SigPloit: A New Signaling Exploitation Framework

Loay Abdelrazek
School of Communication and Information Technology
Nile University
Cairo, Egypt
l.hassan@nu.edu.eg

Marianne A. Azer
National Telecommunication Institute
Nile University
Cairo, Egypt
mazer@nu.edu.eg

***Abstract*— Mobile communication networks are using signaling protocols to allow mobile users to communicate using short messages, phone calls and mobile data. Signaling protocols are also used to manage billing for operators and much more. The design flaws that signaling inherits made them vulnerable to attacks such as location tracking of subscriber, fraud, calls and SMS interception. With the high rate of these emerging attacks on telecommunication protocols there is a need to create a comprehensive penetration testing framework for signaling. In this paper, we propose a framework called Sigploit that takes into consideration the following protocols: SS7, GTP, Diameter and SIP.**

Keywords— Fraud; GTP; Interception; SS7; Signaling; Tracking; Telecom; User Privacy;

I. Introduction

System Signaling no.7, best known as SS7, is a protocol suite that was first invented in the 70s by Bell Systems initially for the land-line telecommunications companies aiming to separate signal channel from voice channels in order to make more use of the bandwidth to enhance voice quality. With [1] the emergence of mobile companies and technologies starting with the 2G, inter-compatibility was an issue. Mobile companies adopted the same signaling protocol to handle signaling for their own infrastructure and exchanged communication between mobile and land-line technologies. SS7 is only used when mobile subscriber is in an idle status or performing mobile related operations. It is not only used to setup and release calls, but also for a variety of other mobile related operations including: Supplementary services, SMSs, cellular mobility management and roaming, charging and other more [2]. The security of the SS7 protocol was not taken into consideration in the protocol design, the security was solely based on the mutual trust between the interconnecting operators. SS7 was regarded to as the telecommunication wall that is only enclosed to those whom provide the service. This is not valid anymore and there is an urgent need to pay more attention to the implementation of the protocol and analysis of the security gaps in those networks.

There are online free tracking public services [3] that rely on the SS7 protocol and exploit the fact that the operators lack the security towards one of the most critical messages which is in most cases SendRoutingInfoForSM, used in locating a subscriber prior sending an SMS. These public services have also included the ability to retrieve the International Mobile Subscriber Identity (IMSI). Various researches have shown how the SS7 messages could be abused to intercept and track targets [5]. GSM Association (GSMA) has also highlighted the critical SS7 messages that must be filtered [15]. However, many operators have not yet filtered these messages, leaving them a prey to the online public services and yet for remote attackers [4] [6].

The myth of two way factor authentication, 2FA that is supposed to provide an extra layer of security was recently busted with an attack on a German mobile operator. Attackers took advantage of SS7 vulnerability to intercept the 2FA tokens sent via SMS for the target's bank accounts, leading to draining the accounts and transferring money to attackers [7].

This paper proposes an exploitation framework, not only for SS7 but also for GTP, SIP and Diameter. SigPloit's architecture and development is explained in details. The contribution of SigPloit and a comparison with other tools is highlighted as well.

The remainder of this paper is organized as follows Section II introduces the SS7 network architecture and its critical components that are subject to the attacks.

978-1-5386-4646-5/18/$31.00 ©2018 IEEE

Section III presents several types of attacks, the way are conducted and their impact. Section IV presents the contribution and the compariosn between SigPloit and current available tools. Finally, conclusions and future work are presented in section V.

II. SS7 Architecture

This section presents the SS7 architecture. Section A presents the network architecture and the critical components subject to attacks, while section B presents the addressing scheme used in a mobile operator.

A. Network Architecture

SS7 is used within the core of the operator's infrastructure and the international interconnects between roaming partners. Therefore, the main threat vector comes from the external networks that are communicating with the home network over the interconnects.

This section discusses the critical components and their role in the network, to highlight the critical information they hold and how severe the attack's impact could be.

The Home Location Register (HLR) is the subscriber's database in the home network. Each subscriber is stored in only one HLR; the operator may have more than one depending on number of subscribers. The HLR is responsible of holding the following information:

(1) User identification (IMSI) and Numbering (MSISDN).

(2) User security information: Network access control information for authentication and authorization (K_i, K_c).

(3) User location information: Mobile switching center/visitor location register (MSC/VLR), that a user is currently attached to, as well as cell ID.

(4) User profile information: Services that the user is subscribed to. For instance call forwarding, current balance,.. etc. The HLR also generates user security information for mutual authentication, communication integrity check and ciphering [8].

The Mobile Switching Center (MSC) performs all the necessary functions in order to handle the circuit switched services to and from the mobile stations. MSC is an exchange which performs all the switching and signaling functions for mobile stations located in a geographical area designated as the MSC area. The main function of MSC is to switch and deliver user data (voice, sms and data) to the user. The current serving MSC is stored in the HLR.

The Visitor Location Register (VLR) is a temporary database that is mostly physically on the same node as the MSC. The VLR holds a subset of information stored in the HLR described as follows: IMSI, MSISDN, Mobile Station Roaming Number (MSRN), location area where the mobile has been registered(Cell ID), and other more.

The Short Message Service Center (SMSC) is the node responsible to deliver and queue the short messages (SMS) to and from the subscribers.

Fig. 1 [4] depicts the typical network architecture for handling calls and SMS and presents how two operators are connected through SS7 interconnects for roaming operations.

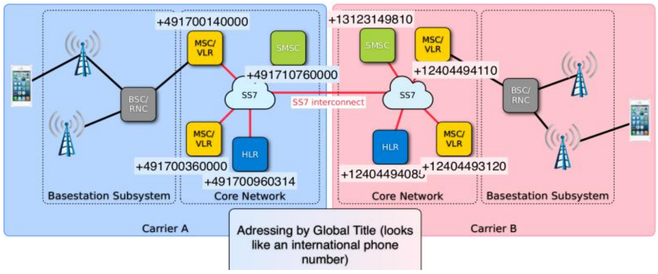


Fig.1 SS7 Network Architecture [4]

B. Addressing

Addressing and routing in mobile networks rely on two main unique addresses: Global Title (GT) and Sub System Number (SSN).

Every node in the core network of an operator is assigned a GT. The GT is the counterpart of the public IP address in the TCP/IP suite. Communication between two distant nodes of roaming partners occurs with the GT which could be found in the Signaling Connection Control Part (SCCP) layer in the SS7 packet. It is used for routing the SS7 messages between the nodes. GT has the same international format of the MSISDN, with the below structure, as show in Fig. 2 [9].

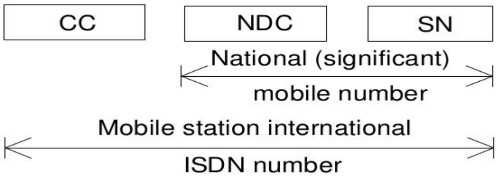


Fig.2 MSISDN Structure [9]

For example, in the number +201012345678, the CC represents the country code varying from 2-3 digits (+20), NDC represents the national destination code (a.k.a operator code (10) and lastly SN which represents the Subscriber Number (12345678).

The components described earlier could be treated as layer 7 applications in TCP/IP networks; each is identified by a constant SSN. For example, in TCP/IP HTTP is defined as being server port number 80, the same mapped to mobile networks MSC is served on SSN 8. SSN helps to identify and deliver the SS7 message to the correct node.

IV. Exploiting the SS7

The GSM Association (GSMA) has categorized the SS7 messages into 5 categories based on the following criteria [10]:

CAT1: Message that are only allowed within the core network of the home network.

CAT2: Message that are allowed from the roaming partners towards their inbound roamers in the home network.

CAT3: Messages that must be allowed between operators and cannot be filtered.

CAT4: Messages that are related to SMS operations.

CAT5: CAMEL related messages.

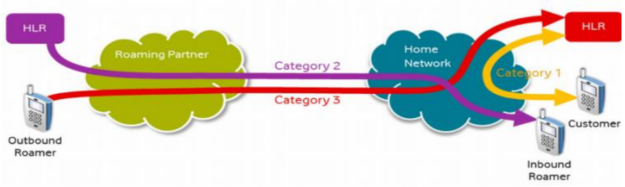


Fig.3 SS7 Messages Categories [10]

The SS7 messages categories are shown in Fig. 3 [10]. In this section, we present the different vulnerabilities, and attack scenarios. We also explore the threats to each message category.

A. Location Tracking

The main goal of this attack is to determine the exact location of the target. Determining the accuracy of the location returned depends fairly on the SS7 message that has been initially used. The location retrieved may vary between the MSC that the subscriber is attached to and Cell ID. In the following, we present example of messages that can be used to achieve this type of attack.

Message 1: SendRoutingInfo(opcode==22)

SRI message is considered as CAT1 message that should be filtered/dropped by the home network operator from any GT source other than its own. The legitimate flow of this message is used internally between the Gateway MSC (GMSC) and the HLR. When terminating a phone call, it is required to determine the current location of the subscriber to successfully route the incoming call. The most important returned location value that is used to terminate a call is the current visiting MSC. it is responsible afterwards to switch the call and deliver it to the correct cell where the subscriber currently resides. Moreover the HLR returns a surplus amount of location information and other information that could be used in further attacks. This attack only requires the target's phone number to be initiated.

Information returned is not limited to the following:

[MSC GT, Cell ID, (LAT, Long), IMSI, IMEI, Allowed Services] and much more.

An open source public cell ID database online could further be used to exactly determine the location of a user on the map. The IMEI returned determines the exact type of handset the subscriber has. This information in turn could develop a targeted malware for this specific type of handset. The IMSI could be used to trigger further attacks that will be discussed later. Fig.4 depicts the traffic flow of a location tracking attack using SRI message.

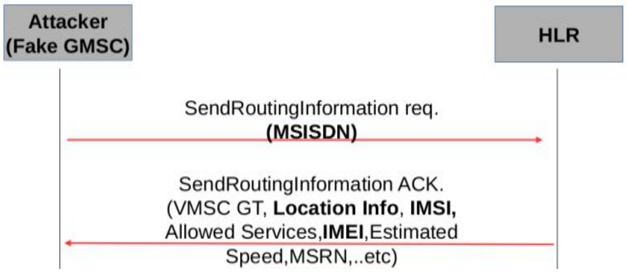

Attacker (Fake GMSC)
HLR
SendRoutingInformation req. (MSISDN)
SendRoutingInformation ACK. (VMSC GT, Location Info, IMSI, Allowed Services,IMEI,Estimated Speed,MSRN,..etc)

Fig.4 SRI Location Tracking

B. Interception

The main goal of this attack is to intercept any terminating or originating communication to the mobile subscriber. The message used in interception depends on the traffic direction. Techniques for intercepting terminating traffic differs from intercepting originating traffic from the mobile subscriber. The following describes how a mobile terminated SMS is performed.

Message: UpdateLocation(opcode==2)

UL is classified as a category 3 message. All category 3 messages are to be allowed by the operators as they provide the essential operations for mobility.

The legitimate flow of this message is used when a subscriber performs an intra/inter roaming. The subscribers update their new VLR that they are attached to, in order for the home network to route all the traffic of the subscribers towards the new MSC.

A malicious attacker could advertise a new fake location using the IMSI, which the home network must store to enable subscriber's communication and mobility. Subsequently, any SMS or call terminating to the subscriber will pass through the new node under the control of the attacker that has been updated successfully in the subscriber's home network. The full man-in-the middle attack scenario described is shown in Fig. 7.

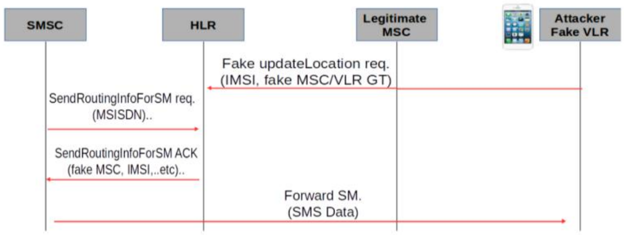
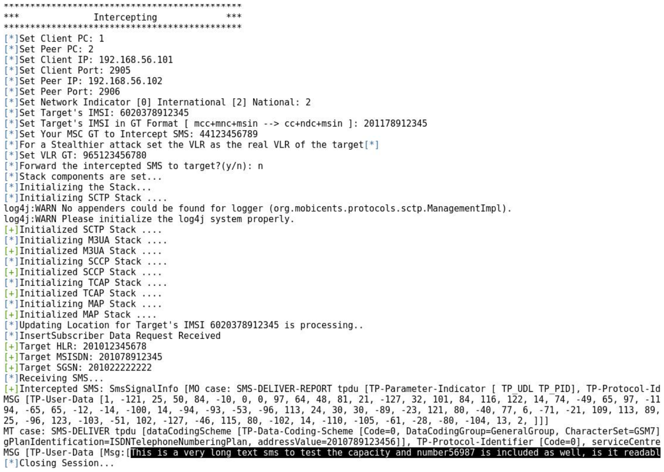


Fig.7 UL SMS Interception

Fig.8 presents a simulation of the SMS interception attack using UL message in SigPloit. When the UL message is received by the target HLR, it responds back with InsertSubscriberData (ISD) message which includes the profile of the subscriber. SigPloit parses some important parameters of this message that could be later used in other attacks. An example of these parameters are the subscriber's HLR GT, the current Serving GPRS Support node and other information like the subscribed services. After sending back the ISD ack packet to the target HLR, the terminating SMS is delivered to SigPloit and the intercepted SMS is shown on the terminal. In this simulation the intercepted SMS is "This is a very long text sms to test the capacity and number 56987 is included".



```
*********************************************
***              Intercepting           ***
*********************************************
[*]Set Client PC: 1
[*]Set Peer PC: 2
[*]Set Client IP: 192.168.56.101
[*]Set Client Port: 2905
[*]Set Peer IP: 192.168.56.102
[*]Set Peer Port: 2906
[*]Set Network Indicator [0] International [2] National: 2
[*]Set Target's IMSI: 6020378912345
[*]Set Target's IMSI in GT Format [ mcc+mnc+msin --> cc+ndc+msin ]: 201178912345
[*]Set Your MSC GT to Intercept SMS: 44123456789
[*]For a Stealthier attack set the VLR as the real VLR of the target[*]
[*]Set VLR GT: 965123456780
[*]Forward the intercepted SMS to target?(y/n): n
[*]Stack components are set...
[*]Initializing the Stack...
[*]Initializing SCTP Stack ....
log4j:WARN No appenders could be found for logger (org.mobicents.protocols.sctp.ManagementImpl).
log4j:WARN Please initialize the log4j system properly.
[+]Initialized SCTP Stack ....
[*]Initializing M3UA Stack ....
[+]Initialized M3UA Stack ....
[*]Initializing SCCP Stack ....
[+]Initialized SCCP Stack ....
[*]Initializing TCAP Stack ....
[+]Initialized TCAP Stack ....
[*]Initializing MAP Stack ....
[+]Initialized MAP Stack ....
[*]Updating Location for Target's IMSI 6020378912345 is processing..
[*]InsertSubscriber Data Request Received
[+]Target HLR: 201012345678
[+]Target MSISDN: 201078912345
[+]Target SGSN: 201022222222
[*]Receiving SMS...
[+]Intercepted SMS: SmsSignalInfo [MO case: SMS-DELIVER-REPORT tpdu [TP-Parameter-Indicator [ TP_UDL TP_PID], TP-Protocol-Id
MSG [TP-User-Data [1, -121, 25, 50, 84, -10, 0, 0, 97, 64, 48, 81, 21, -127, 32, 101, 84, 116, 122, 14, 74, -49, 65, 97, -11
94, -65, 65, -12, -14, -100, 14, -94, -93, -53, -96, 113, 24, 30, 30, -89, -23, 121, 80, -40, 77, 6, -71, -21, 109, 113, 89,
25, -96, 123, -103, -51, 102, -127, -46, 115, 80, -102, 14, -110, -105, -61, -28, -80, -104, 13, 2, ]]]
MT case: SMS-DELIVER tpdu [dataCodingScheme [TP-Data-Coding-Scheme [Code=0, DataCodingGroup=GeneralGroup, CharacterSet=GSM7]
gPlanIdentification=ISDNTelephoneNumberingPlan, addressValue=2010789123456]], TP-Protocol-Identifier [Code=0], serviceCentre
MSG [TP-User-Data [Msg:[This is a very long text sms to test the capacity and number56987 is included as well, is it readabl
[*]Closing Session...
```

Fig.8 SigPloit's SMS Interception

IV. SigPloit's Contribution

In this section, we present the effort done in the literature to assess SS7 as well as our proposed framework. Earlier methods and our proposed framework SigPloit are presented in sections A and B respectively.

A. *Earlier Projects*

Two projects were introduced to the open source community in this domain. ss7MAPer [11] by Daniel Mende from ERNW research team, and SafeSeven [12] by Akib Sayed. Both tools added a great value to the community.

In ss7MAPer toolkit is built upon the Osmocom SS7 [13] stack using Erlang as its programming language and implements some MAP messages. It has tests against the HLR, VLR, MSC and SMSC. It aims to test the secure configuration of the internal and external SS7 network access. What is remarkable about this tool that it has a binary release that supports windows not only Linux making it available to everyone and every environment, there is also a Docker image running on Ubuntu 16.04.

SafeSeven [12] built by Akib Sayed, based on Mobicents SS7 stack, does the tests related to HLR, VLR, SGSN, MSC. This tool has a splendid dashboard, giving a great user experience along with statistical view on the running tests.

B. *SigPloit*

The highlighted restrictions of ss7Mapper [11] and safeseven [12] were the motive for us to develop SigPloit [14] and introduce to mobile operators and security researchers. SigPloit has been noticed globally and referenced in the GSMA FS.07 standard [15] as a reliable penetration testing tool. SigPloit added a new flavor to the arsenal of penetration testers in the domain of telecommunications security. Its intent is to provide a Metasploit like experience, trying to provide a smooth transition from IT domain, for those with an intense IT background, to the Telecommunications domain in order to grasp the concepts easily.

1) *Architecture*

The framework is structured as python modules. Each protocol included in the tool has its own main module. In return the modules include the logic and functions that call on the payloads of each attack. Fig. 9 depicts the current components and building blocks of SigPloit.

The core is sigploit which currently handles requests from the command line interface. Subsequently, the core has linkages to all protocol's modules, each protocol module is then linked independently to its attacks module and its payloads. SS7 protocol module for example, it is linked only to 5 attack modules, which are:

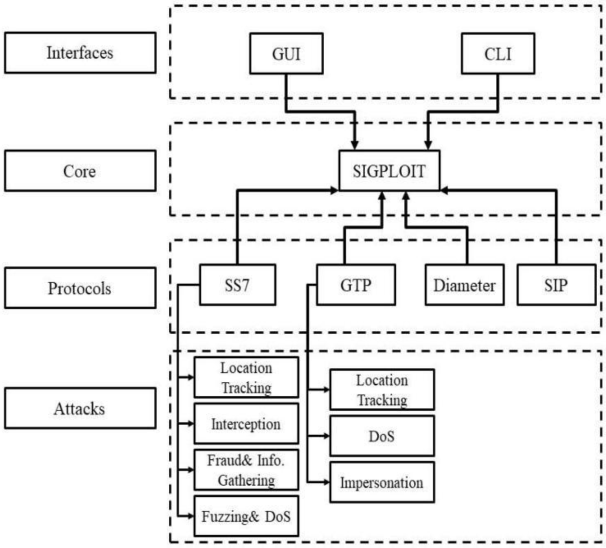


Fig.9 SigPloit's modules

1) Location Tracking
2) Call and SMS Interception
3) Fraud and Information Gathering
4) DoS
5) Fuzzing

The payloads are then organized according to their relevance to the respective attack module. Some SS7 messages could have different impact, for example updateLocation could be used for interception as well as performing denial of service attacks against an HLR. Therefore, there are payloads that are reused in multiple attacks modules based on their relevance and provided parameters.

The proposed architecture provides flexibility and decoupling of the modules that makes it easier for contributors and developers to import new modules and add new attack modules and payloads.

2) *Comparison between SigPloit and Other Tools*

The perspective and motive behind SigPloit's development, was mainly to enhance in a way previous work done in this area. The key points of difference between the proposed framework and other projects are described below.

a) Coverage

Not all attack scenarios that were noted in GSMA standards and the updated ones were included. On the other hand, SigPloit includes the latest exploitation techniques. SigPloit had recently added a new technique for SMS interception using updateLocation, where it could bypass velocity checks done by most of the SS7 firewall vendors [6]. Also a new attacking technique using SendRoutingInfoForSM, by changing the used numbering plan format to E.214 format, the impact will result in bypassing the home routing defense control.

b) Representation

The tools mentioned earlier might not have the flexibility to choose the attack scenario or a specific message to test against. Their main focus is to run related sets of messages at once, to test whether or not any protection is applied on the target node. However, SigPloit's aim is to add the a bit of an offensive like experience to simulate a real attack scenario, giving a flexibility for the parameters to be configured along with the sequence of initiated attacks building a strong base for the future not only to discover variants of the known attacks but as well to work towards building indication of compromises related to signaling based attacks adding on that the organization of the messages is in risk-message fashion, meaning that the messages that have a risk of fraud are grouped together. Those for tracking are grouped together and so on, it is not organized in a node-message fashion like the other respectable tools.

c) Comprehensiveness

The mentioned tools [11][12] are restrictive only to SS7 and do not include other signaling protocols that are vulnerable as well. On the other hand, SigPloit only supports SS7 but adds as well GTP, Diameter and SIP assessments.

d) Openness for Contribution

The flexibility of the programming language used and the interfacing between the core and user is lacking from previous work. One of the mentioned tools uses erlang. It is one of the most powerful programming languages to be used in the telecommunications industry and almost every vendor uses it in their core of their nodes. However, this limits contribution to those who only know erlang as it is not that popular when it comes to penetration testers. On the other hand SigPloit offers further flexibility and scalability, the core of SS7 and Diameter uses the open source java stack restcomm [16], GTP and SIP use python, all managed by python as the main interface between users and core of the code.

Key points	SS7Mapper	SafeSeven	SigPloit
Coverage and updates	Not updated with emerging new attacks	Not updated with emerging new attacks	Includes GSMA known attacks and other attacks discovered
Representation	Fixed set of attacks that tests the exploits against a specific node	Fixed set of attacks that tests the exploits against a specific node	Scenario based framework, focusing to test against the vulnerabilities and existing controls of the network not a specific node.
Comprehensiveness	SS7 only	SS7 only	SS7, GTP , Diameter and SIP
Open source	It is developed in Erlang which limits its contribution	Easy to contribute	Dedicated to the opensource community, it is a modular framework and developed in common programming languages allowing further contributions

Tabel 1. Comparison summary between SigPloit and existing tools.

This enables contributors to add a new code, compile it in java, in case of SS7 and Diameter, and just add its calling module in the core sigploit module. This is also one of the advantages of making the messages separate and independent not in a node-message structure.

A brief summary of the main comparison points between SigPloit and the other existing tools is depicted in Table1.

V. Conclusions & Future Work

In this paper, we have briefly come across the architecture and the main components of SS7 that are affected with these different types of threats. We also highlighted few attack scenarios and their simulation in SigPloit. The paper also focused on the architecture of SigPloit and its building blocks along with its difference and contribution from other related work.

For the future, the road-map for SigPloit has two directions. The first is to finish the core of the project, finalize the GTP module, which features DoS and information gathering attacks, SIP and Diameter attacks as well, add a reporting feature to meet the main goal of this project which is a comprehensive tool for telecommunication penetration testing. Another important point is to add a user friendly graphical interface to simplify its use. The second direction is to follow an optimized architecture following a front-end and back-end scheme, decoupling the core from the user interface in order to optimize the solution. Finally,adding analytics that could be useful in providing intelligence feeds for the community.

To conclude, this domain requires a lot of contribution and engagements to increase the awareness and avail the tools and resources to effectively assess the infrastructure of mobile networks that form a critical economical and strategic asset in a country.

References

[1] R.David, D.Adrian, H.Thorsten, W.Edgar, P.Christina. ”On Security Research towards Future Mobile Network Generations”, *IEEE Communication Survey and Tutorials* (2018).

[2] The 3rd Generation Partnership Project. “Mobile Application Protocol Specification”, *3GPP TS 29.002 rel 14* (2018).

[3] “HLR Lookups”, *www.hlr-lookups.com*.

[4] Engel, Tobias.”SS7-locate-track-manipulate”, *Computer Chaos Club* (2014).

[5] Nohl, Karsten. “SS7 Attack Update and Phone Phreaking”, *GeekFest* (2016).

[6] Puzankov, Sergey.”Stealthy SS7 Attacks”, *Journal of ICT Standardization* 5.1 (2017): pp.39-52.

[7] Kaspersky. “Why two-factor authentication is not enough”, *Kaspersky Lab Official Blog* (2017).

[8] The 3rd Generation Partnership Project. “UMTS & LTE Network Architecture Specification”, *3GPP TS 23.002* (2016).

[9] The 3rd Generation Partnership Project. “Number, addressing and identification Specification”, 3*GPP TS23.003* (2016).

[10] Positive Technologies. “Signaling System 7 Security Report” (2014).

[11] “SS7Maper”, www.*insinuator.net/2016/02/ss7maper-a-ss7-pen-testing-toolkit/.*

[12] “SafeSeven”, www.*github.com/akibsayyed/safeseven.*

[13] “Osmocom SS7 Stack”, www.*osmocom.org/projects/osmo_ss7*.

[14] “SigPloit”, www.*github.com/SigPloiter/SigPloit*.

[15] GSM Association. “SS7 and Sigtran Network Security”, *GSMA FS.07 (*2017).

[16] “Restcomm”, www.*restcomm.com.*