Telecommunication Systems
https://doi.org/10.1007/s11235-023-01018-0

Attacks to mobile networks using SS7 vulnerabilities: a real traffic analysis

Luiza Odete H. de Carvalho Macedo[1] · **Miguel Elias M. Campista**[1]

Accepted: 24 April 2023

Abstract
The SS7 (Signaling System n^o 7) protocol stack is still in use today to interconnect networks from different mobile telecommunication providers. These protocols were proposed in the 80 s, taking into account mutual trust relationships between participants. With the success of IP communications and the growth in the number of carriers, mobile networks have become exposed to many SS7 attacks. In this paper, we discuss important threats to SS7 networks as well as the main countermeasures. We also analyze a dataset obtained from a major telecommunication provider in Brazil. From this dataset, we observe that thousands of threats are triggered daily, that the main attacks are proportional along the time, that attacks are concentrated on a subset of attack sources as well as on a subset of victims, and that attack orchestration is possible but still not clear. These findings justify all the concerns regarding SS7 vulnerabilities and encourage new proposals towards attack mitigation.

Keywords Mobile communications · Legacy mobile networks · SS7 vulnerabilities · Real dataset analysis · SS7 attack characterization

1 Introduction

Even though we are witnessing more and more advances in mobile communications, a known pitfall persists as a consequence of SS7 (Signaling System n^o 7) signaling still in use among mobile operators. SS7 was conceived in the 80 s when network security was not at the focus of networking discussions. In 2008, during the 25th Chaos Computer Club Conference, however, the main SS7 attacks were exposed, and threats such as fraud, interception of customers' sensitive data, customers tracking, and even DoS attacks were publicly put in evidence [6].

The security aspect of mobile networking has been considered in recent standardization efforts led by the industrial sector. Many security requirements to interconnect operators have been included in documents called Permanent Reference Document (PRD), which was not enough to refrain attacks as it assumes that standards are still established between trustworthy parties. In practice, however, this reality is not fully reflected. A definitive solution, in this case, would be the total replacement of legacy mobile networks, 2 G and 3 G, and the consequent banishment of SS7. This, however, is far from reality, as reported by GSMA. Only in 2018, 4 G outnumbered 2 G with 47% of the total connections against 36% of 2 G [9]. In 2019, the difference increased, 52% against near 23% [10], without a precise forecast of when 2 G will be discontinued. Tearing down 2 G still finds resistance mostly because of corporate applications, such as mobile payment machines, and also because of the huge amount of investments on infrastructure replacement this would require [15]. Hence, even though all the attention is currently devoted to 5 G, the number of users affected by SS7 vulnerabilities and the need for technology fallback in 4 G/5 G networks do represent a challenge that cannot be overlooked [28].

This paper contributes to the literature extending the comprehension of SS7 vulnerabilities and consequent attack opportunities. We start by briefly introducing 2 G/3 G mobile networks and then we explain the SS7 vulnerabilities and the reason behind this is still a threat to 4 G/5 G networks. We identify four different attacks, explain the impact of each one with practical and protocol-level aspects, and introduce current countermeasure directions. Finally, we analyze a dataset from a major Brazilian telecommunication operator collected

✉ Miguel Elias M. Campista
miguel@gta.ufrj.br

Luiza Odete H. de Carvalho Macedo
luiza@gta.ufrj.br

[1] GTA-PEE/COPPE-DEL/Poli, Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, Brazil

Published online: 16 May 2023

throughout five months. The analysis could reveal four main findings:

- the large volume of attacks triggered to a single operator;
- the main attack types and the proportion to all others;
- the concentration of malicious actions on a subset of attack sources and on a subset of victims; and
- the small fraction of malicious actions from the same sources.

We are confident that our results from real production networks can shed more light on efforts to mitigate SS7 threats [19, 28].

The reminder of this paper is organized as follows: Sect. 2 overviews legacy mobile networks architectures, while Sect. 3 presents SS7 signaling vulnerabilities. Section 4 introduces current attack countermeasures, while Sect. 5 analyzes a real dataset from a Brazilian major operator to attest the impact of the attacks. Finally, Sect. 6 concludes this paper and draws future research directions.

2 Legacy mobile networks overview

The traditional 2 G (i.e., Global System for Mobile Communications – GSM) and 3 G (i.e., Universal Mobile Telecommunication System – UMTS) architectures are composed of access and core networks. Figure 1 depicts the interconnection between the access and core networks with external networks, like SS7 or IP networks.[1]

The access network, commonly known as Base Station Subsystem (BSS) for 2 G architecture or as Universal Terrestrial Radio Access Network (UTRAN) for 3 G architecture, enables users (also referred as subscribers herein) to attach their mobile terminals to the network. The access network comprises a Base Transceiver Station (BTS) and a NodeB for 2 G and 3 G, respectively, which are used to provide the main resources for communications between the Mobile Station (MS) and the network. Also, the access network has the controllers, called Base Station Controller for 2 G and Radio Network Controller for 3 G, which are responsible for allocating radio resources to BTSes and maintaining radio connections, including handovers when needed.

The core network, or Network Switching Subsystem (NSS), is responsible for all network control functions such as operation and maintenance, quality of service, and outgoing calls. The NSS is further subdivided into mobile switching center, user databases, and interconnection elements. The Mobile Switching Center (MSC) accumulates functions including call control, handover, billing, and network interconnection with external networks, like circuit-switched networks, SS7 networks, and IP-based networks. Switching centers that do not interconnect to access networks are called Gateway Mobile Switching Centers (GMSC), acting as access points to roaming users.

The network relies on database elements to store users' information at home, Home Location Register (HLR), and at visited networks, Visitor Location Register (VLR). The HLR stores permanent data, such as the telephone number or Mobile Station International Subscriber Directory Number (MSISDN) and the SIM Card identification (International Mobile Subscriber Identity - IMSI), which is used to locate the user in the network. The VLR stores temporary information from visiting subscribers for roaming purposes. As GSM does not support data packets, GPRS (General Packet Radio Service) was introduced to incorporate this functionality. Within the NSS, two new GPRS elements were included, the SGSN (Serving GPRS Support Node) and the GGSN (Gateway GPRS Support Node), similar to the MSC/GMSC, but with IP support.

The purpose of the SS7 is to establish a common language, with syntax and standardized parameters, for the core network elements. The SS7 defines a protocol stack similar in functionality to the OSI model. With the Internet success, the interoperability between SS7 and IP networks became fundamental. To this end, SIGTRAN (Signaling Transport) was created to promote the integration of circuit-switched and packet-switched networks.

Among the protocols added to the SS7 stack, the MAP (Mobile Application Part) protocol was introduced to handle mobile telephony requirements [1]. MAP is used for intra-core communications between network elements (MSC, HLR, SGSN, etc.) and inter-core networking, allowing communications between different networks, like home and visited networks. MAP employs a client–server approach, and attackers often use its vulnerabilities. In addition to MAP, the CAP (CAMEL Application Protocol) is another application protocol that provides services to mobile networks, such as prepaid services. In the SS7 stack, both MAP and CAP protocols are layered on top of the TCAP (Transaction Capability Application Part) protocol, which standardizes the communication between mobile network databases. TCAP supports several services, such as portability, wireless mobility, intelligent network services, and toll-free phone numbers. SCCP (Signalling Connection Control Part), however, is a network layer protocol used for routing in SS7 systems that is also used for malicious actions. Even though SS7 is used for signaling between different networks, as illustrated in Fig. 1, it is also used internally in a mobile network.

[1] The authors would like to thank Flaticon for the icons of the BTS/NodeB, the telephone, and the globe (https://www.flaticon.com/).

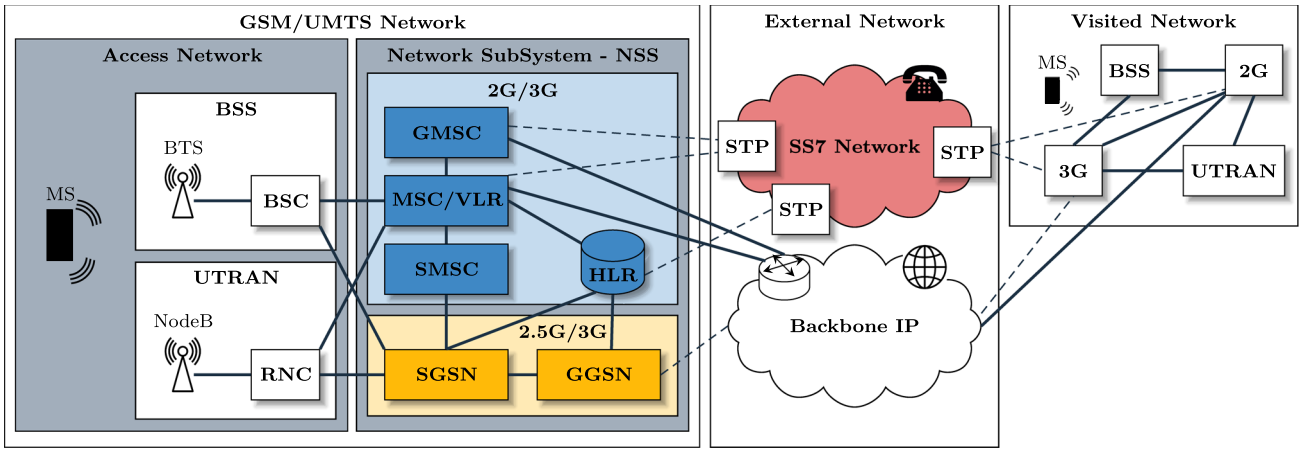


Fig. 1 Basic architecture including external networks interconnection. The elements inside the blue rectangle represent the 2 G/3 G legacy network core, which employs circuit switching. In contrast, the elements inside the yellow rectangle are used for packet switching, later attached to the network architecture. Continuous and dotted lines denote, respectively, physical and logical connections between network entities

3 SS7 signaling vulnerabilities

SS7 vulnerabilities are a consequence of its original design, as it took into account mutual trust between operators. At that time, they were not numerous and generally linked to the government. This scenario, however, has changed over the last decades as a consequence of SIGTRAN and IP networking. The growth in the number of operators with access to the SS7 network is mainly affected by the proliferation of smaller companies and Mobile Virtual Network Operators (MVNOs). Messages from MAP are still in use today to provide services to the core network, like management mobility, roaming, and users' authentication. As the SS7 design did not consider the security concerns we have today and that updates could not avoid attacks, many vulnerabilities can still be exploited with MAP. For instance, it is possible to track users, intercept calls and SMSes, trigger fraud attacks, and even bring down all the services available for a given user or provided by a network element [26].

The problem remains in 4 G (Non-Standalone – NSA) due to possible downgrades to 3 G/2 G to handle voice calls. Voice calls relying on circuit switching are not natively supported, as 4 G is fundamentally based on packet switching. Hence, to provide voice services entirely over LTE, i.e., to use VoLTE (Voice Over Long Term Evolution), one must deploy an IP Multimedia Subsystem (IMS), which provides several features, including voice support. Although IMS is part of 3 G, 4 G, and 5 G standards, some operators do not deploy an IMS core to support VoLTE calls. In this case, they will still need to downgrade to legacy networks (2 G/3 G) with voice support, the so-called Circuit Switched Fallback (CSFB), using SS7 [4]. Some operators have preferred this last alternative as employing an IMS core imposes huge investments on infrastructure. Moreover, to completely migrate to VoLTE, all mobile devices from users would need to natively support VoLTE, which will probably take time and may not be feasible in the short term. The Diameter protocol, which replaces SS7 in LTE, confirms that more recent technologies are not free from vulnerabilities [21, 22, 27]. Even though the Diameter protocol improves the network security, it has not been fully deployed by many operators. Thus, in these cases, many nodes are still hybrid, supporting both SS7 and Diameter protocols. This hybrid configuration postpones a definite solution, leaving it to future generations. As downgrading is the most practical solution for the moment, 4 G providers still have to deal with SS7 signaling and its inherent vulnerabilities.

5 G networks could not provide seamless coverage from the beginning. To accomplish that, 5 G/4 G interoperation was needed for the sake of service continuity. In 5 G non-standalone (NSA) version, devices always use an anchor in LTE networks, and consequently, the network requires the 4 G core, named Evolved Packet Core (EPC). If the 4 G coverage is missing, we have the same problem mentioned earlier, and the network makes a fallback to the legacy 2 G/3 G networks. In 5 G standalone (SA) version, the device anchors to the 5 G NR network, but it also falls back to 4 G when the 5 G coverage is missing [16]. Note that the network may continue downgrading until the voice call is completed. All these arguments corroborate the current security concerns raised by SS7, which do not have a clear perspective for a definitive solution in the short term or at least until the 5 G SA finally takes its place.

3.1 Attacks to SS7 networks

There are several possibilities to launch an attack against mobile users via an SS7 network. The attacker can even com-

bine different strategies to achieve better results. They apply a stepping-stone approach, taking advantage of known vulnerabilities to access information that can be possibly used to attack the mobile network or ultimately to attack legitimate users. We call these steps an "SS7 attack" or "mobile network attack" for the sake of conciseness. The first step of one of these attacks focuses on the air interface used for data communications between mobile stations and BTSes. Even though these communications employ common (Broadcast Common Control Channel (BCCH) and Paging Channel (PCH)) and dedicated logical channels, only the last one relies on authentication procedures. The use of an insecure BCCH and PCH gives the attacker, who has access to the SS7 network, the required information (TMSI, Global Title, etc.) to trigger an attack. By using authentication procedures, after allocating a dedicated channel to the user, communications become encrypted, and the user can securely send sensitive data to the network.

An attacker with passive radio equipment or a Software Defined Radio (SDR) can capture all the clear-text information disseminated through common channels, BCCH and PCH. For example, SDR blades available on the market at affordable prices can be used to eavesdrop on sensitive information from the air interface. Another similar option uses the combination of USRP (Universal Software Radio Peripheral) and open-source software, such as GNURadio, to also eavesdrop access networks.

Besides the common channel, users have a dedicated channel that relies on data encryption. In this case, sensitive data can be securely transmitted. Rupprecht et al. list the algorithms used in GSM dedicated channels, i.e., A5/1, A5/2, A5/3 and GEA4, among others, most with 64-bit size keys [23]. This encryption in GSM proved to be vulnerable, as it was possible to break the security of the communication that was based on the A5/1 and A5/2 algorithms, for example [14]. GSM originally lacked mutual authentication. Mutual authentication was later added to the GSM standard, but may not be used in all deployed networks. When GSM is not using the appropriate algorithm to authenticate both parties (as the UMTS-AKA protocol does, for example), it assumes that base stations are always legitimate, and in this trust model, messages from the network to the mobile stations do not require authentication. As a consequence, an attacker with an active radio (called "Cell-Site simulators" or "IMSI Catcher"), such as a StingRay I/II [20], can perform a Man-in-the-Middle (MiM) attack, establishing an intermediate connection between the user and the network. Open-source software implementing mobile communication standards can also be used for MiM attacks. Softwares such as OsmocomBB [30] can be installed in a mobile phone and connected to a PC running modified GSM Layer-2/3 to passively and actively act in a GSM network. Hence, an attacker with customized software and hardware can continuously broadcast the network's MCC and MNC to impersonate a base station and hide the frequencies of neighboring BTSes. Without being aware of real base stations, subscribers connect to malicious ones as their cell phone joins the BTS, among other parameters, with the highest signal strength. From the network viewpoint, the attacker camouflages himself by impersonating the user. Once connected to the fake base station, all the messages exchanged between the real base station and the subscriber are received by the attacker, who acts transparently, forwarding messages from side to side and, consequently, obtaining information from the subscriber, such as IMSI, IMEI, location, etc. This information can be used to later attack the network or legitimate mobile users. The attacker can additionally divert traffic to a specific modem. Even though in 4 G and 3 G mutual authentication is implemented, attackers can still downgrade to 3 G/2 G or possibly evolve towards an attack by obtaining sensitive information from protocol vulnerabilities [3, 25].

SS7 was not designed to meet rigorous security requirements. Hence, any message from MAP or other protocol from the SS7 stack destined to the mobile network core or some SS7 signaling point is promptly replied back. Although accessing the SS7 network to start generating messages is not so trivial, it is possible to directly rent or purchase an SS7 hub with access to the mobile network. This access is generally provided to MVNOs or small operators by major telecommunication providers to allow outsourcing and services extension, such as roaming and SMS. Once these MVNOs or small operators have access to the hub, in addition to the network access, a GT (Global Title) and a roaming agreement can be obtained. Another possibility to obtain access to the SS7 network is by purchasing a femtocell (or HNB – Home NodeB on 3 G) equipment, which can also be installed at users' residences. This equipment, however, has already shown vulnerabilities to attacks, allowing attackers to obtain subscribers' IMSI and IMEI or even intercepting calls and SMSes [7]. In addition, tools such as SkyLock from Verint, initially proposed for surveillance, have been used by people with malicious intentions. These tools, which are also a combination of software to generate SS7 messages and a hub to have access to the network, permit to track mobile subscribers anywhere in the globe using only as input the user's phone number (MSISDN) [28].

Table 1 summarizes the attacks, showing that the final goal is always to obtain users' sensitive data. Note that attackers exploit SS7 vulnerabilities to obtain privileged access to the network and launch the desired attack, following the so-called stepping-stone approach.

It is worth mentioning that different vectors can be combined to produce a hard-to-identify attack. A group of hackers named "Lightbasin" [12] combines different techniques to obtain access to telecom data. They exploit various methods to access DNS servers running Solaris and Linux systems

Table 1 Tools and respective attacks triggered against SS7 network. All of these alternatives for triggering attacks against mobile networks can be combined to maximize the final impact

Tools	Attack description
SDR + SS7 query generator	SMSes can be intercepted by the joint utilization of an SDR programmed to eavesdrop on subscribers' sensitive information and an SS7 query generator
Active radio + open-source GSM implementation	GSM implementations can be used with radio equipment to fake real base stations and consequently launch Man-in-the-Middle attacks to obtain sensitive data from users
SS7 hub to mobile network	Malicious users acquire legitimate SS7 hubs to obtain access to mobile networks and, consequently, request and receive back sensitive data from users or even their physical location

configured with weak passwords. Once inside the system, these hackers can install malicious software, e.g., malware, to use external DNS servers for roaming services. This access exposes GPRS networks carrying unmonitored traffic. Hence, even if an irregular behavior appears in the monitoring systems, this can also be an attack.

3.2 How SS7 attacks are triggered?

SS7 attacks can be roughly divided into four categories: tracking, interception, denial of service, and fraud. Please refer to [23, 28] for a thorough introduction of SS7 attacks.

Tracking: It consists of tracking the position of the mobile station in real-time, allowing the subscriber to be located at any time. This attack is difficult to mitigate because subscribers need to periodically send location updates to the network to demonstrate its availability and location. Attackers exploit these messages as a consequence of the insecure common channels used for communications between subscribers and respective base stations. The combination of SS7 hubs to mobile networks and tools to generate SS7 messages are used in such attacks.

The tracking attack is the simplest one to execute as long as the attacker has access to some real-time tracking tool, such as SkyLock. Another possibility to launch a tracking attack is to trigger a MiM attack followed by particular MAP messages. An attacker with this type of access and a real subscriber number (MSISDN) can impersonate a legitimate network element. Then, the attacker can send ATI (`anyTimeInterrogation`) messages, from the MAP protocol, to the HLR database of the subscriber's home network. This message requests the subscriber's location (cell ID) and IMEI, the information needed to track anyone in the mobile network. To accomplish that, the HLR contacts the visited network switching center (MSC), asking about

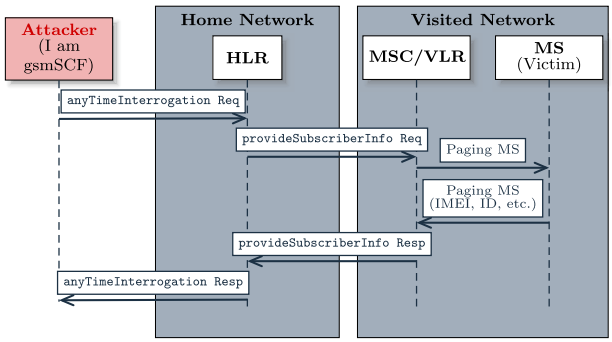


Fig. 2 MAP message exchange in a tracking attack. The SS7 `anyTimeInterrogation` is used to trigger updates regarding subscribers' location

the cell ID using the PSI (`provideSubscriberInfo`) message. This message is sent to the VLR the subscriber is currently in, which performs a Paging process to obtain the subscribers' information from the base station. Afterward, this information is forwarded to the HLR, returning the subscriber's location to the attacker. Figure 2 shows the messages exchanged involving the mobile network databases and also the subscriber's mobile station, which is ingeniously used to send back sensitive information to the attacker. The attacker plays the role of GSM Service Control Function (gsmSCF), a logical entity that communicates to the HLR using MAP.

Interception: The attacker intends to read the data originally sent to or received by a legitimate subscriber. From the information obtained with the tracking attack, it is also possible to start an interception attack. With subscribers' sensitive data, the attacker can record conversations, read passwords, and obtain information about users' activities. This becomes possible as the attacker supposedly acts as a legitimate mobile network element, forwarding SMSes or calls to or from subscribers to himself. Although the information is transmitted

through a dedicated channel, in GSM, there is the possibility of executing the MiM attack, for example, using the lack of mutual authentication and security of SS7. In more recent mobile generations, the attacker can still downgrade to 2 G to perform an interception attack.

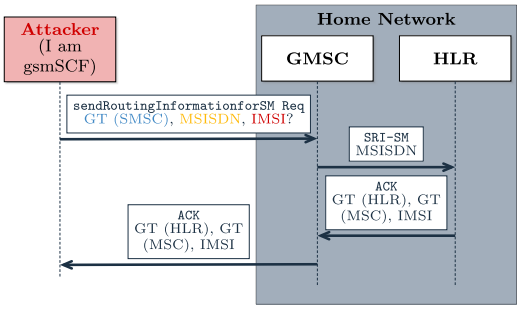
To trigger an interception attack, the attacker needs specific information from the network in advance, such as a valid identifier (GT) of an element, e.g., a valid identifier from the SMSC to intercept SMS messages. This information can be obtained by listening to the air interface, as discussed above in the tracking attack. With this information and the subscriber number, the attacker can generate MAP messages to request routing information from a legitimate user, starting with the IMSI. As network elements ingenuously reply to any valid MAP message, the HLR sends back the information requested from a legitimate subscriber (Fig. 3a). Within the `sendRoutingInformationforSM` MAP request, there is the information obtained from the air interface (GT), in blue; the information already known by the attacker, in yellow; and the information the attacker wants to obtain in red.

After obtaining the IMSI from a legitimate subscriber, the attacker needs a new valid GT to impersonate an MSC switch. This can be obtained from the operator, by purchasing an SS7 hub. The attacker can then act as a valid MSC to send MAP messages directly to the subscriber's HLR. This provides the attacker the ability to change the current location of the subscriber to the new MSC (Fig. 3b). We assume that the content of the MAP message `updateLocation`, the identifier, and the IMSI, is already known by the attacker. The content of the MAP message `updateLocation` is in yellow, assuming that the attacker already knows the identifier and the IMSI.

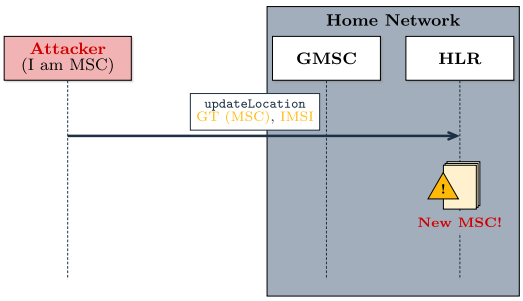
When an SMS arrives in the network, sent for instance by an external user to the victim, the SMSC looks up the database for the subscriber to deliver the message. The SMSC sends the MAP `SRI-SM` (Send Routing Information for Short Message) request to the HLR, containing all the information required to locate the subscriber. The HLR replies with the current location of the legitimate subscriber, which is the MSC of the attacker who has claimed to have the victim in his network. Therefore, all SMSes sent to the subscriber will be redirected to the attacker (Fig. 3c).

Denial of Service (DoS): It consists of interrupting the service for legitimate subscribers (for example, preventing them from making calls and send SMSes) or making some network element unavailable. This attack aims to compromise network availability, integrity, and maintainability.

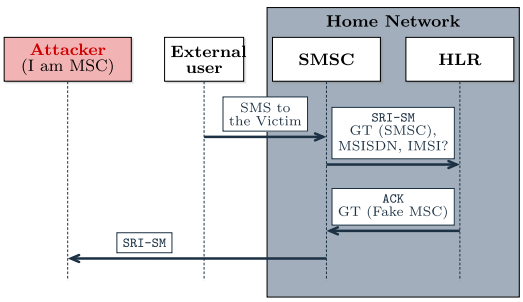
In the DoS attack, the attacker must obtain in advance the subscriber's IMSI and the Global Title (GT) of the MSC and of the VLR database, in addition to the access to the SS7 network and the subscriber's phone number. The GT identification can be obtained on the Internet, publicly available in the International Roaming Document (IR.21), which standardizes roaming agreements between operators. The attacker thus sends the `deleteSubscriberData` MAP message to the MSC/VLR, which removes all services enabled for the targeted subscriber. Sending the `cancelLocationreq` message, the attacker can achieve the same effect, which eliminates the subscriber's connection to the network, preventing calls and SMSes from being delivered to this user.



(a) Attacker obtains sensitive information from legitimate users.



(b) Attacker impersonates an MSC to update the current subscriber location to fake one.



(c) Attacker intercepts an SMS message.

Fig. 3 MAP message exchange in an SMS interception attack. Upon obtaining an SMS, attackers can store, modify, or even forward the SMS to the legitimate subscriber

An attacker with access to the SS7 network can also produce several roaming requests to bring down a network element (Fig. 4). At each request, a roaming number is provided for the fake network element. The attacker sends a MAP `provideRoamingNumber` message with his GT, requesting the MSRN number (Mobile Subscriber Roaming Number) associated with the victim's IMSI. The MSC replies by informing the requested number. The attacker then repeats the request several times, flooding the switching center, until new Roaming Numbers are no longer available. When a real

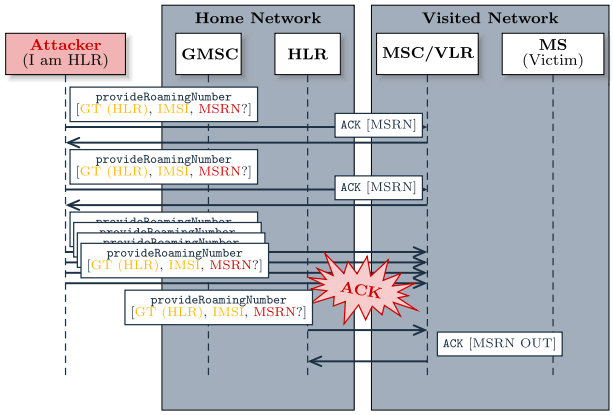


Fig. 4 MAP message exchange in a DoS attack. The attacker saturates the MSC by sending consecutive MAP `provideRoamingNumber` messages

database (HLR) makes the same request, the MSC will not be able to provide a new Roaming Number.

Fraud: The attacker aims to obtain financial advantages from a network subscriber. An example is changing the call forwarding settings using the MAP protocol so that the cost of the call is reverted to another user. This attack procedure is similar to an interception attack, where the attacker impersonates a fake element (Fig. 3b), obtains sensitive data from the victim, and after that, USSD (Unstructured Supplementary Service Data) codes are used to transfer or receive prepaid credits. The motivation of this attack is to use more sophisticated services such as phone numbers used for online gambling, chats, VIP number, etc., without being charged for it.

4 Countermeasures

The IR.82 document published by GSM Association highlights SS7 vulnerabilities [8] concerned with the original assumption on mutual trust between operators. It is worth mentioning that this information can be inferred from public sources [24, 26]. From these sources, three categories of MAP and CAP messages are inferred. These categories define filtering recommendations for outgoing and incoming messages at terminal nodes (nodes at the mobile network core) and transit nodes (SS7 network signaling points), as listed next:

- **Category 1**: This is composed of MAP messages exchanged within the network, i.e., network internal messages. A message of this type from external networks should only be accepted if a contract explicitly permits this action. One of these messages is the ATI (`AnyTimeInterrogation`), which should be received and treated only if the source node is the HLR of the originating network. For this category, the recommendation is to adopt a policy that filters out these messages at the network edge using firewalls.
- **Category 2**: This is composed of MAP messages sent from subscribers' home networks to visited networks, which may happen to handle roaming users. For example, a subscriber from city A is traveling in city B, and the HLR database from A queries the network at B to check a subscriber's location. To prevent attacks in this category, the GSMA recommends checking the source of the MAP message to verify if the IMSI of the visiting subscriber indeed belongs to the HLR of the home network.
- **Category 3**: This is composed of MAP messages from visited to home networks, also as a consequence of roaming users. It is similar to Category 2, except that the process starts at the VLR at city B (visited) to the HLR at city A (home), for example. In this reverse situation, applying filters becomes more difficult because the message can be originated anywhere. Hence, an attacker could claim that the subscriber is in his own network. The home network must then compare the information from the user's last location to the information within the received MAP message. If the information does not match, it should be taken into account whether it would be possible for a subscriber to travel from her last location to the new one informed during the corresponding elapsed time. If it is concluded that the current location is unreasonable, the message must be filtered out.

4.1 Approaches

Even though there is an effort to propose strategies to avoid SS7 attacks, the definitive solution would be to replace the system completely. This solution, however, is not feasible for the years to come. Thus, some alternatives have been studied, such as filtering MAP messages, already discussed above. In addition to these filtering categories, there are also initiatives to block CAP, SCCP, and SMS messages. All in all, preventing SS7 attacks is a matter of deterring attackers from obtaining sensitive information. Again, considering the stepping-stone approach, this information is the first step toward an attack on the network and, ultimately, on users. Hence, most countermeasures aim to interrupt this attack preparation at its first step, protecting subscribers' data and network identifiers.

In 2007, the 3GPP published changes to SMS handling to minimize the incidence of interceptions. Previously, the SMSC would send a query to the HLR to discover the phone exchange, where the destination subscriber is allocated. Once discovered, the SMS would be forwarded to the discovered phone exchange and finally to the subscriber. Therefore, an attacker impersonating the SMSC could intermediate this

procedure to intercept the SMS message. From the information collected (such as the GT address of the phone exchange and the IMSI of the subscriber), the attacker can impersonate the destination phone exchange as soon as an SMS is received, not delivering the message to the destination or acting transparently to read the SMS without the destination awareness. To avoid this attack, operators can deploy an "SMS Home Routing", an SMS router placed between the home and the visited network. The idea is to avoid message forwarding to be carried out directly. Depending on an intermediate (router), the SMS Home Routing, all sensitive messages are exchanged internally to the source network. The only information externally available is concerned with the SMS Home Routing. In addition, the IMSI is not exchanged between the router and the visited network, as they use a mapped identifier to hide sensitive data. The big issue here is that not all operators have implemented "SMS Home Routing" and even if they do, misconfigurations can also provide new opportunities for attackers [28].

In the case of network elements impersonation, there are initiatives to detect the presence of anomalies in the network, taking into account applications and sensors [23]. For example, Karsten Nohl introduced an application called SnoopSnitch, developed by Security Research Labs for the Android platform [17]. In addition to detecting the presence of "IMSI Catchers", it is possible to develop applications to show whether the network operator used by a subscriber is under any SS7 attack, such as an SMS interception. The application allows the configuration of an alarm to alert users that an SS7 attack has been detected. SnoopSnitch works only with Qualcomm chipsets, and the user needs to have the root mode enabled in her phone to allow scanning the operator's network. Operators do not clearly reveal how they detect an ongoing attack in the network since this is still strategical for their business. It is assumed, however, that the application turns the cell phone into a passive and active radio. Thus, it is possible to execute SMS attacks to check the operator vulnerability and passively check the radio channel and power transmission signal from nearby base stations. This physical-layer procedure is used to detect the presence of "Cell Site Simulators" in the network. The data collected by the application can be sent to the database that feeds the "GSMMap", an online map that exposes SS7 attacks to the network of major operators at a global scale.

Dabrowski et al. pointed out several items that can be used as a reference to define if there is a sniffing device in the access network, such as an unusual Cell ID or an unusual frequency. Other references are encryption disabled and abnormal cell usage capabilities [5]. In addition, two false network element detectors are developed, called "IMSI Catcher Catcher" or ICC. The stationary ICC (sICC) is a hardware developed with Raspberry Pi with access to the 3 G network, capable of operating in the 900 to 1800 MHz range. The mobile ICC (mICC), similarly, is an Android application with the same purpose. Both were effective in capturing characteristics of neighboring cells (sICC managed to capture in a range of 90 km distance) and proved to be viable in capturing attackers. Another proposal to deal with IMSI catchers is to improve network authentication using a pseudonym for this identifier, called PMSI (Pseudo Mobile Subscriber Identity) [2, 29]. The PSMI is randomly generated, aiming to hide the true identity of the subscriber for the sake of confidentiality in the communication channel. Strategies relying on mutual authentication have also been proposed for message exchange as well as detection procedures including geographical positioning using GPS, base stations pattern analysis using cellular parameters and, more recently with the emergence of 5 G, the employment of identities using asymmetrical cryptography [23].

Holtmanns et al. [11] describe SS7 attacks as well the corresponding countermeasures. Nevertheless, the focus was on explaining that more recent networks, such as 4 G, are also vulnerable to the same threats of legacy networks in roaming situations. The reasons are many, Holtmanns et al. assume that the configuration of the operator under attack does not use IPSec between SS7 and Diameter nodes, i.e., messages are sent in clear between them; does not apply IP address filtering and, even using white or black lists, the attacker can circumvent these methods; does not use layer matching, i.e., they do no check if the sender and the return address are coherent in terms of protocol layers; and does not run sanity checks, i.e., messages received are not checked against precedent messages possibly from the same flow. Finally, they assume that the attacker knows the MSISDN of the victims, the address of the edge node. The interconnection is not always directly conducted with peers for roaming and using third-party networks can expose both peers.

The literature also presents the use of machine learning techniques to detect anomalies in SS7 networks [13]. In summary, a simulator that reproduces an operator network is developed to generate SS7 attacks. Using the S-H-ESD (Seasonal Hybrid Extreme Studentized Deviate) algorithm, the proposed features were tested as an indication of machine learning feasibility to detect the SMS interception attack.

In contrast to simulated results, the next section presents a set of real SS7 traffic data from a major telecommunications operator in Brazil.

5 Dataset characterization

A major Brazilian telecommunication provider has verified the vulnerability of its network using an extensive analysis of incoming traffic. The goal was to raise possible threats they could be exposed to through their SS7 network. To accomplish that, all SS7 signaling coming from international peers

was sent to an internal destination for further analysis. Network signaling transfer points (STPs) duplicate the received traffic before sending to an internal STP. The raw international traffic was sent to a server combining the roles of IDS and firewall, both available at the market, able to detect possible SS7 attacks. This solution was chosen because other alternatives using more accessible software, such as Wireshark, could not handle the traffic volume appropriately as it continuously saturated an incoming buffer. Therefore, the solution adopted was to use a firewall, which in addition to a larger storage capacity, was a tool for detecting and mitigating attacks in SS7 networks. Basically, the solution employed used the Analytics tool to analyze the data and find anomalies.

The deployed server applied particular filters configured to identify messages destined to the current operator and its peers. The server took into account an MCC configured with "724" (Brazil), and an MNC and NDC configured with values corresponding to the operator and its location. The goal was to observe all the signaling traffic sent to IMSI's starting with the prefix "724XX", where "X" is the operator number. After filtering out undesired traffic, the server used an IDS to detect SS7 attack occurrences based on predetermined profiles. Even though the operator configured the IDS along with the server provider, they did not eliminate the possibility of false positives. For example, the telecommunication provider used the SMPP (Short Message Peer-to-Peer) protocol and a gateway SMS to forward SMS messages. Thus, an SMS interception attack was not collected. We prefer hereinafter to use the word threat instead of attack because not all attempts to attack the network and its users were successful.

We characterize all the data produced after filtering and classification. The attack source is the true origin of the message, obtained with the E.164 identifier of the network element (ISDN identifier that is informed along with the Global Title – GT). This identifier is the one that has interacted with the operator elements during the attack. The network sniffer identified these numbers using the collected PCAP files. Even though the Global Title could be spoofed, the telecommunication provider validated the identifier using an external tool, e.g., EAGLE from Oracle [18]. For the sake of confidentiality, however, we struggle to keep hidden all the sensitive information for the operator, including its name. The data was collected for five months, between 15 December 2018 and 15 May 2019. The main threats observed, the number of threats as well as the their intensity, the source and destination, and their frequency along the time are shown.

5.1 Experimental results

Figure 5 shows the number of threats triggered to the network of the operator, which is close to the average value of 21,900 threats/day most of the time. We observed peaks close to

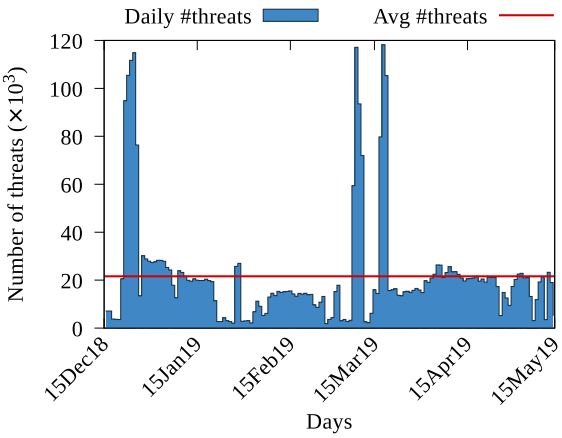


Fig. 5 Daily number of threats

holidays, Carnival in February, St. Patricks' Day in March, and Christmas/New Year's Eve in December. Even though these peaks need further investigation, we believe that the attackers are aware of better chances of success during off-hours or periods of more intensive use by subscribers. Hence, the attacks on these dates become more attractive.

Even though we have subdivided the attacks into four categories, this division is a simplification to express the potential attacks an operator may suffer. The same attack is accounted on different categories if they can be used as a stepping-stone to anyone of them. In fact, there are different types of MAP messages found in the network considered threats for many reasons, including abortion of message exchange or unauthorized message exchange. Messages with incomplete parameters are also considered threats, as well as messages that would lead to quick relocation. In addition to MAP, TCAP, CAP, and SCCP messages appear in the data collection process and are also considered threats. Hence, taking a deeper look into our dataset, we highlight the six most common threats triggered against the operator using these protocols. These top-seven threats are called "Fast Relocation", "Abnormal TCAP Handshake Aborted", "Fast Relocation with SMS", "Send Routing Info For SM Abnormal", "Cancel Location Completed", "E214 Suspicious" and "Provider Subscriber Info Completed". They account for more than 91% of the total number of threats collected in our dataset.

A threat can be considered as "Fast Relocation" when the transition time (or relocation) of a subscriber is below an acceptable threshold. Hence, if a subscriber moves from one country to another using the international roaming service, the operator must be aware of the user's location to keep its number able to receive calls, send SMS, and consume data. The user's location is complemented with a timestamp of the last time the user was connected to the network and the current date and time. Suppose the difference between the timestamps is not feasible considering the

Table 2 Top-7 threats triggered against the operator and its peers. We also add the protocol used from the SS7 stack, the categories involved, and the proportion considering the total number of threats

Threat	Protocol	Category	Proportion (%)
Fast Relocation	MAP	Subscriber DoS, Fraud, or Interception	52.45
Abnormal TCAP Handshake Aborted	TCAP	Interception	26.21
Fast Relocation with SMS	MAP	Subscriber DoS, Fraud, or Interception	4.20
Send Routing Info For SM Abnormal	MAP	Subscriber DoS, Fraud, or Interception	2.73
E214 Suspicious	SCCP	Location Tracking, Fraud, Interception	2.34
Cancel Location Completed	MAP	Subscriber DoS	1.75
Provider Subscriber Info Completed	MAP	Interception	1.66

distance between the two countries and the timezone. In that case, this movement is viewed as a threat, as the attacker may have maliciously transferred the victim to another network. Similarly, the "Fast Relocation with SMS" occurs when the operator receives an SMS message from a subscriber roaming in another country. These two threats, whenever they happen, are categorized simultaneously as a "Subscriber DoS" (if the services become unavailable for the user), a "Fraud", and an "Interception". The "Abnormal TCAP Handshake Aborted", on the other hand, is categorized only as an "Interception" and occurs when a TCAP message is received without part of the required parameters. Therefore, this message is not legitimate and is considered by the network as a threat. By default, the network discards incomplete messages upon arrival as they do not follow the 3GPP criteria. The "Send Routing Info For SM Abnormal" threat is a request message using MAP to recover user data such as IMSI and location. When an SMS message does not precede, this request is considered a threat. The network discards such messages and categorizes them as "Fraud", "Interception", and "Subscriber DoS". The threat "Cancel Location Completed" occurs when the network receives a request sent by an unauthorized node to exclude a user from the temporary database (VLR). This case falls into the "Subscriber DoS" category. The "E214 Suspicious" threat appears when a foreign GT attempts to query a home network IMSI, this is considered suspicious. Finally, the "Provider Subscriber Information Completed" is an unauthorized request to the VLR regarding the subscriber's location. By default, the network replies to this request, which is clearly a step toward an "Interception" attack. Table 2 presents the Top-7 threats found in this work against the network operator. Note that the highest proportion of threats is on the "Fast Relocation" attack, which corresponds to more than 50% of the total number and uses the update location message of the MAP protocol. In addition, we can also observe that the MAP protocol is used for most attacks.

Figure 6 plots the proportion of threats along the time for the different categories. Interception threats are the most

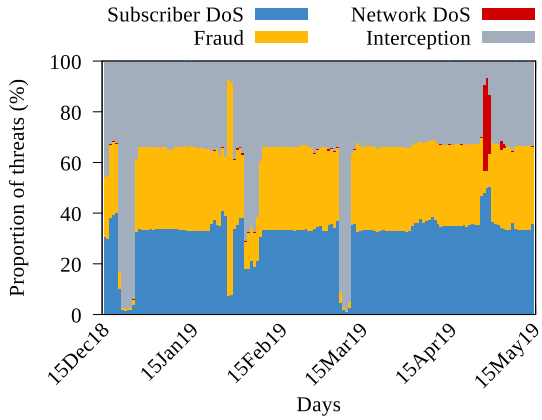


Fig. 6 Proportion of threats

popular ones, representing 40.90% of all threat occurrences. In this type of attack, attackers obtain subscribers' sensitive data from the operator. With 30.25 and 28.82%, we have threats related to DoS and fraud attacks, respectively. We subdivide the DoS threat to show that network DoS can also be triggered. Threats related to tracking are not observed. We observe that DoS remains stable along the time, whereas all the other threats have more bursty behavior.

Figure 7 shows the daily number of threat sources (#attackers) and the daily number of victims (#victims). We note that the number of attack sources shows more stability than the number of victims and that the number of victims is more numerous. This result indicates that attackers typically target multiple victims. Figure 7 also shows the Jain Index (JI) to compute the concentration of threats from the attackers' and victims' viewpoints. The Jain Index is used to compute fairness on resource distribution, where 0 and 1 denote totally unfair and fair distribution, respectively. Bringing to our case, 0 denotes a single attacker executing all threats (Attackers JI = 0) or a single target being the victim of all threats (Victims JI = 0), whereas 1 denotes an equal share of threats per source (Attackers JI = 1) and threats targeted to each victim (Victims JI = 1). In the figure, we note that threats are concentrated on a subset of attackers and victims, as both JI are always near to 0. This may indicate threats orchestration on particu-

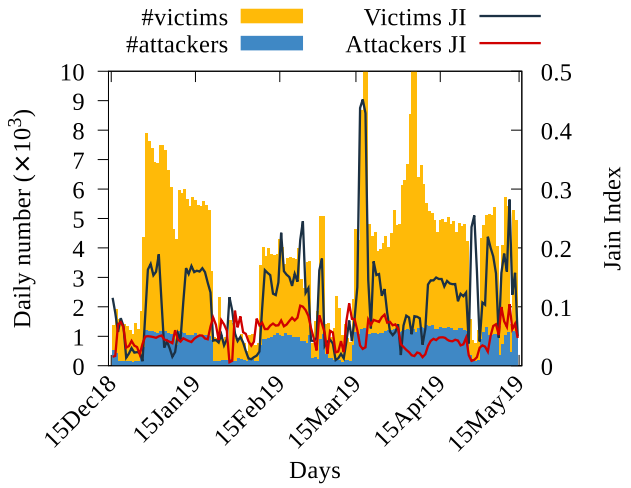


Fig. 7 Victims vs. attackers

lar targets. We note, however, that except in mid-April, peaks in the number of victims involve more distributed threats as Victims JI increases. The attack in mid-April is the unique counterexample, as the number of different victims is elevated at the same time we have a concentration on attackers and victims. This observation indicates other attack profiles, which would require further investigation.

We model the dataset as a symmetric edge-weighted graph, where threat sources are the vertices, and the edges are built between vertices triggering attacks on the same day. Edge weights are the number of days an edge appears in the entire dataset. Figure 8 shows the cumulative distribution function of vertices (attackers) degree and edge (attacker pairs) weights. The x-axis is the total number of edges and vertices in the entire dataset, 10,209,264 and 6,916, respectively, normalized; while the y-axis shows the normalized edge weights and vertices degree. We note that only a small fraction of nodes triggers attacks every day, i.e., most

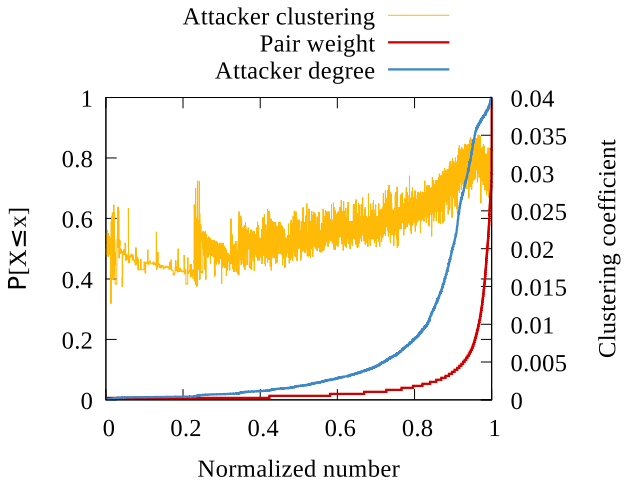


Fig. 8 Edges weight and vertices degree distribution

nodes avoid repeatedly attack the same operator. Figure 8 also shows the clustering coefficient of each corresponding attacker. We note that the clustering coefficient increases with edge weight, also suggesting attackers orchestration. Persistent attackers possibly act with predefined peers.

6 Conclusion

Even though SS7 signaling has been left aside given all the advances in new mobile generations, it is still a severe threat to many users who still use legacy services. Moreover, problems regarding 5 G/4 G coverage do still require technology fallback to 3 G/2 G networks for voice calls. Changing this scenario requires investments in infrastructure to either enlarge coverage or replace equipment. This change, however, will not happen in a horizon of at least 4 or 5 years to come.

This paper characterized SS7 attacks triggered against the network of a major Brazilian operator using a real dataset. We observed the large volume of attacks triggered against a single operator, the main attack types, and the concentration of actions on a subset of participants. The obtained results evidenced all the existing risks of using SS7 signaling in modern generations of mobile networking and the importance of taking countermeasures to minimize the risks. We aim to inspire new proposals toward SS7 attack mitigation based on firewalls or even SS7 traffic prediction.

In future work, we are looking toward more recent data from major mobile operators to reevaluate the trend regarding attacks using SS7 signaling. In addition, we would like to investigate the deployment of blockchains to introduce auditability on network interconnection in mobile networks.

Funding This paper was partially supported by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior— Brasil (CAPES)— Finance Code 001, CNPq, FAPERJ grant number E-26/211.144/2019 and Grant Number E-26/202.689/2018, and FAPESP Grant Number 15/24494-8.

Availability of data and materials Not applicable.

Code Availability Not applicable.

Declarations

Conflict of interest Not applicable.

References

1. 3GPP: Mobile Application Part (MAP) specification. (1999). Technical specification (TS), 3rd generation partnership project (3GPP). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1585

2. Ateniese, G., Herzberg, A., Krawczyk, H., & Tsudik, G. (1999). Untraceable mobility or how to travel incognito. *Computer Networks, 31*(9), 871–884.
3. Bais, A., Penzhorn, W. T., & Palensky, P. (2006). Evaluation of umts security architecture and services. In *4th IEEE international conference on industrial informatics (INDIN)* (pp. 570–575). IEEE
4. Bautista, J. E. V., Sawhney, S., Shukair, M., Singh, I., Govindaraju, V. K., & Sarkar, S. (2013). Performance of CS fallback from LTE to UMTS. *IEEE Communications Magazine, 51*(9), 136–143.
5. Dabrowski, A., Pianta, N., Klepp, T., Mulazzani, M.,& Weippl, E. (2014). IMSI-catch me if you can: IMSI-catcher-catchers. In *30th annual computer security applications conference (ACSAC)* (pp. 246–255)
6. Engel, T. (2008). Locating mobile phones using signalling system #7. 25th Chaos Communication Congress. https://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf
7. Gold, S. (2011). Cracking cellular networks via femtocells. *Network Security, 2011*(9), 5–8.
8. GSMA: IR.82 SS7 security network implementation guidelines (2016). Tech. rep., GSM Association. https://www.gsma.com/security/resources/ir-82-ss7-security-network-implementation-guidelines-v5-0/. Version 5.0
9. GSMA: The mobile economy 2019 (2019). Tech. rep., GSM Association. https://www.gsma.com/r/mobileeconomy/
10. GSMA: The Mobile Economy 2020 (2020). Tech. rep., GSM Association. https://www.gsma.com/r/mobileeconomy/
11. Holtmanns, S., Rao, S. P., & Oliver, I. (2016). User location tracking attacks for LTE networks using the interworking functionality. In *IFIP Networking conference (Networking) and workshops* (pp. 315–322). IEEE
12. Ilascu, I. (2021). Lightbasin hacking group breaches 13 global telecoms in two years. https://www.bleepingcomputer.com/news/security/lightbasin-hacking-group-breaches-13-global-telecoms-in-two-years/ . Online; Accessed in December 30, 2022
13. Jensen, K., Do, T. V., Nguyen, H. T.,& Arnes, A. (2016). Better protection of SS7 networks with machine learning. In *6th international conference on IT convergence e security (ICITCS)* (pp 1–7). IEEE
14. Kalenderi, M., Pnevmatikatos, D., Papaefstathiou, I.,& Manifavas, H. (2012). Breaking the GSM A5/1 cryptography algorithm with rainbow tables and high-end FPGAs. In *22nd international conference on field programmable logic and applications (FPL)* (pp. 747–753)
15. Kulkarni, P., & Oviedo, R. M. (2014). Should operators switch-off their legacy infrastructure or re-purpose it for M2M? In *IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)* (pp. 1–6). IEEE
16. Liu, G., Huang, Y., Chen, Z., Liu, L., Wang, Q., & Li, N. (2020). 5G deployment: Standalone vs. non-standalone from the operator perspective. *IEEE Communications Magazine, 58*(11), 83–89.
17. Nohl, K. (2014). Mobile Self-Defense. Tech. rep., Security Research Labs . https://fahrplan.events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf
18. Oracle: EAGLE Database Administration- GTT User's Guide (2022). https://docs.oracle.com/en/industries/communications/eagle/46.9/index.html
19. Peeters, C., Abdullah, H., Scaife, N., Bowers, J., Traynor, P., Reaves, B., & Butler, K. (2018). Sonar: Detecting SS7 redirection attacks with audio-based distance bounding. In *IEEE symposium on security and privacy (SP)* (pp. 567–582). IEEE
20. Pell, S. K., & Soghoian, C. (2014). Your secret Stingray's no secret anymore: The vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy. *Harvard Journal of Law and Technology*, 28(1)
21. Rao, S. P., Kotte, B. T., & Holtmanns, S. (2016). Privacy in LTE networks. In *9th EAI international conference on mobile multimedia communications* (pp. 176–183). ACM
22. Roth, J. D., Tummala, M., McEachen, J. C., & Scrofani, J. W. (2017). On location privacy in LTE networks. *IEEE Transactions on Information Forensics and Security, 12*(6), 1358–1368.
23. Rupprecht, D., Dabrowski, A., Holz, T., Weippl, E., & Pöpper, C. (2018). On security research towards future mobile network generations. *IEEE Communications Surveys & Tutorials, 20*(3), 2518–2542.
24. Schaeken, V. (2019). Vulnerabilities, potential risks and recommendations . https://www.itu.int/en/ITU-T/Workshops-and-Seminars/102019/Documents/Vulnerabilties_and_Categories.pdf
25. Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., & Seifert, J. (2015). Practical attacks against privacy and availability in 4G/LTE mobile communication systems. CoRR abs/1510.07563
26. Technologies, P. (2018). SS7 vulnerabilities and attack exposure report . https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Positive-Research-2018-eng.pdf
27. Tu, G. H., Li, C. Y., Peng, C., & Lu, S. (2015). How voice call technology poses security threats in 4G LTE networks. In *2015 IEEE conference on communications and network security (CNS)* (pp. 442–450). IEEE
28. Ullah, K., Rashid, I., Afzal, H., Iqbal, M. M. W., Bangash, Y. A., & Abbas, H. (2020). SS7 vulnerabilities—A survey & implementation of machine learning vs rule based filtering for detection of SS7 network attacks. *IEEE Communications Surveys & Tutorials, 22*(2), 1337–1371.
29. Van Den Broek, F., Verdult, R., & de Ruiter, J. (2015). Defeating imsi catchers. In *Proceedings of the 22nd conference on computer and communications security (SIGSAC)* (pp. 340–351). ACM
30. Zheng, Y., Huang, L., Shan, H., Li, J., Yang, Q., & Xu, W. (2017). Ghost telephonist impersonates you: Vulnerability in 4G LTE CS fallback. In *IEEE conference on communications and network security (CNS)* (pp 1–9). IEEE

Luiza Odete H. de Carvalho Macedo received an M.Sc. degree in Electrical Engineering from Universidade Federal do Rio de Janeiro in 2019 and a B.Sc. degree in Telecommunications Engineering from Universidade Federal Fluminense in 2014. From 2014 to 2021, she worked as a telecommunications specialist with Embratel, and since 2021 she has been with Nokia as a Customer Application Engineer. Her research interests are computer networking and telecommunications.

Miguel Elias M. Campista is an associate professor at the Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, Brazil, since 2010. His major research interests include network and data science, wireless networking, and cloud and fog computing. Campista received his D.Sc. degree in Electrical Engineering from UFRJ in 2008 and spent 2012 in the LIP6 lab at Sorbonne Université, Paris, France, as invited professor. He is a former affiliate member of the Brazilian Academy of Sciences, and an associate editor of Annals of Telecommunications, Springer.