new VLR, prefix of which

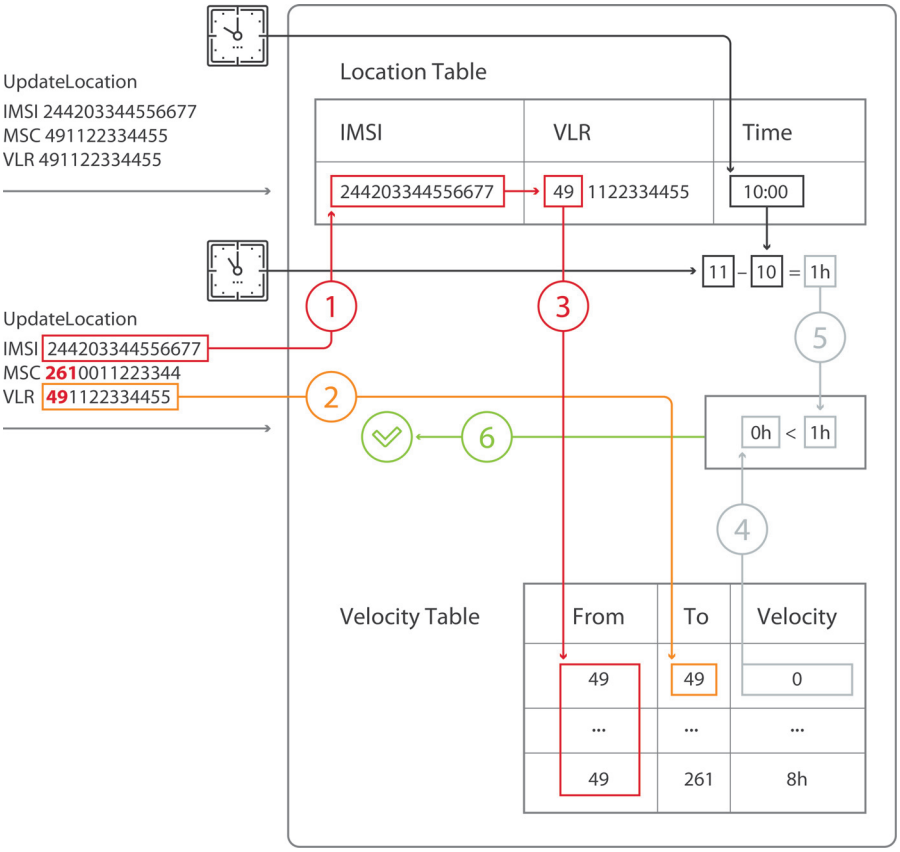

Figure 4 SS7 firewall bypass.

will be later used as a key to find the velocity value (see Step 2 in Figure 4). After that, the SS7 firewall looks for the latest location of a subscriber in the database. The SS7 firewall takes the previous VLR prefix (see Step 3 in Figure 4) and uses it as the second key to define the velocity value (see Step 4 in Figure 4); and then calculates a time shift between the current time and the time of previous registration (see Step 5 in Figure 4). If the time shift is shorter than the velocity value, the UpdateLocation message is regarded as hostile and should be blocked. Otherwise, the UpdateLocation message should be permitted (see Step 6 in Figure 4).

In order to bypass such a protective mechanism, the malefactor can register the subscriber in the "fake" network spoofing the MSC address only, keeping

the real VLR address. So the check of the VLR address only is not enough to decide if the traffic must be blocked.

Thus, registration with spoofed MSC and real VLR addresses is more reliable for an intruder and helps bypassing some SS7 firewalls with simple rules.

As we can see now, some of SS7 firewalls are not reliable protection tools, despite of the fact that the attack signature is quite simple.

4 Security Management Process

In order to reduce risks from external connections, 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.

First, the operator needs to know if its network is vulnerable to signaling attacks. After the relevant assessment, the operator obtains information about weak chains and has a clear view of what and how should be changed to improve security.

Then the operator has to monitor external SS7 connections in order to detect malicious and suspicious signaling traffic. As soon as the operator sees unauthorized activity originating from the SS7 network, it has to decide which measures should be taken to prevent it.

The following measures can be taken:

- Sending a note to the operator that generates unauthorized activity. This is the easiest and quickest way to stop bad Provide foundations for the penetration of signaling traffic;
- Blocking the hostile GT (Global Title). But first, the operator must make sure that the blocking does not affect the operator's services.

Configure the core equipment to ensure security.

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

Clearly, all operators need to employ additional security measures to better address threats.

References

[1] Ostman, L. (2001). *A Study of Location-Based Services. Cell Point Systems.* Available at: https://www.opencolleges.edu.au/informed/teacher-resources/style-guide-resources-mla-apa-cse-chicago/
[2] Porter, T., and Gough, M. (2007). *How to Cheat at VoIP Security (2007)*. Available at: https://goo.gl/dxQfgs
[3] Kolker, R. (2016). *What Happens When the Surveillance State Becomes an Affordable Gadget? Bloomberg Businessweek.* Available at: http://goo.gl/weqptW
[4] Coulthart, R. (2015). *Special Investigation: Bugged, Tracked, Hacked*. Available at: https://goo.gl/m9V1NK
[5] Schneier, B. (2015). *SS7 Phone-Switch Flaw Enabled Surveillance. Schneier on Security*. Available at: https://www.schneier.com/blog/archives/2015/08/ss7_phone-switc.html
[6] Soltani, A., and Gellman, B. (2013). *New Documents Show How the NSA Infers Relationships Based on Mobile Location Data. The Washington Post.* Available at: https://goo.gl/cCmIzn
[7] Engel, T. (2008). *Locating Mobile Phones Using Signalling System #7*. https://berlin.ccc.de/∼tobias/25c3-locating-mobile-phones.pdf
[8] McDaid, C. (2015). *Can They Hear You Now? Hacking Team & SS7*. Available at: http://www.adaptivemobile.com/blog/can-they-hear-you-now-hacking-team-ss7
[9] Rao, S., Holtmanns, S., Oliver, I., and Aura, T. (2015). *Unblocking Stolen Mobile Devices Using SS7-MAP*. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7345408

Biography

Sergey Puzankov is a Telecom Security Expert, Positive Technologies. Sergey was born in 1976. He graduated from Penza State University with a degree in automated data processing and management systems in 1998.

Before joining Positive Technologies in 2012, he worked as a quality engineer at VimpelCom. Being a security expert in telecommunication systems at Positive Technologies, he is engaged in the research of signaling network security and in audits for international mobile operators.

He is part of the team that revealed vulnerable points in popular two-factor authentication schemes using texts and demonstrated how easy it is to compromise Facebook, WhatsApp, and Telegram accounts. As an expert in telecom security, he researches signaling network security and participates in audits for international mobile operators.

Sergey is also the general developer of the SS7 Vulnerability Scanner tool and member of the Telecom Attack Discovery development team and co-author of Positive Technologies annual reports on telecom security.