University of Piraeus

Department of Digital Systems

MSc Digital Systems Security

Attacks on SS7

Master Thesis

Christos Xenakis
Associate Professor

Eustratios Magklaris
MSc student

Piraeus, June 2019

Abstract

Signalling System No 7 is the global network that interconnects all telecom operators around the world. Even though it is still used to control 3G traffic, it was design many years ago, when most operators were state controlled companies. Back then, modern threats could not have been foreseen and thus SS7 was adopted without any measures of security, such as authentication, integrity or confidentiality. The whole structure of trust was based on international trade agreements between the operators.

With the emerging market liberalization and the increased switch to *All-IP* technology, access to SS7 has become easier than ever. Access to such an insecure network could mean the compromise of the global telephone network, landline and mobile.

In this thesis, we analyse the structure of the SS7 protocol stack, we outline its known attacks, we show some ways to emulate an operators network and finally we present an automated tool as a proof of concept, along with some defence solutions.

Acknowledgements

I would like to express my sincerest gratitude towards my supervisor Dr. Christos Xenakis. His guidance and patience are beyond compare.

Contents

Introduction

Transfer of information in the *Public Switched Telephone Network* (PSTN) takes place over landline trunked lines (called *trunks*) comprised of optical fibers, copper cables, microwave links and satellite links. The network configuration in the PSTN is virtually static, since the network addresses may only change when a subscriber changes residence. On the other hand, wireless networks are highly dynamic with the network configuration being rearranged every time a subscriber moves into the coverage region of a different base station. While fixed networks are difficult to change, wireless networks must reconfigure themselves for users within small intervals of seconds, to provide roaming and imperceptible handoffs between calls as a mobile subscriber moves around. Each country is responsible for the regulation of the PSTN within its borders. Over time, some government telephone systems have become privatized by corporations which provide local and long distance service for profit. [4]

Modern mobile telephone networks can be, generally, divided into two parts; the wireless cellular network that it used to communicate with mobile devices, nowadays known as *Radio Access Network* (RAN), and the landline, wired network that is based on the old PSTN and interconnects all the network elements of the operator, known as *Core Network* (CN).
Signalling System No. 7 (SS7) is a worldwide network that interconnects all telecom providers around the globe. In practice, it is a set of protocols used for communication inside the Core Network, for both the *Global System for Mobile Communications* (GSM) and the *Universal Mobile Telecommunications System* (UMTS), commonly known as 2G and 3G respectively. Primarily, it used for setting up and tearing down phone calls, sending short messages and other general information exchange, but it also enables the transmission of data in packets.

In particular, the process of placing voice calls in modern mobile networks is still based on SS7 technology, which dates back to the 1970s. At that time, safety protocols involved physical security of hosts and communication channels, making it impossible to obtain access to an SS7 network through a remote unauthorized host. In the early 21st century, a set of signaling transport protocols called SIGTRAN were developed, that allows the use of IP networks to transfer messages. However, even with these new specifications, security vulnerabilities within SS7 protocols remained. As a result, an intruder is able to send, intercept and alter SS7 messages by executing various attacks against mobile networks and their subscribers.

Vulnerabilities in SS7 based mobile networks allow an intruder with basic skills to perform dangerous attacks that may lead to direct subscriber financial loss, confidential data leakage or disruption of communication services. Such attacks as discovering a subscriber's location, disrupting a subscriber's service, SMS interception, Unstructured Supplementary Service Data (USSD) forgery requests (and transfer of funds as a result of this attack), voice call redirection, conversation tapping and disrupting the availability of a mobile switch. [6]

Regardless of what security assurances mobile network operators provide, there is plenty of hard evidence that in fact shows how vulnerable these systems are. Lately, it seems like a common occurrence when private telephone conversations or pictures of government officials, celebrities and business leaders appear on the Internet, even though these individuals usually take extra precautions when it comes to their personal privacy and safety. [6]

The SS7 system, which dates to the 1970's, is riddled with security vulnerabilities like the absence of encryption or service message validation. For a long time, it didn't pose any risk to subscribers or operators, as the SS7 network was a closed system available only to landline operators. The network evolved to meet new standards of mobile connection and service support and in the early 21st century, a set of signalling 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 signalling 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[**?**]. In 2015, Berlin hackers from SR Lab were able to intercept SMS correspondence between Australian senator Nick Xenophon and a British journalist during a live TV broadcast of the Australian program *"60 Minutes"*. They also managed to geo-locate the politician during his business trip to Tokyo[**?**]. In 2013, Edward Snowden identified SS7 exploitation as one of the techniques used by the National Security Agency. [7]

Second and third generations of mobile networks (2G/3G) are based on SS7. Signalling System 7 (SS7) is a set of signalling protocols developed in 1975, used to exchange information among different elements of the same network or between networks (call routing, roaming information, features available to subscriber etc.). The current mobile generation (4G) uses Diameter as a replacement for SS7. However, all generations (2G/3G/4G) have kept the same interconnect principles, inherited from wireline networks. Public Switched Telephone Networks (PSTN) have been interconnected based on trust, between a small number of operators, within a closed group. Deregulation and market opening have made access to interconnect networks much easier resulting in a huge number of operators interconnected worldwide. [5]

SS7 was standardized in the 70's before the widespread adaption of the Internet protocol (IP), thus it was created by closed groups of organizations, like the *International Telecommunication Union* (ITU) and the *European Telecommunication Standards Institute* (ETSI), in comparison with the public system of standardization (RFC) followed by IEEE.
Back then, engineers could not imagine the magnitude of the problems created when they designed an international communication system that lacks any notion of security either in the authentication or the confidentiality domain.
In fact, the whole structure was based on the *"walled–garden"* paradigm; every node of the network was considered *a-priori* trustworthy and legitimate, even beyond the borders of an operator. An opinion that may stood firm forty years ago, when all of the telecom operators were national, state controlled, public-interest companies.

Afterwards, SS7 became more exposed due to the increased liberalization of the telecom market, in conjunction with the industry switching to IP technology. This *"walled garden"* has acquired a number of possible entry points.
Security researchers have been drawing media attention to the problem of SS7 weaknesses since 2014. In the following years, new attacks were published in the media and security literature. Most of these attacks only use functions provided by mobile networks to succeed. The only requirement for a successful attack is access to an SS7 network, which is typically reserved to network operators. But, nowadays SS7 access can be easily purchased. [5]
With access to SS7 and a victim's phone number, an attacker can listen to a conversation, pinpoint a person's location, intercept messages to gain access to mobile banking service, send a USSD command to a billable number, and conduct other attacks.
It's important to note that it is still impossible to penetrate the network directly. It must be accessed via an SS7 gateway. But getting access to an SS7 gateway is relatively easy. An attacker can obtain the operator's license in countries with lax laws or purchase access through the black market from a legal operator for several thousand dollars. If there is an engineer in a hacker group, they will be able to conduct a chain of attacks using legitimate commands or connect their equipment to SS7. There are several ways to get into a network using hacked carrier equipment, GGSN or a femtocell. [7]
Meanwhile, telecom personnel is not used to security incidents as is the internet counterpart, as is the culture of the internet. [2]

SS7 attacks may be performed from anywhere and an attacker doesn't have to be in physical proximity to a subscriber, so it's almost impossible to pinpoint the attacker. Additionally the hacker does not need to be a highly skilled professional either. There are many applications for SS7 on the internet, and cellular carriers are not able to block commands from separate hosts due to the negative impact this would have on service and the violation of roaming principles. [7]

Lately, turns out that SS7 networks have several built-in vulnerabilities, mostly because of the lack of Authentication between the *signalling nodes*. Many vulnerabilities were disclosed in the recent years, which allow attackers to exploit network communications for subscriber tracking, call interception, denial of services and other fraudulent actions.
Telephony is one of the most critical infrastructures of society, next to water and electricity, and subscribers, operators and national governments depend on its availability and security.

The number of successful attacks using other types of threats are changed insignificantly. The reason is that implementation of traffic filtering and blocking systems cannot compensate for SS7 architecture flaws. To minimize them, another approach is required. The following flaws allow various attacks: [8]

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

SS7 vulnerabilities are not new. One of the first public presentations about SS7 vulnerabilities was given in 2008 at the Chaos Computer Club Conference, in Germany. German researcher Tobias Engel showed how the location of a mobile phone could be determined [**?**]. However, the risks associated with SS7 vulnerabilities have long been understood. Well before Engel's demonstration, telecom engineers had warned that various attacks using SS7 were possible [2, 3, and 4]. Some governments also knew of the potential threats. For example, the book "How to Cheat at VoIP Security" by Thomas Porter and Michael Gough (2007) contains the following excerpt from an official US report about possible GSM threats:

> "The risk of attack has been recognized in the USA at the highest level with the President's office indicating concern on SS7. It is understood that T1, an American group, is seriously considering the issue." [5]

For obvious reasons, providers didn't want the public to know about these associated risks. However, the issue received publicity in 2013 when former CIA specialist Edward Snowden disclosed the fact that the National Security Agency (NSA) had been exploiting SS7 vulnerabilities to spy on people [10].
Soon after, a host of private companies began offering a range of commercially available services (like the ones described) to the general public. By example, USA based Verint Systems provides a service called SkyLock for determining the location of a mobile subscriber anywhere in the world. [6]

The Signalling System No. 7 (SS7)

In telecom, we describe as *Signalling* the messages exchanged between the nodes of the *Core Network* (CN), which actually *do not transfer user data*, but merely information related to user and service management. It is called signal as it really was until recently an electrical signal, like the 'wait' tone you could hear just before the beginning of a call, or the different frequencies for every dialled number, or the 'end' tone when the called party hangs up the phone.

Common Channel Signalling (CCS) is a digital communications technique that provides simultaneous transmission of user data, signalling data and other related traffic throughout a network. This is accomplished by using *out-of-band signalling channels* which logically separate the network data from the user information (voice or data) on the same channel. For second generation wireless communications systems, CCS is used to pass user data and control/supervisory signals between the subscriber and the base station, between the base station and the MSC, and between MSCs.
The SS7 signalling protocol is widely used for common channel signalling between interconnected networks. SS7 is used to interconnect most of the cellular MSCs throughout the world and is the key factor in enabling autonomous registration and automated roaming. [4]

All nodes in a SS7 network can be described as *Signalling Points* (SP). SS7 networks are composed of a number of different kinds of signalling points, each designed to meet different requirements. SPs are connected to each other using *"signalling links"*. Signaling links are logically grouped into a *"linkset"*. Links may be referenced as A through F links, depending on where they are in the network. Additionally, there are a number of ways in which signalling can be passed through the network and the use of a particular mode relates to a specific function of the signalling points concerned. [3]

SS7 is a data communications network that acts as the nervous system to bring the components of telecommunication networks to life. Call set-ups, inter-MSC handoffs, and location updates are the main activities that generate the maximum signalling traffic in a network, and which are all handled under SS7. Setting up of a call requires exchange of information about the location of the calling subscriber (call origination, calling-party procedures) and information about the location of the called subscriber. Either or both, of the calling and the called subscribers can be mobile, and whenever any of the mobile subscribers switches MSC under a handoff condition, it adds to the amount of information exchanged. [4]

In addition to setting up and releasing calls, SS7 is the workhorse behind a number of telecommunication services, including: [1]

- Telephone-marketing numbers such as toll-free and freephone
- Televoting (mass calling)
- Single Directory Number
- Enhanced 911 (E911), used in the United States
- Supplementary services
- Custom local area signaling services (CLASS)
- Calling name (CNAM)
- Line information database (LIDB)
- Local number portability (LNP)

- Cellular network mobility management and roaming
- Short Message Service (SMS)
- Enhanced Messaging Service (EMS), ringtone, logo, and cellular game delivery
- Local exchange carrier (LEC) provisioned private virtual networks (PVNs)
- Do-not-call enforcement

Although there are global standards for SS7, there are many regional differences that have lead to widespread variation in standards. The principal bodies responsible for the evolution of SS7 standards remain the *International Telecommunication Union – Telecommunication Standardization Sector* (ITU-T) and *American National Standardisation Institute* (ANSI) organizations, but the *European Telecommunication Standardization Institute* (ETSI), Bellcore and others continue to develop their own versions. While it is not important to know each standard, it is important to recognize the key differences and to be aware of the fact that SS7 is not a generic standard, but a collection of standards that follow the same core model. [3]

Differences in the user parts are not uncommon. For example, the UK telephony user part (now known as IUP) uses a message called an IFAM instead of the IAM used in standard TUP. ANSI ISUP, used within the United States does not support overlap dialing, whereas most other standards do. The result of this kind of differentiation is that there is often a requirement for a protocol converter at the boundary of two SS7 networks.
Similarly, many manufacturers do not wish to invest in numerous different SS7 variants, so rely on suppliers to offer conversion solutions. Of course, vendors wishing to deploy the most complete solution should partner with a SS7 supplier that can offer a comprehensive range of SS7 variants. [3]

Variation occurs at all layers of the SS7 protocol stack. MTP Point Code implementations, for instance, tend to fall into two camps – those which use the standard ITU-T 14 bit point code address scheme and those that use a derivative of the ANSI 24 bit point code scheme (Japan offers an unusual 16 bit version that has features of both). Expanding the length of the point code field allows many more addresses to be included within a particular network and allows for greater differentiation within the addressing scheme. [3]

There is only one international SS7 protocol defined by ITU-T in its Q.700-series recommendations.There are however, many national variants of the SS7 protocols. Most national variants are based on two widely deployed national variants as standardized by ANSI and ETSI, which are in turn based on the international protocol defined by ITU-T. Each national variant has its own unique characteristics. Some national variants with rather striking characteristics are the China (PRC) and Japan (TTC) national variants.[1]

[1] http://4g5gworld.com/wiki/signaling-system-number-7-ss7

SS7 Architecture

SS7 is really a suite of protocols that use a common transport mechanism for the distribution of messages between functional entities. This common transport layer is the *Message Transfer Part* or *MTP levels* (MTP1/2/3) and is responsible for reliable routing of the messages. Above this layer, there are a number of alternative functional blocks that perform functions like call control (ISUP, TUP), or search and retrieve information related to subscribers (SCCP, MAP, CAP, INAP). SS7 establishes a framework by which data is exchanged between systems in the network via dedicated signalling channels. [3]

Signaling is transferred using the packet-switching facilities afforded by SS7. These packets are called signal units (SUs). The Message Transfer Part (MTP) and the Signaling Connection Control Part (SCCP) provide the transfer protocols. MTP is used to reliably transport messages between nodes, and SCCP is used for noncircuit-related signaling (typically, transactions with databases). The ISDN User Part (ISUP) is used to set up and tear down both ordinary (analog subscriber) and ISDN calls. The Transaction Capabilities Application Part (TCAP) allows applications to communicate with each other using agreed-upon data components and manages transactions. [1]

SS7 is an outgrowth of the out-of band signalling standard first developed by the CCITT, the *CCS No. 6*. Further work caused SS7 to evolve along the lines of the ISO-OSI seven layer network definition, where a highly layered structure (transparent from layer to layer) is used to provide network communications.

Several protocols exist to support different types of services. The SS7 protocol stack provides an architecture which is, in many respects, similar, but which departs from the OSI model particularly in the higher layers. Even though the SS7 architecture does not comply with the OSI model, there is an abstract relation between the two.

At the bottom of the SS7 protocol stack, it is said that the lower three layers (MTP1/2/3) are equivalent to their corresponding in the OSI model (Physical, Link-local and Network). This is not completely true, because the MTP was originally designed to transfer call-control messages coming from the Telephony User Part (TUP). Therefore, it was designed to transfer only circuit-related signalling. In combination with the MTP, the SCCP can transfer messages that are not circuit-related. SCCP was developed after the MTP, and together with the MTP3, it provides the capabilities corresponding to Layer 3 of the OSI reference model. Because SCCP is OSI Layer 3 compliant, in theory it can be transmitted over any OSI-compliant network. [1]

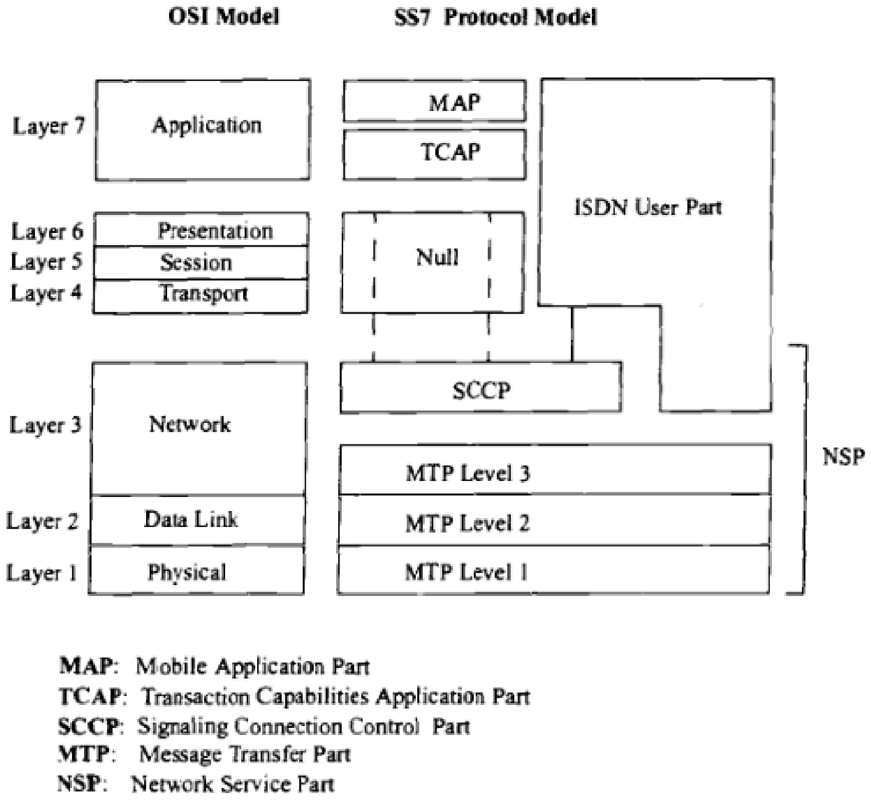
The lowest three layers of the OSI model are handled in SS7 by the network service part (NSP) of the protocol, which in turn is made up of three *Message Transfer Parts* (MTPs) and the *Signalling Connection Control Part* (SCCP) of the SS7 protocol. SCCP integrates two more addressing frameworks: one that enchants the old, *Point Code* (PC) routing system of MPT3, and another that uses an *incremental routing system*, that can provide every node with a globally unique address, the *Global Title* (GT). [4]

Message Transfer Part, MTP

MTP is divided into three distinct functional layers that perform specific tasks. Overall, it is concerned with the safe routing of messages and the management of SS7 links.

MTP Level 1 (MTP-1) provide an interface to the actual physical channel over which communication takes place. Primarily, this involves the conversion of messaging into electrical signal and the maintenance of the

Figure 1: Comparison of the OSI reference model and the SS7 protocol stack.



physical links through which these pass. Physical channels may include copper wire, twisted pair, optical fiber, mobile radio or satellite links, and all of them are transparent to the higher layers.

MPT Level 2 (MTP-2) correspond to the second layer in the OSI reference model and provide a reliable link for the transfer of traffic between two directly connected signalling points. Variable length packet messages, called *Message Signal Units* (MSUs), are defined in MTP-2. A single MSU cannot have a packet length which exceeds 272 octets and a standard 16 bit cyclic redundancy check (CRC) checksum is included in each MSU for error detection.
MTP-2 also provides flow control data between two signalling points as a means of sensing link failure. If the receiving device does not respond to data transmissions, MTP-2 uses a timer to detect link failure, and notifies the higher levels of the SS7 protocol which take appropriate actions to reconnect the link. [4]
With potentially large amounts of information being transmitted, MTP-2 must also monitor message flow control, sorting messages based on queues and buffers.

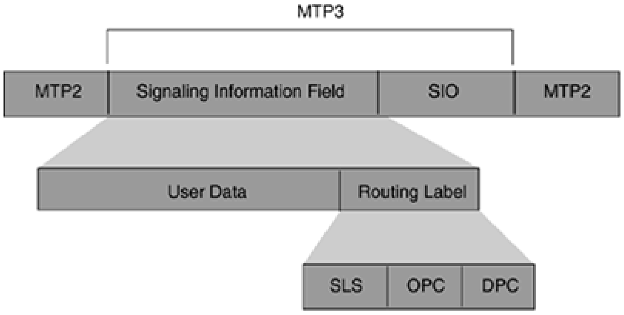
MTP Level 3 (MTP-3) ensures that messages can be delivered between signalling points across the SS7 network, regardless of whether they are directly connected. It includes such capabilities as node addressing, routing, alternate routing, and congestion control. MTP-3 performs two basic functions:

Signalling Message Handling is used for the delivery of incoming messages to their intended User Part and routing of outgoing messages toward their destination. MTP-3 uses the PC to identify the correct node for message delivery. Each message has both an *Origination Point Code (OPC)* and a *Destination Point Code* (DPC). The OPC is inserted into messages at the MTP-3 level to identify the SP that originated the

message. The DPC is inserted to identify the address of the destination SP. Routing tables within an SS7 node are used to route messages.
Each of the layers that sit above MTP-3 can be considered as its *"users"*. They rely upon MTP-3 for the safe delivery of messages they send to it and for the safe reception and onward routing of messages that are bound for them. Since there are several layers that can sit above MTP-3 (SCCP, ISUP, TUP, etc), there must be some way of indicating which layer should receive a particular message. *Message Discrimination*, as it is known, is an important function of MTP-3 and is the process by which a signalling point determines whether a packet data message is intended for its use or not.

Moreover, messages in MTP are called *Message Signal Units* (MSUs) and are divided into a number of sub fields that contain information that is important in message routing and ensuring transmission integrity. Each message header has a sub field known as the *Service Information Octet* (SIO) that allows message discrimination to take place. Each of the possible protocols that run at Layer 4 (SCCP, ISUP, TUP) has been allocated a particular value. MTP-3 inspects this value and then ensures that the data part of the message is passed to the correct receiving layer.
The *Signalling Information Field* (or SIF) contains information that allows routing to take place. MTP-3 will complete this field by adding the *Originating Point Code* (OPC) of the signalling point that generates the message and the *Destination Point Code* (DPC) of the signalling point for which it is bound. There many variations of the PC routing system. The ITU-T and ANSI Routing Labels are similar in structure, but differ slightly in size and meaning. The ITU-T Point Codes are 14 bits in length, while the ANSI Point Code is 24 bits in length. *Signalling Link Selector* (SLS) is an identifier used for load sharing across linksets and links. [1]

Figure 2: MTP-3 Routing Label Fields.

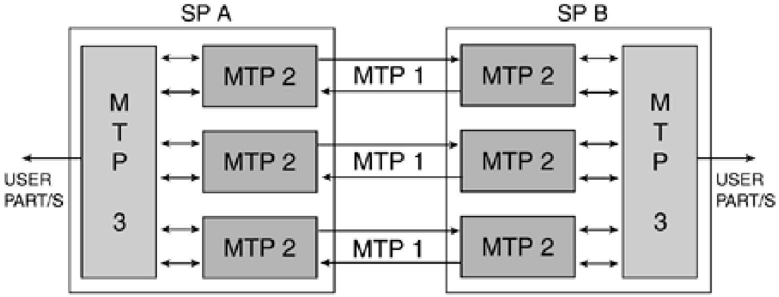


SS7 network nodes are called Signaling Points (SPs). Each SP is addressed by an integer called a Point Code (PC). The international network uses a 14-bit PC. The national networks also use a 14-bit PC, except North America and China, which use an incompatible 24-bit PC, and Japan, which uses a 16-bit PC.
SS7 routes are statically provisioned at each SP. There are no mechanisms for route discovery.

Signalling network management concerns the control of traffic routing, the links which bear the traffic and dealing with errors. It monitors linksets and routesets, providing status to network nodes so that traffic can be rerouted when necessary. This way, it allows the network to reconfigure in case of node failures and has provisions to allocate alternate routing facilities in the case of congestion or blockage in parts of the network. SS7 signalling links are able to carry information about many thousands of bearer circuits, so load balancing or *"loadsharing"* is essential to the efficient operation of the network. By distributing messages down available links in a linkset, MTP-3 is able to lessen the chances of a total breakdown in message

transmission and attempts to avoid congestion on a single link.
A single MTP-3 may control many MTP-2s, each of which is connected to a single MTP-1. The figure below outlines this relation.

Figure 3: Relation of MTP Levels.



Signalling Connection Control Part, SCCP

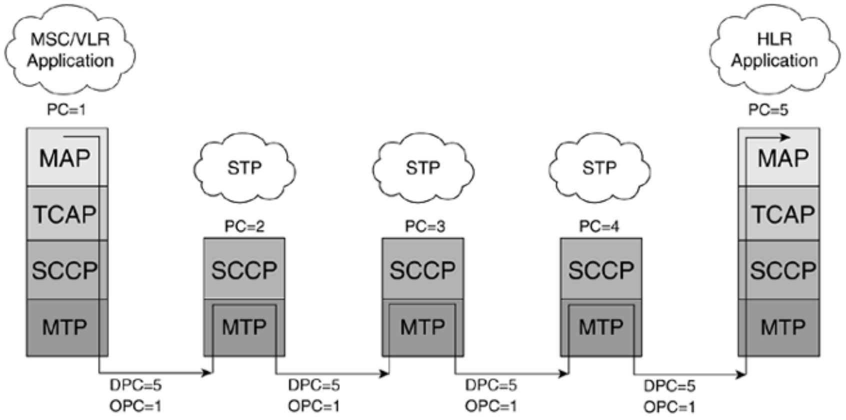
The *Signalling Connection Control Part* (SCCP) is an additional network protocol that enhances the routing system provided by the MTP-3. While the addressing capabilities of MTP are limited in nature, SCCP uses extended local addressing based on *Subsystem Numbers* (SSN), supplementary to the *Point Code* (PC) system of MTP3. Although an individual node can be identified by a PC, there may exist several components within this signalling point that provide functions to support different kinds of services. In this case, each component can be termed a "*subsystem*".
SCCP is able to reach any destination in the network by using a combination of the SSN and the PC address. Since the SSN is represented by a single byte in the MSU structure, there can be a maximum of 256 SSNs at a particular signalling point. [3]

There are a number of subsystems; the most common are: [1]

- Toll-free (E800)
- Advanced Intelligent Network (AIN)
- Intelligent Network Application Protocol (INAP)
- Customizable Applications for Mobile Enhanced Logic (CAMEL)
- Mobile Application Part (MAP)

SCCP addressing capabilities are flexible in contrast to those of MTP-3. As a result, the addressing capabilities are somewhat complex, thereby allowing several different combinations of routing parameters. SCCP provides a routing function that allows signalling messages to be routed to a Signalling Point based on dialled digits, for example. This capability is known as *Global Title Translation* (GTT), which translates what is called a *Global Title* into a signalling Point Code and a Subsystem Number so that it can be processed at the correct application.

Figure 4: Example of MTP-3 Point Code routing.



There are a number of subsystems. The SSN field is one octet in length and, therefore, has a capacity of 255 possible combinations. The globally standardized Subsystem Numbers that have been allocated by *3rd Generation Partnership Project* (3GPP) for use by GSM/GPRS/UMTS cellular networks are:

Figure 5: SSNs used in 2G & 3G cellular networks.

Bits	Subsystem	Bits	Subsystem
0000 0110	HLR	1111 1010	BSC
0000 0111	VLR	1111 1011	GMSC
0000 1000	MSC	1111 1100	SMLC
0000 1001	EIR	1111 1101	BSS O&M
0000 1010	AuC	1111 1110	BSSAP
1000 1110	RANAP	1001 0011	gsmSCF
1000 1111	RNSAP	1001 0100	SIWF
1001 0001	GMLC	1001 0101	SGSN
1001 0010	CAP	1001 0110	GGSN

Additionally, SCCP supports another extremely important means of routing data: *Global Title Translation* (GTT). It keeps SPs from having overly large routing tables that would be difficult to provision and maintain. A *Global Title* (GT) is a directory number that serves as an alias for a physical network address. A physical address consists of a Point Code and an application reference called a Subsystem Number (SSN). GT routing allows SPs to use alias addressing to save them from having to maintain overly large physical address tables. A centralized Signalling Transfer Point (STP) is then used to convert the GT address into a physical address; this process is called *Global Title Translation* (GTT). It provides the mapping of traditional telephony addresses (phone numbers) to SS7 addresses (PC and SSN) for enhanced services.
A *Global Title* (GT) is a form of address used when the SCCP is unable to produce a PC and SSN to route data effectively. Instead, it produces a Global Title message, which contains the data it has received and an indication of the kind of data it requires. The SCCP concerned does not actually know where to find the required information, but it does know of a place that will be able to locate it. In a given network, there may be only one location capable of dealing with Global Titles, and all other SCCP systems in the network should be connected to it.

GTT is particularly useful as it allows systems to gain information from outside their own network without knowing where to look for it. For example, roaming subscribers in a mobile network will not be able to register initially, as their Mobile Subscriber Number will not be recognized by any of the databases in the visited network. Global Title allows the visited network to interrogate a GTT location and determine the origin of the visitors so that they can be registered with their home networks. If a particular database is unavailable, the Global Title location can redirect the query to another without the knowledge of the interrogating SCCP.

Global Title also limits the information that given SPs need to retain and monitor. If each switch needed to know where to locate all of the information that it might require, the volume of data each would have to store would be unmanageable. Instead, there can be nominated points within the network to which such queries can be directed. This is another example of the way in which SS7 can provide powerful call routing and control management, as the protocols have a built-in capacity for enhancements. Once services such as these are abstracted from the telephone exchange itself, they can grow without reference to the original apparatus of call delivery, as they depend only upon the transfer of information. [3]

A common example for a GT would be a subscriber's personal phone number. The *Home Location Register* (HLR) stores details of every *Subscriber Identity Module* (SIM) card issued by the mobile operator. Each SIM has a unique identifier called *International Mobile Subscriber Identity* (IMSI) which is the primary key to each HLR record. Another important number associated with the SIM is the *Mobile Station International Subscriber Directory Number* (MSISDN), which is the telephone number used to make and receive calls.

Primary goal of this number is for making and receiving voice calls and SMS, but it is possible for a SIM to have other secondary MSISDNs associated with it for fax and data calls. This mean, that those number is also a primary key to the HLR record. The HLR data is stored for as long as a subscriber remains with the mobile phone operator. MSISDN is a primary key to the HLR record with maximum 15 digits without prefixes.[2]

For example, a number in America would be:

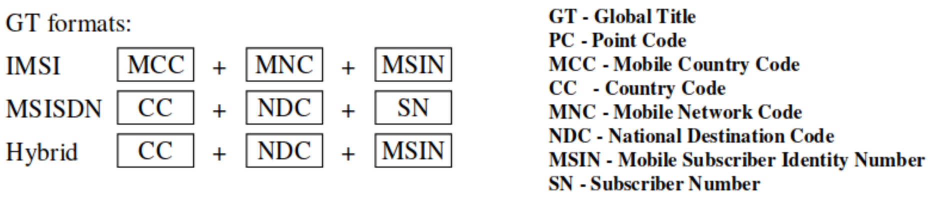
Figure 6: An example of MSISDN.

Global Title	MSISDN	13109976224	Landline Telephone Number
Country Code	CC	1	United States of America
National Destination Code	NDC	310	California
Subscriber Number	SN	9976224	John Doe

Also, the length of Global Titles is not restricted. That way, they allow for an infinite number of addresses that could identify every single device on the world. There exist many variations of the GT scheme, but all consist of a subscriber id, a network id and a country id. Every country is responsible for the regulation of telecom services, at a national level. Therefore, many different standards have emerged over time, with USA, Europe and Japan having the main differences.

[2] https://www.imsi.org

Figure 7: Variations of the Global Title format.

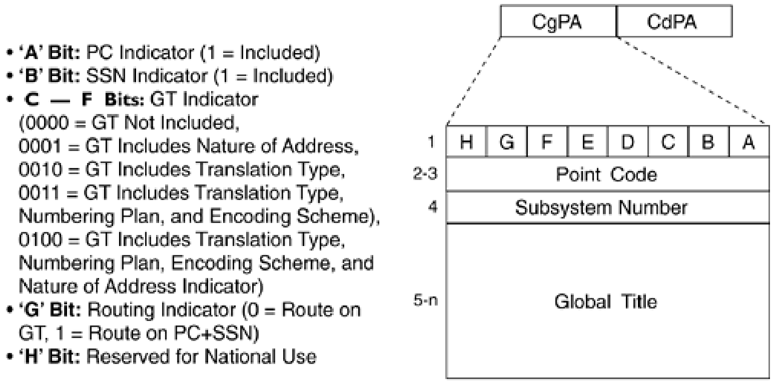


A GT is a telephone address. As such, the GT address must be translated into an SS7 network address (DPC+SSN) before it can be finally reached.
Global Title routing is used in cellular networks for exchanging messages when an HLR and VLR belong to different networks, or when several signalling points separate them. Global Title Translation is *an incremental indirect routing method* that is used to free originating signalling points from the burden of having to know every potential application destination, that is PC and SSN. [1]
However, as the specification puts it:[3]

> *"A GT is an address, such as dialled-digits, which does not explicitly contain information that would allow routing in the SS7 network."*

The GT is placed in the *"Calling Party Address"* (CgPA) and *"Called Party Address"* (CdPA) fields of the SCCP header. The next figure shows the fields that are found within the Calling Party Address and Called Party Address.

Figure 8: The subfields found in the Calling Party Address field of the SCCP header.


• 'A' Bit: PC Indicator (1 = Included)
• 'B' Bit: SSN Indicator (1 = Included)
• C — F Bits: GT Indicator
(0000 = GT Not Included,
0001 = GT Includes Nature of Address,
0010 = GT Includes Translation Type,
0011 = GT Includes Translation Type, Numbering Plan, and Encoding Scheme),
0100 = GT Includes Translation Type, Numbering Plan, Encoding Scheme, and Nature of Address Indicator)
• 'G' Bit: Routing Indicator (0 = Route on GT, 1 = Route on PC+SSN)
• 'H' Bit: Reserved for National Use
CgPA
CdPA
1
H
G
F
E
D
C
B
A
2-3
Point Code
4
Subsystem Number
5-n
Global Title

There are two general routing services are provided by SCCP. These are:

- the *connection-oriented* service class (voice)
- and the *connectionless* service class (datagram)

In connection-oriented routing, the communications path between the source and destination is fixed for the entire duration of the message transmission. Since the path through the network is fixed, the traffic

[3] ITU-T-T Q.714 Subclause 2.1

in connection–oriented routing arrives at the receiver in the exact order it was transmitted. Thus, it is particularly useful in real-time services, like voice transmission.

Connectionless routing, on the other hand, does not establish a firm connection for transport and instead relies on packet-based transmissions. Several packets form a message and each individual packet in a connectionless service is routed separately. Successive packets within the same message might travel completely different routes and encounter widely varying delays throughout the network, arrive out of order or get lost due to network failure. Typical packet overhead information includes the routing information and information needed to properly order packets at the receiver. [4]

Transaction Capabilities Application Part, TCAP

TCAP is primarily designed to be used for the querying and retrieval of information from databases. It formats data that can be presented using SCCP transport to a number of different databases. It can request that operations be carried out and await the result. It can also control the flow of information to the operation and the presentation of results to one or other of the higher layers that utilize TCAP's services. TCAP initiates queries and receives responses. In order to ensure that responses and queries can be correlated and sorted into the correct order, a numeric value is inserted into each query. The responding SP simply copies this number into its response so that the two can be cross-referenced.
There are two kinds of operations that are supported by TCAP. *"Dialogues"* take place between TCAP and one of the higher layers that use its services. Within a given Dialogue, many operations may be active. Each operation may yield a result known as a *Component*. Components can be viewed as instructions sent between applications. For example, when a subscriber changes VLR location in a GSM cellular network, his or her HLR is updated with the new VLR location by means of an *"UpdateLocation"* component.
TCAP also provides transaction management, allowing multiple messages to be associated with a particular communications exchange, known as a *transaction*. Components can be stored by TCAP until it is notified by a dialogue handling indicator to dispatch them as a single TCAP message. When TCAP receives a message, it unbundles all of the separate components and sends them individually to the appropriate higher layer. Since multiple dialogues can take place at any one time, each separate dialogue is given an individual identity that is conserved in the components. A TCAP transaction occurs when all stored components relating to a dialogue are presented to SCCP for routing to the relevant TCAP. [3, 1]

It is important to note that TCAP uses the SCCP connectionless service class. Although the applications (subsystems) use TCAP directly, they are considered SCCP users because TCAP is actually transparent. Common subsystems include Local Number Portability (LNP), Customizable Application Part (CAP), MAP, INAP, and AIN. [1]

Signalling Transport, SigTran

In order to connect to an SS7 network through the Internet, the SigTran function needs to be utilized, which essentially translates IP traffic to native SS7 signalling. *Signalling Transport* (SigTran) is IETF effort for signalling transportation over an IP network.

The IETF SigTran Working Group focused on defining architectural and performance requirements for transporting signalling over IP, evaluating existing transport protocols, and, if necessary, define a new transport protocol to meet the needs and requirements of signalling transport. They also defined methods of encapsulating the various signalling protocols. The framework was defined in RFC 2719. The document identified three necessary components for the SigTran protocol stack:

- Adaption Layer

- Common Transport Protocol (SCTP)
- Internet Protocol (IP)

Because of the deficiencies of UDP and TCP, a new transport protocol, was developed for transporting circuit-switched signalling, the *Stream Control Transmission Protocol* (SCTP).

SCTP is a new transport protocol, designed with the transport of time sensitive signalling data in mind. It remains flexible enough however, to be of general use. One question to be addressed is why the SigTran group went to all the trouble of defining a new transport layer protocol, when they could have chosen to use TCP?
The easiest way to run a SS7 layer over IP is to take the chosen layer, define an interface to the IP transport layer (TCP) and plug the two together. Unfortunately, there are some fundamental flaws with this approach:

- It's inflexible – once you've got SCCP running over IP/TCP, you are still without solution to run ISUP.
- It's unlikely that any other equipment vendor will have designed a SS7 to IP interface which is anything like yours. The structure of IP packets, holding the SS7 information, will appear alien to any other vendor's packets.
- There may be peer-to-peer management issues, such as connection establishment or quality of service negotiation, which have not been addressed.

It's clear from the above that we have to address the issues of standardization and scalability. One way of approaching this is to provide an *"adapter"* over TCP/IP which redefines the transport service in terms of what the upper signalling protocol would expect. In essence, to make TCP/IP look like a lower layer of SS7, for example MTP-3. Such an object is referred to as a *User Adaption* (UA) layer.

SCTP provides the following features:

- Acknowledged error-free, non-duplicated transfer of user data
- Data segmentation to conform to path MTU size (dynamically assigned)
- Ordered (sequential) delivery of user messages on a per "stream" basis
- Option for unordered delivery of user messages
- Network-level fault tolerance through the support of multi-homing, meaning that SCTP is able to connect more than 2 endpoints for redundancy, in contrast of TCP's strict Client–Server scheme.
- Explicit indications of application protocol in the user message
- Congestion avoidance behaviour, similar to TCP
- Bundling and fragmenting of user data
- Protection against blind denial of service and blind masquerade attacks
- Graceful termination of association
- Heartbeat mechanism, which provides continuous monitoring of reachability

SCTP is connection-oriented; it requires initial handshake. It supports multiple addresses per host. It avoids *"Head-of-Line Blocking"*, a usual problem in wireless communications. SCTP provides failure detection mechanisms. Multi-homing is achieved with the use of Transmission Sequence Number (TSN) parameter. SCTP was defined in RFC 2960.

- SCTP provides reliable transport, ensuring that data is transported across a network without error and in sequence, like TCP/
- Unlike TCP, the retransmission of lost messages in one stream does not block the delivery of messages in other streams. The use of multiple streams within SCTP resolves the head of line blocking you see with the use of TCP.
- Unlike TCP, SCTP ensures the sequenced delivery of user messages within a single stream.
- Unlike TCP, SCTP supports multi homing for added redundancy and faster retransmission of non-acknowledged packets.
- Unlike TCP, SCTP support built-in heartbeat, destination check.
- Unlike TCP, SCTP supports a security cookie against SYN flood attack.
- SCTP supports Selective Acknowledgements (SACK).

The User Adaptation (UA) layers encapsulate different SCN signaling protocols using SCTP. While each UA layer is unique in terms of the encapsulation because of the differences of the signalling protocols themselves, there are some common features among all UA layers. Firstly, support for seamless operation of the UA layer peers over an IP network, and also, support for the primitive interface boundary of the SS7 lower layer, which the UA layer replaces. For example, M2UA supports the primitive interface boundary of MTP-2. Additionally, support for the management of SCTP associations, as well as support for asynchronous reporting of status changes to layer management.
The SigTran Working Group has defined several UA layers, which include the following:

M2UA MTP2 User Adaption for the transport of MTP Level 3 messages between a SG and a MGC or IP database, defined in RFC 3331.

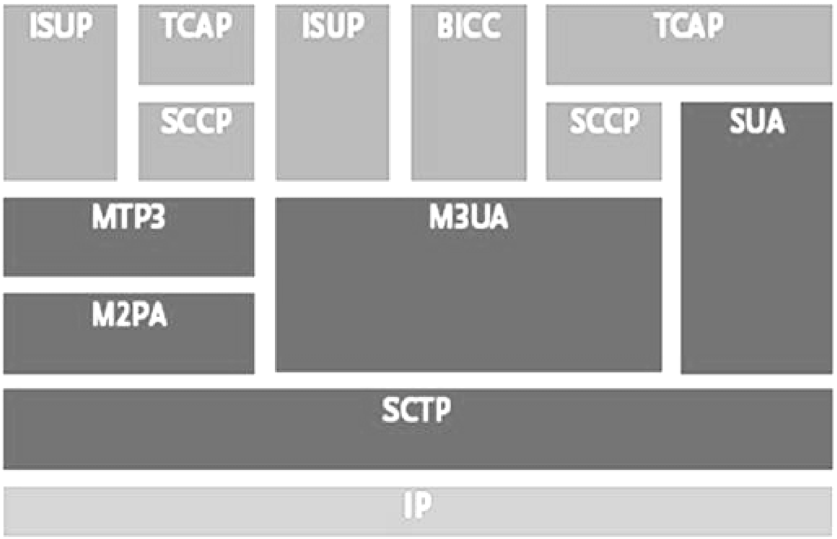
M3UA MTP3 User Adaption for the transport of SS7 User Part messages (SCCP) between an SS7 SG and a MGC, defined in RFC 3332.

SUA SCCP User Adaption for the transport of SCCP User Part messages (TCAP) from SG to IP nodes, defined in RFC 3868.

M2PA MTP2 Peer Adaption for the transport of MTP Level 3 data messages over SCTP. It can replace the MTP2 and so create an IP SS7 *link*. Defined in RFC 4165.

IUA ISDN User Adaption for the transport of Q.931 (telephony signalling) between an ISDN SG and a MGC.

Figure 9: The SigTran protocol stack.



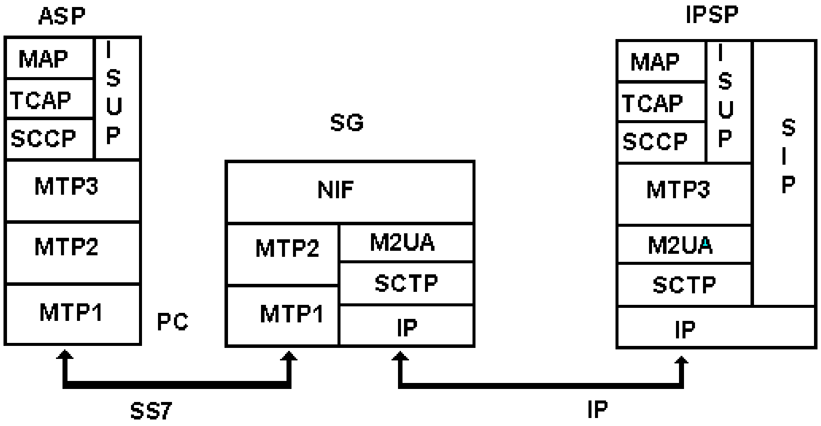
A *Signaling Gateway* (SG) is a signalling agent that sends and receives SS7 native signalling at the edge of the IP network. An SG appears to the SS7 network as a Signaling Point and contains a set of unique SG Processes, of which one or more is normally actively processing traffic. Where a SG contains more than one SGP, the SG is a logical entity, and the contained SGPs are assumed to be coordinated into a single management view to the SS7 network and the supported Application Servers. An SG must be capable of distributing incoming SS7 signalling messages to the appropriate Application Server. This is achieved with the use of a *Routing Key*.

A Routing Key is a set of SS7 parameters and parameter values that describe the routing information for a particular Application Server Process. It serves the MTP3 and SCCP User Adaption Layers (M3UA, SUA). MTP2 is point to point, so M2UA does not need routing aid. It is uniquely identified by a 32-bit value, the *Routing Context*. The parameters can be any of the following:

- Network Indicator (NI) (MTP3)
- Service Indicator (SI) (MTP3)
- Destination Point Code (DPC) (MTP3)
- Originating Point Code (OPC) (MTP3)
- Subsystem Number (SSN) (SCCP)

Traffic increased by local Number Portability and SMS has pushed SS7 networks beyond capacity. SigTran allows PSTN networks to offload traffic into IP networks. PSTN infrastructure is many times larger and far reaching than IP networks. SigTran will last as long as PSTN networks last.

Figure 10: A Signalling Gateway architecture operating on M2UA.



A common case of a client connecting from an IP based device would require the following steps.

Firstly, SCTP association requires both the IP address and port of the client, as well as that of the server. Also, note that SCTP layer can be configured to run over TCP for transport, rather than actual SCTP, which requires the 'lkstcp' kernel module in order to run and is only considered useful in wireless environments.

Next is the M3UA layer, which defines the Routing Context and the Network Appearance, prior to creation of the ASP and the routing association.

The rest of the layers define SS7 specific parameters, which may/should vary from provider to provider. Namely, SCCP requires the configuration of SS7 addressing, such as 'Server SPC', 'Client SPC', 'Network Indicator' and 'SSN'. Remember that routing in SS7 can be achieved either through Point Code format (PC+SSN), or with the use of Global Titles (IMSI/MSISDN).

Finally, TCAP and MAP define the actual service to be implemented, along with its parameters. This part of the stack we will try to exploit.

Mobile Application Part, MAP

Global System for Mobile communications (GSM) is the most popular digital cellular network standard in terms of architecture. It was formulated by the *European Telecommunication Standard Institute* (ETSI). The protocols that are found in GSM perform functions as mobility management and call processing. Namely, *Base Station Subsystem Application Part* (BSSAP) and *Mobile Application Part* (MAP) are two applications (or subsystems) that utilize the underlying functionality of the SS7 protocols and network.

The *Mobile Application Part* (MAP) is a SS7 protocol that provides an application layer functionality to the various signalling points in GSM and UMTS core networks to communicate with each other and provide services to mobile end-users. MAP allows implementation of functions such as location updating, roaming, SMS delivery, handover, authentication, and incoming call routing information. The MAP protocol uses the TCAP protocol to transfer real-time information. Therefore, MAP only makes use of the connectionless classes (0 or 1) of the SCCP. [1]

In GSM, every mobile phone device is called a *Mobile Station* (MS) and plays the role of an *"agent"* between the subscribers and the network. In order to authenticate with the network, every MS uses a "smart" card provided by the operator, that is called *Subscriber Identity Module* (SIM).
GSM was unique in the use of SIM cards to break the subscriber ID apart from the equipment ID. The SIM card is fully portable between *Mobile Equipment* (ME) units. This allows many features that we take for granted, such as being able to swap MS simply by swapping our SIM card over. All functionality continues seamlessly, including billing, and the telephone number remains the same.
An MS has several associated identities, including the *International Mobile Equipment Identity* (IMEI), the *International Mobile Subscriber Identity* (IMSI), the *Temporary Mobile Subscriber Identity* (TMSI) and the *Mobile Station ISDN Number* (MSISDN). The following sections examine each of these identities, in turn, so that signalling sequences in which they are involved make sense. [1]

IMEI Each ME has a unique number, known as the IMEI, stored on it permanently. The IMEI is not only a serial number; it also indicates the manufacturer, the country in which it was produced, and the type approval. It is assigned at the factory. To display the IMEI on most MSs, enter '`*#06#`' on the keypad.

IMSI Each subscriber is assigned a unique number, which is known as the IMSI. The IMSI is the only absolute identity a subscriber has within GSM, and as such, it is stored on the SIM. The SIM contains the subscriber's subscription details and grants the subscriber service when placed into a piece of ME. Among other purposes, it is used for subscriber billing, identification and authentication when roaming. In GSM, IMSI is divided into three parts:

MCC the Mobile Country Code that refers to the country of origin (3 digits),

MNC the Mobile Network Code which identifies the subscriber's home PLMN (2 or 3 digits) and

MSIN the Mobile Station Identification Number identifies the mobile subscriber (10 or less digits).

Together, the IMSI cannot exceed 15 digits in length.

TMSI A TMSI is an alias used by the VLR and the SGSN in GPRS enabled networks, to protect subscriber confidentiality. It is temporarily used as a substitute for the IMSI to limit the number of times the IMSI is broadcast over the air interface, because intruders could use the IMSI to impersonate a GSM subscriber. The VLR assigns the TMSI to an MS during the subscriber's initial transaction with an MSC. Because the TMSI has only local significance, each network administrator can choose its structure to suit his needs. To avoid double allocation, it is generally considered good practice to make part of the TMSI related to time.

MSISDN The Mobile Station ISDN Number is what the calling party dials in order to reach the called party. In other words, it is the mobile subscriber's directory number. A subscriber might have more than one MISDN on their SIM. In GSM, MSISDN can be divided into three sectors:

CC The Country Code that identifies a specific country,

NDC the National Destination Code that relates to a geographical area within a country or a national mobile network and

SN the Subscriber Number which identifies a subscriber in a particular network.

MSRN The Mobile Station Roaming Number is a temporary identifier that is used to route a call from the gateway MSC to the serving MSC/VLR. The serving MSC/VLR is the MSC/VLR for the area where the subscriber currently roams. The VLR assigns an MSRN when it receives a request for routing information from the HLR. When the call has been cleared down, the MSRN is released back to the VLR.

Mobility Management

In cellular telephony systems, the subscriber's location can change drastically without the system being aware. For example, the subscriber might switch his cell phone off just before boarding a plane, and then switch it back on in a new country. There is no direct relationship between the subscriber's location and the cellphone number.

Because the location and other information are needed before a call can be delivered to a subscriber, such mobile-terminated calls require a large amount of initial signalling. In contrast, mobile-originated calls place far less initial signalling overhead, because the radio system to which the subscriber is connected knows the subscriber's location. [1]

Furthermore, because a subscriber may be on the move, the BTS, the BSC and even the MSC can change. These changes require a lot of non circuit-related signalling, particularly if the subscriber is currently engaged in a call The subscriber should not be aware that such handovers take place. Mobility management entails keeping track of the MS while it is on the move. The mobility management procedures vary across three distinct scenarios, namely:

- MS is turned off
- MS is turned on but is idle
- MS has an active call

In the first scenario, when it cannot be reached by the network because it does not respond to the paging message, the MS is considered to be in the turned-off state. In this scenario, the MS obviously fails to provide any updates in relation to changes in Location Area (LA), if any exist. In this state, the MS is considered detached from the system (IMSI detached).

In the second scenario, the MS is in the ready state to make or receive calls. The system considers it attached (IMSI attached), and it can be successfully paged. While on the move, the MS must inform the system about any changes in LA; this is known as location updating.

In the third scenario, the system has active radio channels that are allowed to the MS for conversation/data flow. The MS is required to change to new radio channels if the quality of current channels drops below a certain level; this is known as handover. The MSC (sometimes BSC) makes the decision to handover an analysis of information that is obtained real-time from the MS and BTS. [1]

If a mobile terminal moves from one cell to another during an active call, it should be clear that the call must be handed over to the new cell; this should be done in a fully transparent fashion to the subscriber. This process is known as a *handover*. The Mobile Switching Centre (MSC) monitors the strength of the incoming signal from the cellular phone (known as MS). When the signal power drops below a certain level, it indicates that the user might have entered another cell or is at the edge of the current cell. The MSC then checks to see if another cell is receiving a stronger cell. If it is, the call is transferred to that cell. The approximate location of an MS, even if idle, has to be tracked to allow incoming calls to be delivered.

Handovers and location tracking involve extensive and complex SS7/C7 signaling. In a cellular network, most signalling relates to the support of roaming functionality. Only a fraction of the signalling relates to call control. [1]

Authentication and Subscriber Management

An HLR uses subscriber management procedures to update a VLR with specific subscriber data when the subscriber's profile is modified. A subscriber's profile can be modified, because the operator has changed the subscription of the subscriber's basic services or one or more supplementary services. A subscriber's profile might also be modified, because the subscriber himself has activated or deactivated one or more supplementary services. Subscriber management uses the following two operations. [1]

- InsertSubscriberData
- DeleteSubscriberData

Call Handling

The call handling procedures primarily retrieve routing information to allow mobile terminating calls to succeed. When a mobile originating or a mobile terminating call has reached the destination MSC, no further MAP procedures are required.
Call handling does not have subcategories of operations; it simply has the following two operations:

- SendRoutingInfo
- ProvideRoamingNumber

Because of past location updates, the HLR already knows the VLR that currently serves the subscriber. To obtain a Mobile Station Roaming Number (MSRN), the HLR queries the VLR using the operation **ProvideRoamingNumber** with the IMSI as a parameter. The VLR assigns an MSRN from a pool of available numbers and sends the MSRN back to the HLR in an acknowledgement.
Because the GMSC now knows the MSC in which the MS is currently located, it generates an **IAM** with the MSRN as the called party number. When the MSC receives the IAM, it recognizes the MSRN and knows the IMSI for which the MSRN was allocated. The MSRN is then returned to the pool for use on a future call.

Autonomous Registration and Automated Roaming

Autonomous registration is a process by which a mobile notifies a serving MSC of its presence and location. The mobile accomplishes this by periodically keying up and transmitting its identity information, which allows the MSC to constantly update its customer list. The registration command is sent in each control channel at five or ten-minutes intervals and includes a timer value which allows the mobile terminal to determine the precise time at which it should respond to the serving base station. Each mobile reports its MCC and MSISDN during the brief registration transmission so that the MSC can validate and update the customer list. The MSC is able to distinguish home users from roaming users based on the MCC of each active user and maintains a real-time user list in the Home Location Register (HLR) and Visitor Location Register (VLR). Autonomous registration allows the MSCs of neighboring systems to automatically handle the registration and location validation of roamers so that users no longer need to manually register as they travel. The visited system creates a VLR record for each new roamer and notifies the home system so it can update its own HLR. [4]

Second generation wireless networks have introduced new network architectures that have reduced the computational burden of the MSC. GSM has introduced the concept of a Base Station Controller (BSC), which is inserted between several base stations and the MSC. This architectural change has allowed the data interface between the Base Station Controller and the MSC to be standardized, thereby allowing carriers to use different manufacturers for MSC and BSC components. Eventually, wireless network components, such as the MSC and BSC, will be available as off-the-shelf components, much like their wireline telephone counterparts. [4]

All second generation systems use digital encoding and digital modulation. The systems employ dedicated control channels (CSS) within the air interface for simultaneously exchanging voice and control information between the subscriber, the base station and the MSC while a call is in progress. The mobile units in these networks perform several functions, such as received power reporting, adjacent base station scanning, data encoding and encryption. [4]

MAP can also be used to enable communication between the HLR and the MS directly. For example, a subscriber can query the central network regarding one of his identifiers, like IMEI, or regarding the balance of his call and SMS credits. This kind of communication is achieved through the use of a supplementary service, called *Unstructured Supplementary Service Digits* (USSD). It is called *supplementary*, as it allows each operator to develop its own versions of what kind of information may be available this way. They can also add extra, custom applications, that are not defined in the standard. For each application, the subscriber dials a specific sequence of digits on his MS, usually starting with an asterisk, or a hash. For example, according to the standard, one can query the HLR about his IMEI with the sequence: `*031*` and his MSISDN number.

SS7 Network Elements

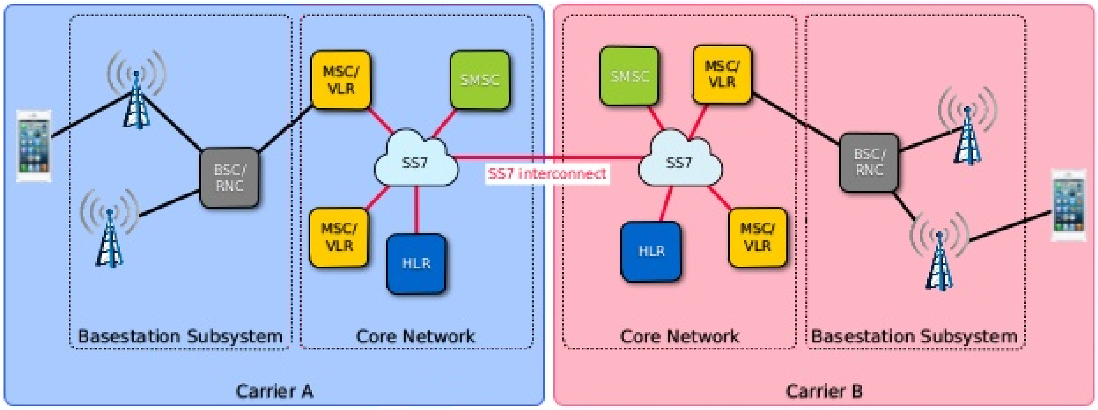
A mobile operator core network can be very complex, since it usually contains multiple application level servers, each serving a different purpose. New kind of services have always been added during all these years, which finally leads to a very complex network structure. Main elements consist of the central database for location (HLR), the client switch (MSC), a server for authentication (AuC), another for billing and accounting (PCRF), along with numerous gateway interfaces to other types of networks (SGSN/GGSN/MGW) and other common switches and routers (STP).

Second generation networks access several databases for authentication of mobiles, location updates, billing, etc. The visitor location database, home location database and the authentication center are the major databases that are accessed by various processing elements in the network.

The MSC uses the SS7 signalling network for location validation and call delivery for its roaming users and relies on several information databases. These database are the home location register (HLR), the Visitor Location Register (VLR) and the Authentication Center (AuC), which are used to update location and registration records for all subscribers in the network at any time. These databases may be co-located at the MSC or may be remotely accessed.

SS7 networks always follow a strict hierarchical architecture and GSM utilizes a cellular structure. Each cell is hexagonal in shape so that the cells fit together tightly. Each cell contains a *Base Transceiver Station* (BTS), which is an antenna that communicates with all the terminal devices inside the cell. Cells are grouped together in *Location Areas* that are controlled by a single Base Station Controller (BSC). Many BSCs are dictated by a single MSC, while every MSC is paired with a local location database, the *Visitor Location Register*, but all of them query the same central location database (HLR) or Authentication Center.
Below is a simplified view of two interconnected SS7 networks:

Figure 11: SS7 network overview.



BTS The *Base Transceiver Station* provides the connectivity between the cellular network and the Mobile Station via the air interface. The BTS houses the radio transceivers that define a cell and handles the radio interface protocols with the mobile station.

BSC A number of BTSs are connected to the *Base Station Controller* on an interface that is known as the Abis interface. It manages the radio interface channels, such as setup, release, frequency hopping, and handovers.

MSC The *Mobile Switching Center* is the network subsystems' central component. Because a large number of BSCs are connected to an MSC, an MSC is effectively a regular ISDN switch. The MSC provides routing of incoming and outgoing calls and assigns user channels on the A-interface.

It acts like a normal switching node of the PSTN or ISDN and provides all the necessary functionality for handling a mobile station, including registration, authentication, location updating, inter-MSC handovers, and call routing to a roaming subscriber.

HLR The *Home Location Register* can be regarded as a huge database that contains the information for hundreds of thousands of subscribers. Every PLMN has at least one HLR. While there is logically one HLR per GSM network, it might be implemented as a distributed database.

The HLR contains all administrative data that are related to each subscriber, his registration info along with his current location. The location of each mobile station is stored in the HLR, in order to be able to route calls to the mobile subscribers served. The location information is simply the VLR address that currently serves the subscriber. An HLR does not have direct control of MSCs.

Below is the critical info held in an HLR:

- IMSI
- IMEI

- MSISDN
- Authentication keys of subscriber
- Subscriber latest location (VLR)
- Subscription profile
- Supplementary services
- Services allowed (call forwarding, barring, etc...)

VLR Like the HLR, the *Visitor Location Register* contains subscriber data. However, it only contains a subset (selected administrative information) of the data stored in HLR. Each VLR is responsible for a specific region and keeps information regarding call control and service provision. These data are only temporarily stored while the subscriber is served by the particular VLR. A VLR is responsible for one or several MSC areas, but is usually deployed in pair with a MSC, for speed and simplicity reasons.

Every subscriber roaming in a specific region is attached/connected to the VLR responsible for this region. The VLR acts as a temp database for the period of the roaming subscriber.

When a subscriber roams into a new MSC area, a location updating procedure is applied. When the subscriber roams out of the area that is served by the VLR, the HLR requests that it remove the subscriber-related data.

EIR The *Equipment Identification Register* is the database that contains a list of all valid handset equipment on the network. Each Mobile Station is identified by its IMEI. An IMEI is marked as invalid if it has been reported stolen or is not type approved.

AuC The *Authentication Center* is a protected database that stores a copy of the secret keys that are stored in the subscriber's SIM card and are used for authentication and ciphering on the radio channel.

SGSN The *Serving GPRS Support Node* is responsible for delivering data packets from and to the mobile stations. Its tasks include packet routing and transfer, mobility management, authentication and charging functions. The location register of the SGSN stores location information, such as current cell and current VLR and user profiles, such as IMSI and addresses used in the packet data network. SGSNs detect subscribers in their service area, query HLRs to obtain subscriber profiles and maintain a record of their location.

GGSN The *Gateway GPRS Support Node* maintains routing information that is necessary to tunnel the Protocol Data Units (PDUs) to the SGSNs that serve specific mobile stations. Other functions include network and subscriber screening and address mapping.

SMSC Is a gateway MSC that is responsible for delivering short messages (SMS) to subscribers. SMSs may be temporarily stored on the SMSC in case the receiving subscriber is unreachable.

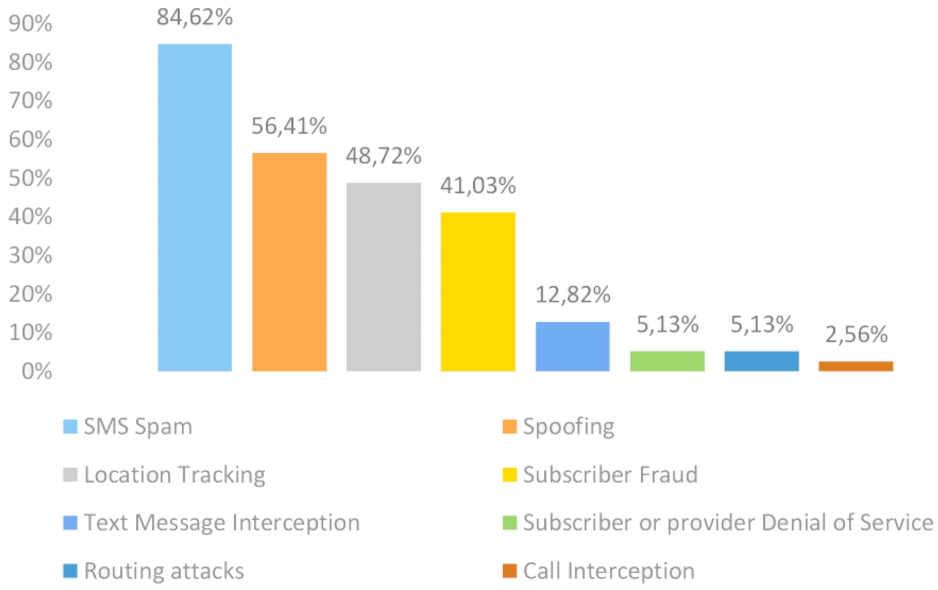
STP The *Signalling Transfer Point* acts as a router for the operator, that is responsible for all the routing, path determination and relaying of SS7 signalling messages.

Attacks on GSM Networks

Nowadays, mobile networks are the most dynamic part of critical communication infrastructures and the key medium used to perform daily activities ranging from voice and text messaging to providing signalling for emergency services and critical infrastructure.

According to Enisa [5], the most common type of attacks include SMS spamming, subscriber location tracking and identity spoofing. There is also a significant amount of fraudulent attacks, that aim to leverage monetary expenses to other unsuspicious subscribers. The figure below outlines the percentage of each incident type.

Figure 12: Common type of attacks.



SMS traffic is still a big source of revenue for mobile operators. Even if SMS peer-to-peer traffic decreases every year, SMS traffic from applications to users still increases significantly. Attackers have started to find new ways to bypass charging associated with SMS termination. That is why SMS Spam attack is a type of incident that almost every operator had faced. [5]

Tracking attacks are generally easy to perform. Furthermore, detection of these attacks is more subject to false positives than any other type of attacks. The main cause for such false positives is misconfiguration. In many cases, the operator cannot distinguish between traffic coming due to misconfiguration errors or because of a real incident. Therefore, the occurrence of such an attack is most probably overrated. [5]

Intercept attacks are more complex and require the attacker to keep a connection open in the network, waiting for victims to communicate. While operators have observed such kind of incidents, they still count as the least part of the perceived attacks. However, publicly available tools will make the deployment of intercept attacks easier and an increase is expected for the coming years. [5]

Denial of service attacks involve procedures associated with the reset of a Mobile Station. Thus, their impact is limited to a part of the network, usually much less than the whole infrastructure. Denial of service attacks may also affect a specific component, in which case the impact is again limited to a part of the network. Small-scale denial of service attacks are harder to detect. [5]

Common characteristics of these attacks are:

- An intruder doesn't need sophisticated equipment. A Linux based computer and a publicly available SDK for generating SS7 packets is all it takes. There is also an increasing amount of ready open-source platforms.
- After performing an initial attack using SS7 commands, the intruder is able to execute additional attacks using the same methods. For instance, if an intruder manages to determine a subscriber's location, only one further step is required to intercept SMS messages, commit fraud, etc.
- Attacks are based on legitimate SS7 messages. Therefore, you cannot simply filter messages as it may have a negative impact on the overall quality of service.

In many instances, a common misconception is that security breaches like these are very complicated and expensive to execute and can only be accomplished by high-ranking security intelligence agencies, organized crime or the most sophisticated hackers. This perception is understandable, since most people are trained to view a mobile communication network as a system made up of only the most cutting edge technologies. However, in reality a telecommunications network is a complex system built on subsystems that each have different technological levels, with the security of the whole network usually defined by the security level of the weakest link. [6]

An attacker can be a person or a group of people sufficiently qualified to build a node to emulate that of a mobile operator. To access an SS7 network, attackers can acquire an existing provider's connection on the black (underground) market and obtain authorization to operate as a mobile carrier in countries with lax communication laws. In addition, any hacker who happens to work as a technical specialist at a telecommunications operator, would be able to connect their hacking equipment to the company's SS7 network. In order to perform certain attacks, legitimate functions of the existing communication network equipment must be used. There is also an opportunity to penetrate a provider, through a cracked device (GGSN or a femtocell) at the edge of the network. Besides having different ways of accessing an SS7 network, attackers likely also have different motives for doing so including performing fraudulent activities, obtaining a subscriber's confidential data or disrupting service for certain subscribers or the whole network. [6]

In order to attack a SS7, access to the SS7 network is first required. This can often be found at VoIP providers, SMS providers, HLR lookup web application providers, you just need to dig deeper to find a suitable provider. The providers should provide the following parameters:

1. The Global Title that you should use (client GT).
2. The Point Code that you should use (client PC).
3. The peer Point Code of your provider (peer PC).
4. The IP address of your provider's peer, for SCTP association and the used port number (peer IP, peer Port).

From that point on, all you need is a public IP address assigned to your client machine that runs the code and your provider will allow access from her side and route traffic so that you can reach all the operators that she is connected to.

There is a number of possible MAP messages that could prove to be useful. However, these are all legitimate GSM requests, that are supposed to be transferred between specific network components, particularly the Home Location Register of the victim, as well as the MSC currently serving him. They implement basic functionalities of the Core Network, regarding call management, mobility management, user authentication, billing, etc. A complete list of MAP messages supported by the GSM specification can be found in Appendix A.
The attacker, on the other side, needs to spoof her identity every time, so that the requests appear natural. In fact, the absence of authentication measures or location validation makes it possible for her to even use the same GT address on every transaction. The queried HLR is unable to validate any credentials, simply because there is none! Nevertheless, spoofing the attackers identity is always a good practice and she should be very cautious about it. As we have seen, a lot of mobile operators are installing firewalls and other filtering mechanisms at the edge of their network, that could possibly identify suspicious traffic, like a particular GT address being used by several different components simultaneously.

Subscriber location tracking

A mobile terminal exchanges data with the serving network continuously, as long as it is connected to that network. The smallest element of these transactions is called *"Paging request"* and is used to update end user's location, activity, availability and signal strength. These requests are initiated by the visited serving network periodically, and are stored in the VLR currently responsible for the subscriber. The actual delay between each request is dictated by the operator, based on optimization and number of users currently served, but usually takes a few minutes.

End–user's state, like geographical location, is stored in the operator's central database, the HLR. To get this information, HLR needs to find the Base Station that served the terminal most recently. This kind of information is stored in the records of the VLR that is responsible for that area.
To minimize transactions, the HLR only contains location information about the MSC/VLR to which the subscriber is attached. The VLR contains more detailed location information, such as the location area in which the subscriber is actually roaming. As a result, the VLR requires that subscriber's location information be updated every time he changes location area. The HLR only requires his location information to be updated if the subscriber changes VLR. [1]

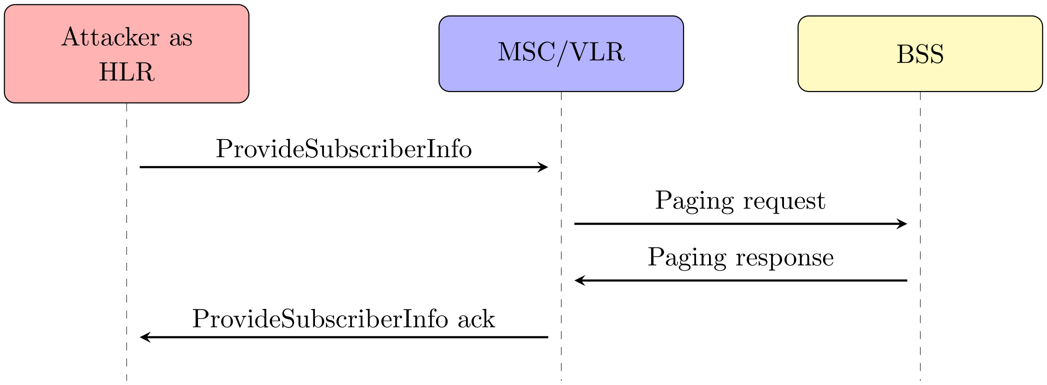
In order to get this kind of information out of the HLR, one may simply send a request named **SendRouting-InfoForSM**, which only requires the knowledge of subscribers telephone number (MSISDN). Since the HLR entity is central and unique for every operator, it can derived from the *Country Code* (CC) and *Operator Code* (MNC). The response to that message is instant, and provides routing information to find the subject in question, like the SS7 address *"Global Title"* (GT) of the MSC/VLR currently serving the mobile terminal. This message is the most commonly used as the first step for all the attacks, as it reveals the precious **IMSI** of the subscriber. Remember, the IMSI serves as a key to the HLR database records.

Another way to extract this kind of information is the request message: **AnyTimeInterrogation**. This request is addressed to the HLR and also requires only the subscriber's MSISDN (phone number). The response includes Base Station cell tower identification, as well as the IMSI and IMEI numbers, which describe uniquely the subscriber. It also includes the GT addresses of the MSC/VLR currently serving the victim, as well as the SGSN that serves data to him.

In particular, in order to obtain a subscriber's whereabouts from the cellular network, a set of specially crafted messages can be used:

ProvideSubscriberInfo is a MAP message that is used by various services to derive location data. The HLR send this request, along with the IMSI of a particular subscriber as parameter, to the MSC/VLR that is currently responsible for the subscriber. Upon reception, the MSC queries the Base Station with a paging request, in order to retrieve the subscriber's state. No external connections to home network subscribers should be allowed.

Figure 13: MAP procedure during a ProvideSubscriberInfo request.



As an attack, this message requires the knowledge of the IMSI of the victim, and it is used only for location tracking purposes.

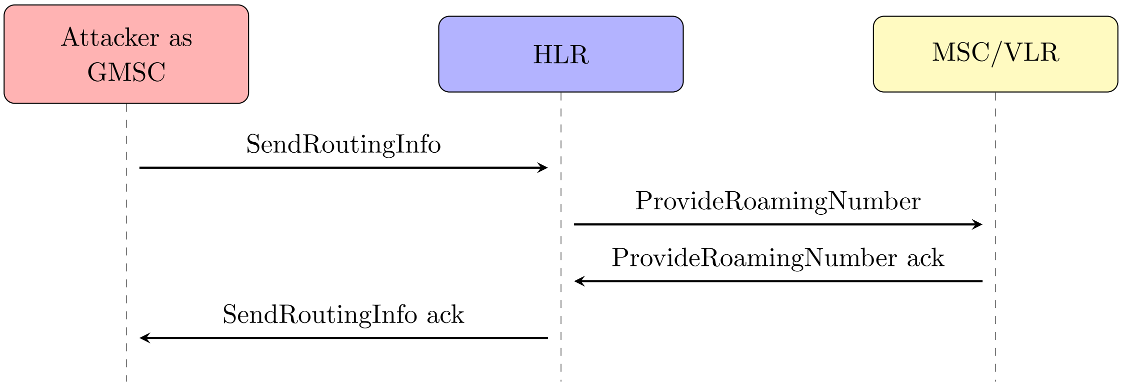
SendRoutingInfo is a MAP message used in call delivery, that inquires routing information about the recipient. As an attack, it is mainly used to gain confidential information about a subscriber's state, such as his **IMSI**,the GT address of the MSC/VLR that he is registered in and other. In the case of a mobile terminating call, the GMSC sends this message to the called party's HLR to obtain routing information, such as the MSRN. Upon receiving the message, the HLR sends a **ProvideRoamingNumber** request to the VLR that is currently serving the subscriber, to obtain his MSRN. Normally, this message should pass only between network elements of the home network.

SendRoutingInfoForSM is similar to message above, but is used for delivery of incoming SMS and inquires routing information to determine the subscriber's location. The message contains the subscriber's MSISDN, and the response contains the destination MSC's ISDN number. This message should be routed to the *"SMS Home Routing"* equipment, if that is deployed in the operator's network. Note that SMS Home Routing is a mechanism designed for performance reasons, rather than security.

SendRoutingInfoForGPRS is also a similar message, inquiring routing information about a subscriber. Although in this case, the respond is companioned with a *PDP Context* identifier, which effectively is an alias for the IP address of the subscriber.

SendRoutingInfoForLCS is a MAP message that is not normally used as a product by the operators. Instead, it is deployed for legal reasons, and should be available only to the national authorities for social security reasons, following a warrant. Normally, this message should be employed only among home network elements.

Figure 14: MAP procedure during a SendRoutingInfo request.



AnyTimeInterrogation is also a MAP message used to determine a subscriber's location. It also reveals the subscribers IMSI, IMEI, the MSC/VLR and the SGSN serving him. The only required parameter is MSISDN of the victim. This message is deprecated however, although still in use, and should be applied exclusively within the home network. Already, many operators are known not to respond to such requests.

SendIMSI is a MAP message that is employed to determine a subscriber's IMSI by his phone number. It is used infrequently, however the equipment often processes it according to 3GPP specification and one in four attempts are successful. [7]

Usually there is no questioning on the legitimacy of such requests.

Call Interception

Call handling can be generally divided into two different procedures:

- The calls that *originate* from the subscriber (calls he dials) and
- the calls that *terminate* to him (incoming calls on his phone).

Originating calls are tapped by using a similar pattern: the message **InsertSubscriberData** replaces the address of the billing platform in the subscriber's profile stored in the VLR database, with her own equipment address. The subscriber profile contains all key information related to the user's subscription, like location, billing information etc. When the subscriber makes a call, the billing request along with the number of the destination subscriber are sent to the attacker's equipment. The attacker can then redirect the call to the called subscriber, thus creating a *tree-way* conference call, that includes the destination subscriber, the calling subscriber and the attacker. So she can tap any conversation of the subscriber. [6]

Redirecting *incoming* calls is usually achieved with an **UpdateLocation** request. When a call is terminated, the gateway MSC (GMSC) sends a request to the HLR to identify the MSC/VLR that currently serves the subscriber. This information is necessary to route the call to the appropriate switch. After successfully performing location update, the HLR will redirect the received request to the fake MSC/VLR, which in turn will send a Mobile Station Roaming Number (MSRN) to redirect the call. The HLR transfers this number to the GMSC, which redirects the call to the provided MSRN. [6]

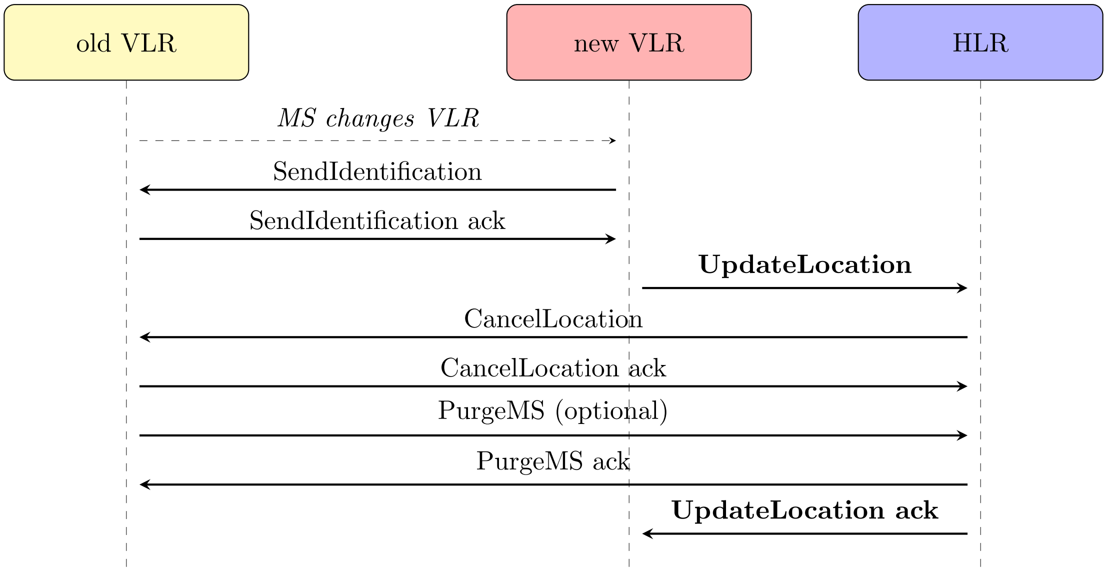
Roaming number spoofing is conducted during a terminating call to a target subscriber. Beforehand, the victim must be registered in the attacker's false network. As a response to a roaming number inquiry, the attacker can send a number for call redirection. All the connections will be at the operator's expense. Redirection manipulation includes unauthorized setting of unconditional forwarding. All originating calls will be redirected to a given number and the subscriber will be the one to pay for all connections. [7]

Redirection means transferring a call to a third-party number. Further development of this attack establishes a connection so that an attacker could tap a subscriber's conversation. The message **UpdateLocation** is used to inform the HLR about a change on a mobile switch. Terminating SMSs or calls are intercepted by sending a fake request to register a subscriber in the attacker's network. When a terminating call is received, the operator's network sends a request to the fake network to obtain the subscriber's roaming number. Naturally, the attacker can send the number of her own telephone exchange (**PBX/Asterisk**) in response and the incoming traffic will be transmitted through the attacker's equipment. After sending another request to register the subscriber in the real network, the attacker can redirect the call to the subscriber's number. As a result, the conversation will pass through the equipment controlled by the attacker. The same principle is used for interception of terminating calls via **RegisterSS**, but in this case terminating calls are unconditionally redirected to the intruder's telephone exchange. [8]

Calls are redirected by using:

UpdateLocation This message is used to inform the HLR when an MS (in the idle state) has moved into a new location area. This message is initiated from the new VLR that the subscriber roams, and contains the IMSI of the victim and the MSC/VLR GT address. In this way, the HLR maintains the location of the MS (VLR area only). Based on this, an attacker could allege a subscriber's registration in a false network, which means that all incoming texts and calls would be transferred to the indicated address. The figure below demonstrates a regular UpdateLocation procedure.

Figure 15: MAP operation sequence involved in a regular location update.



As you can see, transactions are pretty simple and the network components avoid asking too many questions, in favour of performance. There is a number of other messages involved, apart from UpdateLocation, that are used in a regular location update. Note that the PurgeMS message is optional.

Usually, after a succesful UpdateLocation, the HLR send an additional InsertSubscriberData to the new VLR, in order to update the subscriber's profile there.

Because the attacker is able to impersonate any of the Signalling Points involved, she could easily forge the SendIdentification message as well. The attacker could also just send an UpdateLocation right away, and skip the rest, as there is no actual validation done by any of the nodes.

Although the phone would indicate connectivity to the network, the subscriber will not be able to receive calls or text messages. Subscriber services will remain blocked until he travels to another MSC/VLR area, reboots the phone or makes an outgoing call.

RegisterSS is used to register a Supplementary Service for a particular subscriber. The Supplementary Service (such as call forwarding) is often automatically activated at the same time. An attacker can impersonate the subscriber to enable call forwarding to her own network device, effectively becoming a *(wo)man-in-the-middle*.

InsertSubscriberData is a MAP message that is used when to change a subscriber's profile in the VLR database. The VLR uses this message to provide routing information (MSRN) to the HLR in the case of a mobile terminating call, which is sent to the GMSC. Nevertheless, attackers can use this message to modify the platform value in the subscriber's profile, so that call billing would go through their equipment. A mobile switch would first send a request to proceed with an originating call to the indicated address. An adversary needs to send a command to forward a call to a controlled PBX, and then transfer traffic to a destination user. Thus, a conversation between subscribers will be openly held via PBX under the complete control of the attacker.

In fact, the list of data that the HLR can insert into a MSC/VLR is quite long. Interesting fields could be:

- Forwarding Information List
- VLR CAMEL Subscription Info
- Voice Group Call Data
- Voice Broadcast Data
- Regional Subscription Data

For a complete list of InsertSubscriberData parameters, refer to Appendix B.

AnyTimeModification Same as the above, this message is able to update all values of a subscriber's profile. It is normally used by a gsmSCF, but is deprecated.

SendIdentification When the MS changes to a new VLR area, the new VLR queries the old VLR using a SendIdentification operation to obtain authentication information. This operation requires the TMSI as its argument, and the response contains the IMSI and other authentication information (RAND, SRES, and optionally KC). If it is unable to obtain this information, it can retrieve this information from the HLR via a **SendAuthenticationInfo** operation. As a result, when we refer to *Authentication* in mobile networks, we merely mean subscriber's authentication to the network. There is no notion of authentication between nodes of the Core Network.

This message cannot be used for redirection of calls or texts. It is used to obtain the secret keys for the cryptography taking place in the radio channel, between the BTS and the MS. In combination with an UpdateLocation procedure, an attacker can intercept the call of a victim through the air interface, as long as she is in close proximity with the target.

These messages allow manipulation of a subscriber's profile. A subscriber's profile contains all key information related his registration, such as location, billing information etc. During a research that took place recently, attempts to tap or redirect terminating and originating calls were successful in more than half of all cases. [8]

The percentage of successful attacks is high due to the lack of a subscriber actual location check. To reduce the possibility of attacks using these methods, continuous monitoring of signalling traffic and illegitimate activity is required to identify suspicious hosts, build lists of trusted networks, and immediately block requests from banned sources. [8]

SMS Interception

SMS provides paging functionality for alphanumeric messages of up to 160 characters to be exchanged with other GSM users. The network itself can also generate messages and broadcast to multiple MSs or to a specific MS. For example, a welcome message can be sent to a subscriber when he or she roams onto a new network; in addition, it can provide useful information, such as how to retrieve voicemail. The SMS service also transfers ring tones and logos to the MS. The SMS slightly blurs the image of the user traffic being separate from signaling because, in a sense, the messages are user traffic; they are for human processing (written and read), rather than for communication between network entities. [1]

The risk of subscriber traffic interception is still high. The vast majority of attempts to intercept subscriber SMS is successful. Today, extremely important data are transmitted via SMS messages: passwords for two-factor authentication sent by e-banking and internet payment systems. Leakage of such information affects the operator's reputation, and might result in contract termination by customers, including companies with a large volume of traffic. [8]

This attack is very similar to the one described above. After registering the subscriber in the fake MSC/VLR, using an **UpdateLocation** forged request, SMS messages intended for the subscriber will instead be sent to the attacker's host. The attacker will then be able to: send a confirmation that the message was received, so that it will look to the sender as if the message was delivered. Moreover, she could even re-register the subscriber to the previous MSC/VLR, so that he also gets the message. This attack can be used to steal one-time mobile banking passwords delivered as SMS messages, or recover passwords used for various internet services (email, social networks, etc.) [7]

Much like calls, SMS comprises of two basic services:

- *Mobile-Originated Short Message* (MO-SM)
- *Mobile-Terminated Short Message* (MT-SM)

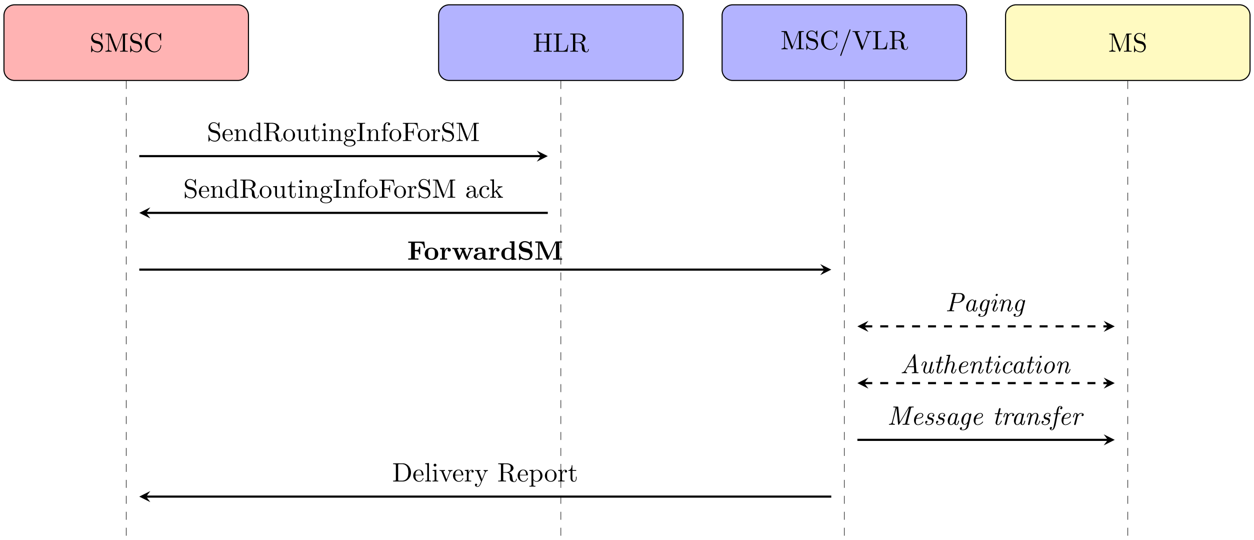
Mobile-Originated (MO) short messages are transported to the SMSC and can be destined to other mobile subscribers. *Mobile-Terminated* (MT) short messages are transported from the SMSC to the handset and can be submitted to the SMSC by other mobile subscribers via MO-SM or by other sources such as voice-mail systems, or operators.

For MT-SM, a report is always returned to the SMSC either confirming the short message delivery to the handset or informing the SMSC of the short message delivery failure and identifying the reason (cause code). Similarly, for MO-SM, a report is always returned to the handset either confirming the short message delivery to the SMSC or informing of delivery failure and identifying the reason.[4]

[4] https://raufakram.wordpress.com/2013/12/17/sms-tutorial/

ForwardSM Both the *Mobile Originating* (MO-SMS) and *Mobile Terminating SMS* (MT-SMS) procedures use this operation to carry text messages between the MSC where the subscriber roams and the SMSC or the GMSC, respectively. An attacker can use this message to unconditionally send SMS messages. When *SMS Home Routing* is in place, MT-SMS is always delivered to the home SMSC first.

Figure 16: Short Message Service transfer procedure.



Phishing or ad messages can be sent on behalf of arbitrary subscribers or services using MT-ForwardSM and MO-ForwardSM methods. MT-ForwardSM is designed for delivering incoming messages and can be used by attackers to generate forged incoming SMS messages. Unauthorized usage of MO-ForwardSM allows sending messages from subscribers and at their expense. [8]

SMS Home Routing cannot be used as a protection mechanism against other attacks. Moreover, it is not intended to protect a network, but rather it is devised for correct routing of incoming SMS messages. Research results show that networks with SMS Home Routing enabled are no more secure than others, perhaps because operators often rely solely on SMS Home Routing, neglecting additional security measures. [8]

Denial of Service

CancelLocation is used to delete a subscriber's profile from the previous VLR, following registration with a new VLR. In other words, following an **UpdateLocation** event. When the HLR receives an UpdateLocation request from a VLR other than the one that is currently stored in its records, it sends a CancelLocation to the old VLR. That message includes the IMSI to identify the subscriber whose profile should be deleted as parameter. An attacker could use this operation to cause a temporal Denial of Service to the subscriber.

PurgeMS is the opposite message of the one above; it serves exactly the same purpose, while the participant roles are reversed. This message is send by a MSC/VLR to the HLR, in order to inform it that a MS has recently get out of its jurisdiction area. It is an optional part of the UpdateLocation procedure. It should only been sent between elements of the same network.

Fraud

GSM defines the concept of *Supplementary Services.* In addition to supplementary services, GSM has also defined the concept of *Unstructured Supplementary Services.* USSs allow PLMN operators to define operator-specific supplementary services and to deliver them to market quickly. USS allows the subscriber and an operator-defined application to communicate in a way that is transparent to the MS and intermediate network entities. The communication is carried out using Unstructured Supplementary Service Data (USSD) packets, which have a length of 80 octets (91 ASCII characters coded, using seven bits) and are carried within the MAP operation. USSD uses the dialogue facility (which is connection-oriented) of TCAP. Unlike SMS, which is based on a store and forward mechanism, USSD is session-oriented and, therefore, has a faster turnaround and response time than SMS, which is particularly beneficial for interactive applications. [1]
There is a wide range of methods that can be used by criminals to gain financial benefit from the operator or subscribers. These methods can be divided into four categories: [8]

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

An attacker can redirect voice calls of subscribers to premium-rate numbers or to a third-party number. The call will be paid by the subscriber in case of establishing unconditional redirection, or by the operator in case the subscriber is registered in a fake network and his or her roaming number is spoofed. Call redirection also helps to implement other fraudulent schemes. For example, if a subscriber makes a call to a bank, an intruder can redirect it to his or her own number impersonating a bank employee, and thus obtain confidential information, such as passport data and a codeword. Another method is redirecting terminating calls and impersonating a subscriber to confirm banking transactions. [8]

An attacker can transfer money from the account of a subscriber or an operator's partners by sending fake USSD requests using the ProcessUnstructuredSSRequest method. UnstructedSSNotify is used to send notifications to subscribers from various services and the operator. An attacker can send a fake notification on behalf of a trusted service containing instructions for the subscriber: send an SMS message to a paid number to subscribe to a service, call a fake bank number because of suspicious transactions, or follow a link to update an application. [8]

Technical details

SigPloit

Signaling exPloiter is a signalling security testing framework, dedicated to telecom security professionals and researchers, to conduct penetration tests on mobile operator networks. It spans from 3G MAP requests, to 4G Diameter messages and other GTP messages for 5G. It was created in 2017 by *Loay Abdelrazek, Rosalia D'Alessandro, Ilario Dal Grande* and *Hardik Mehta*. It is freely distributed under MIT licence and you can get the latest version online, at GitHub.[5]

Current version of SigPloit support only 11 eleven discrete MAP messages, for SS7. They are organized in 4 categories, namely *Location Tracking*, *Interception*, *Fraud* and *Denial of Service*.

Location Tracking Attacks

Particularly, the information gathering messages of the first category are:

- AnyTimeInterrogation
- ProvideSubscriberInfo
- SendRoutingInfo
- SendRoutingInfoForSM
- SendRoutingInfoForGPRS

Interception Attacks

In the interception category there is only one message, the **UpdateLocation** of course. Nevertheless, the drawback in this case is that the message is not actually implemented alone, as it would have no meaning. It is accompanied by an SMS interception scenario, in order to demonstrate the power of this message.

Fraud Attacks

For the fraudulent actions category, we are provided with another 5 messages:

- CancelLocation
- InsertSubscriberData
- SendAuthenticationInfo
- SendIMSI
  to retrieve the IMSI, which is considered confidential and private information.
- MTForwardSMS
  which is used to deliver an SMS message to a particular subscriber. This kind of attack is considered a *phishing* attack, as it can be used to send spoofed or anonymous SMS messages.

[5] https://github.com/SigPloiter/SigPloit

Denial of Service Attacks

The last category also includes only one message, **PurgeMS**, which is generally used to *de-authenticate* a Mobile Station from the network that is currently connected to. This type of attack is assumed a small scale Denial of Service, as it concerns only one subscriber, who only temporarily will be unable to initiate or receive any calls and services. The MS will re-authenticate during the next paging request, which may take several minutes, depending on the operator, or until the user reboots the device, manually registering again to the network, or initiate an outgoing call.

Installation

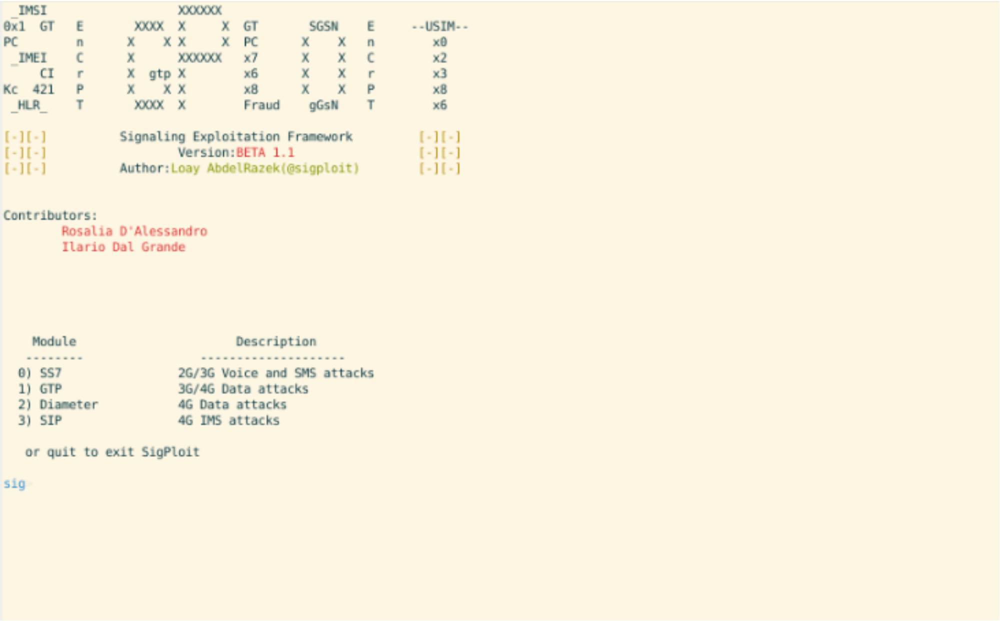
SigPloit is rumoured to be already present in some security distributions. However, it is very easy to install on a any Debian distribution. First off, the project is available on GitHub, so the Git application is required. The project is written in Python and Java, so these two are also required. The build system for the Java code is done with Apache Maven. Last, in order to support the performance requirements of SCTP, Linux kernel needs an additional module installed.

```
# apt-get update
# apt-get install git python openjdk-8-jdk maven lksctp1 lksctp-dev lksctp-tools
```

Now, you can use Git to download the application from GitHub. Also, Python has some requirements, which can be met using PIP. The list of the requirements is inside a file called ‘`requirements.txt`’. The program’s executable is called ‘`sigploit.py`’.

```
$ git clone https://github.com/SigPloiter/SigPloit
$ cd SigPloit
$ pip2 install -r requirements.txt
$ python sigploit.py
```

Figure 17: SigPloit start-up screen.



```
 _IMSI                  XXXXXX
0x1  GT   E       XXXX  X     X  GT       SGSN    E     --USIM--
PC        n      X    X X     X  PC      X    X   n        x0
 _IMEI    C      X      XXXXXX   x7      X    X   C        x2
     CI   r      X  gtp X        x6      X    X   r        x3
Kc  421   P      X    X X        x8      X    X   P        x8
 _HLR_    T       XXXX  X        Fraud    gGsN    T        x6

[-][-]          Signaling Exploitation Framework         [-][-]
[-][-]                  Version:BETA 1.1                 [-][-]
[-][-]          Author:Loay AbdelRazek(@sigploit)        [-][-]


Contributors:
        Rosalia D'Alessandro
        Ilario Dal Grande




    Module                      Description
   --------                ---------------------
  0) SS7                2G/3G Voice and SMS attacks
  1) GTP                3G/4G Data attacks
  2) Diameter           4G Data attacks
  3) SIP                4G IMS attacks

   or quit to exit SigPloit

sig>
```

Configuration

In case of no SS7 access, SigPloit offers the possibility of a simulation mode, where you can have a sense of the attacks and the severity of such a threat. The project provides the server side part of each message, that simulates the corresponding nodes responsible for the requests. The server side '`.jar`' files can be found under '`SigPloit/Testing/Server/`' folder. Each server side code provides the hard coded values that you need to use in the client, in order to simulate the attack, inside the text file named '`Parameters`' in their folder.

For example, in order to simulate the **AnyTimeInterrogation** message, you will need to start the server separately and set particular parameters in the client options. These parameters are different for every message and are present inside a file in the server folder.

```
$ cd SigPloit/Testing/Server/Attacks/Location_Tracking/AnyTimeInterrogation_Server/
$ cat README_Instructions
```

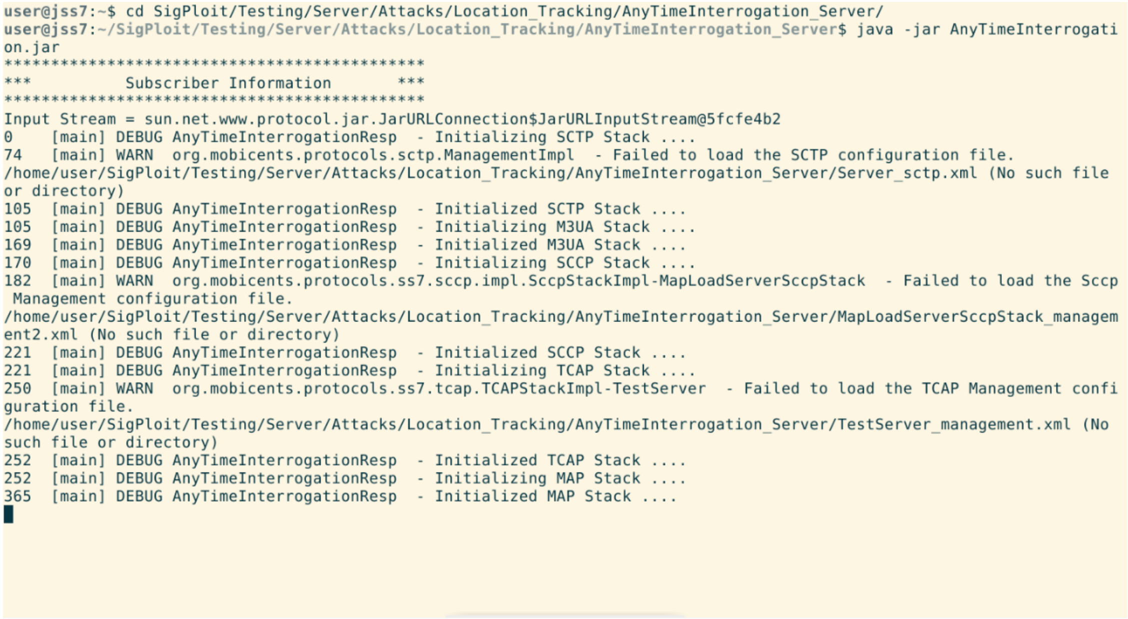
You will need to setup an IP address according to the parameters listed in the file, in order for the server to bind and start accepting connections. This can be achieved with the following command:

```
# ip address add 192.168.56.101/32 dev lo
# ip address add 192.168.56.102/32 dev lo
```

Run the server:

```
$ java -jar AnyTimeInterrogation.jar
```

Figure 18: JSS7 AnyTimeInterrogation server output.

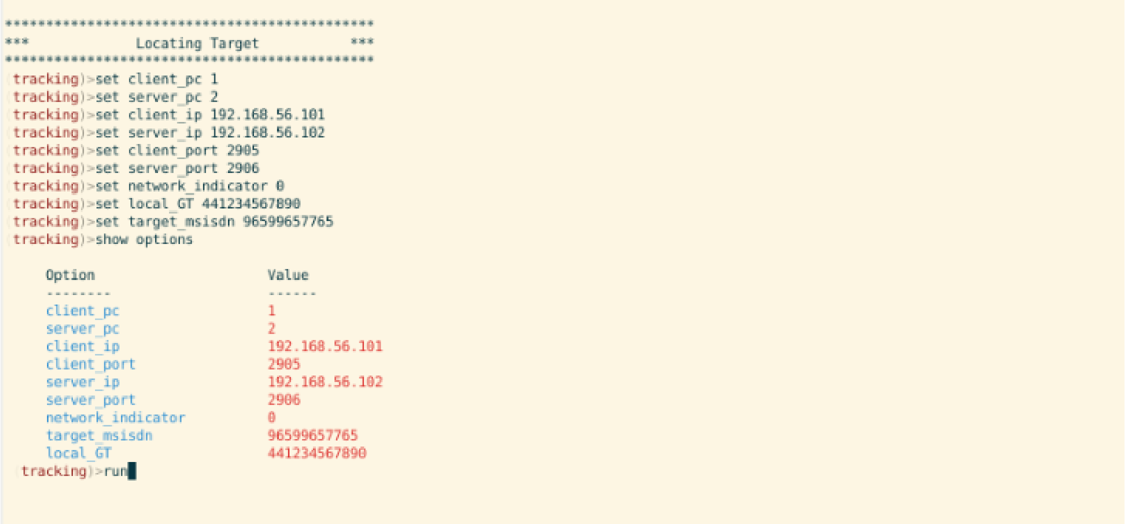


```
user@jss7:~$ cd SigPloit/Testing/Server/Attacks/Location_Tracking/AnyTimeInterrogation_Server/
user@jss7:~/SigPloit/Testing/Server/Attacks/Location_Tracking/AnyTimeInterrogation_Server$ java -jar AnyTimeInterrogati
on.jar
*********************************************
***          Subscriber Information       ***
*********************************************
Input Stream = sun.net.www.protocol.jar.JarURLConnection$JarURLInputStream@5fcfe4b2
0    [main] DEBUG AnyTimeInterrogationResp  - Initializing SCTP Stack ....
74   [main] WARN  org.mobicents.protocols.sctp.ManagementImpl  - Failed to load the SCTP configuration file.
/home/user/SigPloit/Testing/Server/Attacks/Location_Tracking/AnyTimeInterrogation_Server/Server_sctp.xml (No such file
or directory)
105  [main] DEBUG AnyTimeInterrogationResp  - Initialized SCTP Stack ....
105  [main] DEBUG AnyTimeInterrogationResp  - Initializing M3UA Stack ....
169  [main] DEBUG AnyTimeInterrogationResp  - Initialized M3UA Stack ....
170  [main] DEBUG AnyTimeInterrogationResp  - Initializing SCCP Stack ....
182  [main] WARN  org.mobicents.protocols.ss7.sccp.impl.SccpStackImpl-MapLoadServerSccpStack  - Failed to load the Sccp
 Management configuration file.
/home/user/SigPloit/Testing/Server/Attacks/Location_Tracking/AnyTimeInterrogation_Server/MapLoadServerSccpStack_managem
ent2.xml (No such file or directory)
221  [main] DEBUG AnyTimeInterrogationResp  - Initialized SCCP Stack ....
221  [main] DEBUG AnyTimeInterrogationResp  - Initializing TCAP Stack ....
250  [main] WARN  org.mobicents.protocols.ss7.tcap.TCAPStackImpl-TestServer  - Failed to load the TCAP Management confi
guration file.
/home/user/SigPloit/Testing/Server/Attacks/Location_Tracking/AnyTimeInterrogation_Server/TestServer_management.xml (No
such file or directory)
252  [main] DEBUG AnyTimeInterrogationResp  - Initialized TCAP Stack ....
252  [main] DEBUG AnyTimeInterrogationResp  - Initializing MAP Stack ....
365  [main] DEBUG AnyTimeInterrogationResp  - Initialized MAP Stack ....
```

If everything goes according to the plan, then you are good to go start the client, either through SigPloit's user interface, or directly by calling the Java client.

```
$ cd SigPloit/ss7/attacks/tracking/ati/
$ java -jar AnyTimeInterrogation.jar
```

Figure 19: SigPloit AnyTimeInterrogation client.



```
*********************************************
***             Locating Target           ***
*********************************************
(tracking)>set client_pc 1
(tracking)>set server_pc 2
(tracking)>set client_ip 192.168.56.101
(tracking)>set server_ip 192.168.56.102
(tracking)>set client_port 2905
(tracking)>set server_port 2906
(tracking)>set network_indicator 0
(tracking)>set local_GT 441234567890
(tracking)>set target_msisdn 96599657765
(tracking)>show options

     Option                      Value
     --------                    ------
     client_pc                   1
     server_pc                   2
     client_ip                   192.168.56.101
     client_port                 2905
     server_ip                   192.168.56.102
     server_port                 2906
     network_indicator           0
     target_msisdn               96599657765
     local_GT                    441234567890
 (tracking)>run
```

Other Simulation Software

A list for SS7 emulation tool alternatives can grow quite long, but below we present two of the most common in more detail.

Name	URL	Language	Licence
jSS7	https://github.com/RestComm/jss7	Java	open-source
openAirInterface	https://github.com/OPENAIRINTERFACE/openair-cn	C	open-source
openSS7	https://www.openss7.org	C, Perl	open-source
osmo_ss7	https://cgit.osmocom.org/erlang/osmo_ss7/	Erlang, C	open-source
LTEENB	https://www.amarisoft.com/software-enb-epc-ue-simulator/	? C	commercial
openLTE	http://openlte.sourceforge.net/	C++	open-source
srsLTE	https://github.com/srsLTE/srsLTE	C++, C	open-source
openEPC	https://www.corenetdynamics.com/products	?	shared source code

JSS7

jSS7 is a framework that emulates the entire SS7 stack. It is written in Java and it is open source, available on GitHub.[6] It is used as a full stack solution to make it easy to deploy custom services. You can use JSS7 as a Signaling Gateway that acts as an agent that translates Switched Circuit Network at the edge of an IP network. Also, it can be used as a simulation environment on a single terminal.

JSS7 utilizes the M3UA user adaption layer to provide IP access to the SS7 network emulated inside the application. That means in order to connect from an IP based device, one may need to set configuration parameters for:

- IP layer
- SCTP layer
- SCCP level
- MAP level

However, JSS7 has a complete implementation of the SigTran standard. The specification is translated into data types using the ASN.1 notation. There is also a *Command Line Interface* (CLI) that can be used to configure the network, although, most usually the *Graphical User Interface* (GUI) is used. It comes with preconfigured parameters that correspond to specific transaction scenarios.

In order to emulate SS7, SigPloit uses prebuilt executables of the JSS7 platform, in '`.jar`' format. If you want to run JSS7 separately, you can also use the already built binary format available on GitHub.

Usually, building from source is not required to run a simple test. There are already pre-build, binary releases that can serve your purpose. Nevertheless, building from source would also produce a PDF rendered version of the manual, so it deserves a chance.

For the build procedure, some dependencies are required:

- Java, of course, but only version 8 is acceptable. That means you gonna need a working JDK version 8. In a Debian distribution you can install it with:

  ```
  # apt-get update && apt-get install openjdk-8-jdk
  ```

[6] https://github.com/telestax/jss7

To test if java is installed correctly, use:

```
$ java -version
```

Presently, Java has reached version 11. I think it changed 3 different versions in a couple of years. Nevertheless, the JSS7 documentation states that Java version 7 should be used for the build process. Unfortunately, openjdk-7 is no longer available in the stable repository of Debian. That is why we use openjdk-8-jdk, which does the job adequately. On the other hand, if you try to build JSS7 with newer Java versions, like '`openjdk-11`', you are going to hit on a wall.

- Git version control system, install it with:

```
# apt-get install git
```

- Apache Ant and Maven:

```
# apt-get install ant mvn
```

- JMX-Tools, which can be downloaded directly from:

```
http://www.datanucleus.org:15080/downloads/maven2/com/sun/jdmk/
     jmxtools/1.2.1/jmxtools-1.2.1.jar
```

After the download, you have to add the file to your local Maven repository. This is achieved with the following command:

```
$ mvn install:install-file -Dfile=/path/to/jmxtools-1.2.1.jar \
     -DgroupId=com.sun.jdmk -DartifactId=jmxtools \
     -Dversion=1.2.1 -Dpackaging=jar
```

In Linux, Maven local repository lives in the '`/home`' folder, inside a directory called '`~/.m2/repository/`'. You should be able to validate the installation success by looking for a folder named '`jdmk/`' inside '`~/.m2/repository/com/sun/`'.

JMX-Tools is the first, open, Java implementation of all these telecommunication, ASN.1 defined, protocols that we are are going to use. MAP, TCAP, SCCP, ISUP, etc. It is developed and provide freely by Oracle.

- For the SCTP support, you will need:

```
# apt-get install lksctp-tools
```

To ensure that SCTP is correctly configured, try compiling and running the following application:

```
$ nano TestSCTP.java

// a simple SCTP application
public class TestSCTP
{
     public static void main(String[] args) throws Exception {
          com.sun.nio.sctp.SctpChannel sc = com.sun.nio.sctp.SctpChannel.open();
          System.out.println("SCTP library correctly configured!");
     }
}
```

```
$ javac TestSCTP.java
$ java TestSCTP
```

The build process step by step:

1. First, download the source code:
   ```
   $ git clone https://github.com/RestComm/jss7.git
   ```
2. Then, initiate the build process:
   ```
   $ cd jss7; mvn install
   ```
3. Which will probably crash, complaining about 'log4j' setup. The most common solution is to do:
   ```
   $ cd jss7; mvn clean install -Dmaven.test.skip=true
   ```
4. Last, build the binaries:
   ```
   $ cd jss7/release; ant
   ```

By using the Restcomm SS7 Service you will be able to configure the SS7 stack using CLI (Command Line Interface) commands. The SS7 Service wraps SS7 Level 4 (i.e., MAP, CAP and ISUP) and the lower layers and expose them via JNDI, such that the layer above can perform the look-up and use it in any application. The Restcomm SS7 Service binary requires that you have JBoss Application Server installed and 'JBOSS_HOME' environment variable set properly. JBoss Application Server tides together the several parts of SS7 standard. These are seen as Resource Adaptors of different services, coordinated and managed by JBoss.

1. Download the Wildfly library (the *new* JBOSS) from: http://wildfly.org/downloads/
   ```
   $ wget http://download.jboss.org/wildfly/14.0.1.Final/wildfly-14.0.1.Final.zip
   ```
2. Just, unzip somewhere and set the 'JBOSS_HOME' variable:
   ```
   $ cd wildfly-*; export JBOSS_HOME=$(pwd)
   $ echo "export JBOSS_HOME=$(pwd)" >> ~/.bashrc
   ```

JSS7 Attack Simulator

JSS7 Attack Simulator is another project that simulates an SS7 network and demonstrates some of the attacks described above. It is part of a similar thesis, carried out by Kristoffer Jensen, a college from the Norwegian University of Science and Technology. It is licensed under the Free Open Source GNU Affero GPL v3.0. [2]

It supports two modes:

- Simple mode: Used to demonstrate some SS7 attacks.
  - An AnyTimeInterrogation MAP message exchange,
  - and a ProvideSubscriberInfo MAP message exchange.
- Complex mode includes a full network simulation containing 3 operators, where one of the subscribers is the victim, and the adversary has access to the SS7 network. In this mode several nodes communicate using 13 standard procedures following the 3GPP MAP standard. After a mercy period, a number of attacks is launched against the subscriber with the goal of obtaining the subscriber's location and then intercept his SMS messages.

Traffic is generated using the SCTP protocol and all data is sent on the `lo` interface.

The simulator is based on JSS7, thus it requires a working Java runtime environment, preferably `openjdk-8-jre`. Also, make sure you have SCTP support installed on your system. As for JSS7, the same instructions also apply here. The easiest way to run the program is to download the latest built binaries, from Github.com.[7]

Just `unzip` the file and then navigate to the directory where the executable script is located.

```
$ tar -xvzf jss7-attack-simulator.tar.gz
$ cd restcomm-jss7-${jSS7.release.version}/ss7/restcomm-ss7-simulator/bin/
$ ./run.sh help
```

Osmocomm

OSMoComm stands for *Open–Source Mobile Communications*. This platform aims to provide a complete open–source implementation of all of an operator's network components. The project started 10 years ago and is already in the second implementation. Mainly it is written in C++ programming language.

The first implementation was partly based also on the Erlang programming language. Erlang is an offspring of the swedish telecom vendor, Ericsson, and the name is also an acronym for *'Ericsson Language'* (apart from the *"father"* of telecommunications). This implementation was named `OpenBSC`, and integrated all the components of an operator's network into a single application. One of a few, the primary purpose of the project was to create a primitive open-source application for those, new then, *Universal Software Radio Peripheral* (USRP) cards. Thus, it included not only the core, but also the radio part of the network. Nevertheless, the Core Network part, which was written in Erlang, was utilized by one of the first penetration testing platforms for GSM networks, the `SS7Maper`.[8] Sadly, the whole project has been deprecated since 6 years ago and is not easy to get it working, although is still available online, at the project's Git page.[9]

The second implementation was completely re-written from scratch and the network components were separated into different applications, namely `OsmoMSC`, `OscmoHLR`, `OsmoBSC`, etc. This design made the project more redundant, easier to deploy and easier to debug. All the applications are written solely in C++ and the community has also created a lot of collateral tools that aid in the programming and the debugging process. Moreover, the project's modularity allows the integration of applications from other sources, such as the popular `OpenBTS`[10] radio part application for example.

Installation can be as easy as just typing:

```
# apt-get update; apt-get install osmo-hlr osmo-msc osmocom-sgsn telnet
```

Then, you could run the HLR part like this:

```
$ osmo-hlr -c /etc/osmocom/osmo-hlr.cfg

$ telnet localhost 4258
OsmoHLR> enable
OsmoHLR# subscriber imsi 123456789023000 create
OsmoHLR# subscriber imsi 123456789023000 update msisdn 123
```

[7] https://drive.google.com/file/d/0B5wpGwi_jRR5a1pUZ2laWnA0WmM/view?usp=sharing

[8] https://github.com/ernw/ss7MAPer

[9] https://cgit.osmocom.org/erlang/

[10] https://openbts.org/

```
OsmoHLR# subscriber msisdn 123 show
```

Subscribers are kept in a local SQLite database file and can be managed via VTY and CTRL interfaces. If no database exists, OsmoHLR will automatically create and bootstrap a database file with empty tables. Using telnet to administrate the HLR is achieved through the VTY interface. Every Osmocom application can be configured through two different interfaces:

- VTY telnet administration interface and
- CTRL python API interface, used by third party custom applications.

Every network component is assigned a different port range at localhost. They can also be configured to operate on IP addresses, as well as on different machine and location.
However, MSC and HLR communicate with each other over the IP network, by using what is called the *"Generic Subscriber Update Protocol"* (GSUP). GSUP is used to transfer information between HLR and MSC and SGSN. That way, it is effectively a replacement for the MAP stack GSM application framework. Subscriber state, profile and location update are taking place through this interface (GSUP), rather than the official D interface (HLR-VLR), that utilizes the MAP requests described above. The syntax, as well as protocol design, are different and thus different security worries may arise about.
Currently, GSUP supports the following procedures: [11]

- Send Authentication Info
- Update Location
- Location Cancellation
- Purge MS
- Insert Subscriber Data
- Delete Subscriber Data
- Process Supplementary Service
- MO-forwardSM
- MT-forwardSM
- READY-FOR-SM
- CHECK-IMEI

They have also developed a number of applications regarding the SIM cards. A couple of interesting choices would be `PySim`, `SimTrace` and `SoftSim`. For a complete list of tools and applications, you can refer to the project's Git page.[11]

Other tools

In order to attack any network, reconnaissance solutions, such as network discovery and port scanners, are required. P1 Security, has already released open-source solutions, with the following useful tools.

SCTPscan SCTP network and port scanner.[12]

pySCTP SCTP support for Python (C bindings, Python library, tests).[13]

ss7calc Calculate and convert SS7 Signaling Point Code (SPC).[14]

[11] https://cgit.osmocom.org/
[12] https://www.p1sec.com/corp/research/tools/sctpscan/
[13] https://www.p1sec.com/corp/research/tools/pysctp/
[14] https://www.p1sec.com/corp/research/tools/ss7calc/

P1 Security has also released open-source the SigFW, a firewall solution for SS7 and Diameter networks.

Protection Measures

Operators really need to filter messages at the edge of their network. With all this popularity about the matter that took up recently, operators soon will be legally obligated to do so too. Nevertheless, a lot of the vulnerabilities could be mitigated just with the correct configuration. A common problem that many operators face is the inability to distinct whether some irregular traffic comes from an incident or bad configuration.

On the other hand, even though there exist a number of available security solutions, their products are often very expensive for a small operator. With the introduction of IP based services inside the Core Network, small-scale providers would spread all over the internet. An open-source solution is needed to tackle this development, which could also serve as an average consensus implementation.

SigFW

Signalling FireWall promises to be such a solution. It is developed by P1 Security and allows to deploy a firewall in limited scope to protect just select network elements, parts of the networks or individual links. It is also written in Java and based on the JSS7 and JDiameter simulators of Telestax. It is publicly available, along with the other open-source tools of P1 Security, at GitHub.[15]

SigFW has many functionalities:

- Open SS7 TCAP encryption and signing of the SS7 messages, including auto encryption setup
- SS7 SCCP blacklists
- SS7 TCAP blacklists
- SS7 MAP firewall rules
- Signalling IDS integration
- SS7 Filtering and honeypot
- Centralized threat reporting with mThreat integration
- Collaboration with other SS7 and signalling security systems
- Management through open APIs
- Passive run (re-run traffic from PCap or passive interface to test the firewall)
- LUA programmable firewall rules
- Scalable/Decentralized solution

Correct signalling traffic filtering reduces the risks of passing unauthorized requests. Obviously, a filtering system alone cannot protect the network thoroughly. It most potent against threats that involve messages between the nodes of the home network. It is not as useful against treats that involve messages between different operators.

To counteract criminals, an integrated approach to security is required. Regular security assessment of signalling networks is required to identify existing vulnerabilities and develop measures to mitigate threat realization risks, and then to keep security settings up-to-date. Alongside with that, it is important to

[15] https://github.com/P1sec/SigFW/

continuously monitor and analyse messages that cross network boundaries to detect potential attacks. This task can be performed by an attack detection and response system that detects illegitimate activity at an early stage and blocks suspicious requests, or passes information about unauthorized connections to third-party systems, thus increasing the efficiency of existing security measures. This approach ensures high-level protection without disrupting the normal operation of mobile networks. [8]

One important aspect to be considered in terms of security measures is that due to the architecture of the signalling protocols and infrastructure the electronic communication providers are the only ones capable of adopting any kind of security measures for customer protection. Subscribers are capable of adopting limited measures (e.g. data encryption). [5]

Conclusion

Telecommunications are key in nowadays societies. They represent the backbone, the primary infrastructure based on which our society works and it's the main instrument in allowing our democracy (and other EU core values such as freedom, equality, rule of law, human right) to function properly. As a consequence, here in ENISA (the EU cyber security agency) we consider assuring the security of our infrastructure as a top priority.

As mobile technologies evolve so does the threat landscape. Early generations of mobile networks 2G/3G rely on SS7 and SIGTRAN, protocols designed decades ago, without giving adequate effect to modern day security implications. Nobody at that time envisioned the scale that mobile networks could reach in the future, so trust and security were not issues. Nonetheless at the moment we are still using this legacy protocol to assure the interconnection between providers. The industry and security research community has started covering the topic, by providing good practices and necessary tools. But still, a lot more has to be done. Basic security measures seem to be implemented by more mature providers, but these measures assure only a basic protection level. More efforts need to be made so that an optimal protection level is achieved.

Current telecommunication mobile generation (4G) uses a slightly improved signalling protocol called Diameter. Build with the same interconnect principles in mind but on an IP base, the protocol has been proved vulnerable. The industry is still trying to understand exact implications and to identify possible workarounds. Attackers are also in the same phase apparently. It is our impression that the next step will be made soon by all parties involved. As soon as SS7 becomes sufficiently protected their focus will change towards the new attack surface.

While work is being done in addressing SS7 and Diameter attacks, only a small portion of the protocols has been studied. It is expected that new vulnerabilities shall be discovered. In addition, tools to scan and potentially attack mobile networks are now freely available. [5]

Stealing money, determining subscriber location, tapping calls and disrupting communication services are all threats made possible by exploiting SS7 vulnerabilities. With connections made possible by the Internet, mobile communication has become a preferred attack point for hackers looking to penetrate critical infrastructures and the enterprise. If mobile providers do not implement protection systems against SS7-based attacks, there is little doubt that the public, private organizations or even entire nations will be among the victims of such attacks in the near future. [6]

Main protection mechanisms:

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

The majority of flaws that allow an attacker to track a subscriber's location and steal data could be eliminated if we change network equipment configuration, and prohibit the processing of AnyTimeInterrogation and SendIMSI messages via HLR. The way to fix architecture flaws in protocols and systems is to block undesired messages. A system must consider the filtering of SendRoutingInfoForSM, SendIMSI, SendRoutung-InfoForLCS, and SendRoutingInfo. Filtering will help to avoid the risks of DoS, SMS interception, calls forwarding, subscriber's profile modification. Not all indicated SS7 messages are dangerous. Systems need to configure filtering to cut off only undesired messages used in attacks, and implement additional security tools, for example, intrusion detection systems. These systems do not interfere with network traffic and are capable of detecting malicious activity and its source as well as determining necessary configuration for message filtering. The most effective way to counteract all of the identified types of attacks (including the ones that exploit software errors) is a combination of these methods. The described options are most effective in cases where the mobile operator company has a regular and reliable set of procedures for the inner SS7 security audit. However most cellular carriers, especially small ones, struggle to support regular audit procedures. In such cases operators should use outsourcing options as this will help to determine the current level of their protection, uncover existing security threats, and minimize risks at hand by taking necessary actions to fix detected vulnerabilities. [7]

The overall security level of the SS7 networks examined was below average. Every single network fell victim to attacks aimed at data leakage, network disruption, and fraudulent actions. The research demonstrated that telecom companies employ various measures of protection but these are not enough to counteract all possible ways for attackers to penetrate the network. Even large operators are not protected against conversation tapping, messages monitoring, and fraudulent activity such as calls redirection and stealing. Additionally, hackers can pinpoint a subscriber's location at any given moment. In order to reduce risks, operators should employ a global approach to SS7 protection. They should conduct regular security audits of the signaling network and develop appropriate measures to mitigate risk based on vulnerabilities as they evolve. Clearly all operators need to employ additional security measures to better address threats. [7]

Common Security Measures

In general, most of the operators have implemented basic security measures especially for SS7. But basic measures only cover basic attacks.

According to Enisa, most operators (87%) implement SMS home routing, to protect their networks against from leaking sensitive information associated with a subscriber. Namely the IMSI, which uniquely identifies a subscriber for network related operations. It would also help to mount further attacks. SMS Home Routing offers additional security by implementing *message management* mechanisms in the home network to provide protection against external messages. [5]
In fact, that is the exact purpose for which Short Message Service was designed; communication between the home network components.

Monitoring the signalling network is regularly done by 69% of the respondents. Monitoring is of the utmost importance because it is the first step towards identifying and mitigating threats. Without monitoring, you cannot detect malicious traffic, and consequently you cannot react to it. In terms of methods used for traffic analysis, operators are using more than one method to achieve better results:

- 38% indicated statistical analysis of message logs,
- 35% real time detection of occurrences of predetermined signatures and
- 35% mentioned a regular analysis of massage logs.

Signalling firewalls have been implemented by roughly 28% of the respondents, a rather low percentage. But firewalls have their drawbacks also, as a firewall with only filtering could well protect the home subscribers in the home network, but the home subscribers in roaming or inbound-roamers could not be easily protected mainly because SS7 and Diameter are vulnerable to spoofing and the *Location Update* is not authenticated. In this respect signalling protection should not only be based on filtering but also on assuring confidentiality and integrity. [5]

Most of the operators (75%) responded that complexity and cost are blocking the implementation of advanced signalling protection. This is certainly not something unexpected. For example, monitoring should be done as close as possible to the interconnect links. Protection against attack patterns requires to monitor the

traffic in its entirety. The resilient nature of interconnect protocols, using load-sharing raises technical issues and might threaten availability.
In addition, the use of an SS7 or Diameter firewall poses a few problems. Detection and reaction to malicious traffic imposes an analysis on all the interconnect traffic. Detection of malicious traffic will never be perfect and misconfiguration may sometimes be interpreted as malicious actions. Responses to such a false positives may involve operator's liability and potential financial and legal aspects may apply.
Assuredly implementing a proper signalling protection in place will raise many complexity related issues. On top of this, for an operator to address sufficiently signalling security, a considerable investment is required. There are solutions available but their prices are not cheap. [5]

Evolving Security Solutions

MAP Security

The MAP protocol can be protected at the Network layer when IP is used as the transport protocol. However, whenever interworking with SS7-based networks is necessary, protection at the Application layer shall be used. The proposed solution for this is termed *MAP security* (MAPsec). [13]

The security services provided by MAPsec are:

- data integrity
- data origin authentication
- anti-replay protection
- confidentiality (optional)

Before protection can be applied, *Security Associations* (SA) need to be established between the respective MAP network elements. Security Associations define, among other things, which keys, algorithms and protection profiles to use to protect MAP signalling. The necessary MAPsec-SAs between networks are negotiated between the respective network operators. The negotiated SA will be effective PLMN-wide and distributed to all network elements which implement MAP Security within the PLMN.
For routing purposes, Signalling traffic protected at the Application layer should be indistinguishable from unprotected traffic to all parties, except for the sending and receiving entities. Protection at the Application layer implies changes to the Application protocol itself to allow for the necessary security functionality to be added.

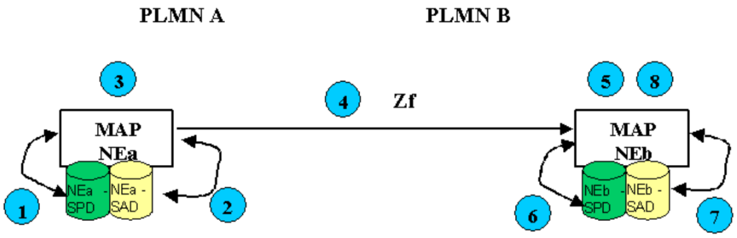
All MAPsec enabled Network Entities should maintain the following databases:

SPD *Security Policy Database* contains MAPsec policy information

SADB *Security Association Database* contains MAPsec SA information.

Imagine a network scenario with two MAP-NEs at different PLMNs (NEa and NEb) willing to communicate using MAPsec. Figure 19 presents the message flow:

Figure 20: MAPsec message flow.



In order to prevent active attacks all interconnected operators must at least use MAPsec with the suitable protection levels as indicated in the specification and treat the reception of all MAP messages (protected and unprotected) in a uniform way in the receiving direction.

The necessary SAs between networks are negotiated between the respective network operators. The negotiated SA will be effective PLMN-wide and distributed to all network elements which implement MAP layer security within the PLMN. Signalling traffic protected at the application layer will, for routing purposes, be indistinguishable from unprotected traffic to all parties except for the sending and receiving entities.
Additionally, inter-domain Security Associations require manual *Key Management* between the different operators, because the SA is subject to the respective roaming agreement. [13]

The Generic Subscriber Update Protocol

The *Generic Subscriber Update Protocol* (GSUP) is developed by the Osmocom project as a replacement to the complex MAP GSM implementation. It is used by OsmoSGSN and OsmoMSC to update and manage the local subscriber list in OsmoHLR. Functionally, it resembles the interface between the SGSN/VLR on the one hand side, and HLR/AUC on the other side.

Traditionally, the GSM *Mobile Application Part* (MAP) protocol is used for this purpose, running on top of a full telecom signalling protocol stack of MTP2/MTP3/SCCP/TCAP, or any of the SIGTRAN alternatives. In order to avoid many of the complexities of MAP, which are difficult to implement in the plain C language environment of the Osmocom cellular network elements like the SGSN, they introduced the GSUP protocol. [11]

The GSUP protocol and the messages are designed after the corresponding MAP messages, with the following main differences:

- The encoding uses TLV structures instead of ASN.1 BER
- Segmentation is not used, and it relies on the fact that the underlying transport protocol (IPA over TCP) can transport signalling messages of any size.

The protocol expects that a reliable, ordered, packet boundaries preserving connection is used. The remote peer is either a service that understands the protocol natively or a wrapper service that maps the messages to/from real MAP messages that can be used to directly communicate with an HLR.

Even though GSUP resembles most of the MAP signalling and authentication procedures, implementation is different and an translation entity is needed to achieve a real communication between traditional MAP enabled network entities. For example, most GSUP messages and their parameters are also found in their

MAP counterparts, although the opposite is not true. The protocol itself is redesigned and thus different security threats may arise. In fact, the main difference between the two Application layer protocols is perhaps their licence nature, with GSUP being an open-source standard. For this reason, we can expect it to dominate GSM installations accross the world in the near future.

Considerations on Diameter

Industry's focus on Diameter security has come later than in the SS7 case, and has certainly not reached maturity yet.[16] Diameter is derived from *Remote Authentication Dial-In User Service* (RADIUS) and provides an Authentication, Authorization and Accounting protocol for computer networks. In terms of design, it has borrowed many concepts from SS7, along with its vulnerabilities. Being a purely IP based protocol, there is an increased risk in the possibility of an intruder gaining access through hacking. The more knowledge the attacker has on Internet related protocols the more chances they have to succeed. This makes it in theory, simpler to exploit than SS7. Nevertheless, existing research indicated that, Diameter is currently less exploited than SS7. Actually, no respondent has mentioned seeing real attacks; nevertheless, there are recent developments indicating their appearance. The exact reason for this must be further investigated but could be related to the narrow adoption of Diameter worldwide, to the fact that attackers did not have the necessary time to prepare the attacks or to the fact that SS7 provides already satisfying results. Nevertheless, its vulnerabilities have been documented and theoretically exploited by the security community. [5]

[16] https://www.theregister.co.uk/2017/12/08/diameter_protocol_security_shortcomings/

References

[1] L. Dryburgh and J. Hewett, *"Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services"*. Cisco Press, 2004. ISBN 1-58705-040-4

[2] K. Jensen, A. Årnes and D. Van Thanh, *"Improving SS7 Security Using Machine Learning Techniques"*. Norwegian University of Science and Technology, 2016.

[3] Guy Redmill, *"An Introduction to SS7"*. Brooktrout Technology, 2001.

[4] Theodore S. Rappaport, *"Wireless Communications: Principles & Practice"*. Prentice Hall, 2002. ISBN 0-13-042232-0

[5] *"Signalling Security in Telecom SS7/Diameter/5G: EU level assessment of the current situation"*. ENISA, 2018.
https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g/at_download/fullReport/

[6] *"Signaling System 7 (SS7) Security Report"*. Positive Technologies, 2014.
https://www.ptsecurity.com/ww-en/analytics/ss7-vulnerabilities/

[7] *"Primary Security Threats For SS7 Cellular Networks"*. Positive Technologies, 2016.
https://www.ptsecurity.com/ww-en/analytics/primary-security-threats-for-ss7-cellular-networks-2016/

[8] *"SS7 Vulnerabilities And Attack Exposure Report"*. Positive Technologies, 2018.
https://www.ptsecurity.com/ww-en/analytics/ss7-vulnerability-2018/

[9] Philippe Langlois, *"Telecommunications Infrastructure Security: Getting in the SS7 Kingdom"*. P1 Security Inc., in the proceedings of Hackito Ergo Sum, 2010.
http://www.hackitoergosum.org/2010/HES2010-planglois-Attacking-SS7.pdf

[10] P. O. Vauboin, A. De Oliveira, *"Worldwide attacks on SS7 network"*. P1 Security Inc., in the proceedings of the Hackito Ergo Sum, 2014.
http://2014.hackitoergosum.org/slides/day3_Worldwide_attacks_on_SS7_network_P1security_Hackito_2014.pdf

[11] Neels Hofmeyr, *"OsmoHLR User Manual"*. Sysmocom s.f.m.c. GmbH, 2017.
http://ftp.osmocom.org/docs/latest/osmohlr-usermanual.pdf

[12] *"Mobile Application Part (MAP) specification"*. 3GPP TS 29.002 V15.4.0 Release 15. European Telecommunications Standards Institute, 2018.

[13] *"Mobile Application Part (MAP) application layer security"*. 3GPP TS 33.200 version 6.1.0 Release 6. European Telecommunications Standards Institute, 2005.
https://www.etsi.org/deliver/etsi_ts/133200_133299/133200/06.01.00_60/ts_133200v060100p.pdf

[14] Karsten Nohl, *"Mobile self-defense"*. 31C3: A new dawn, Chaos Computer Club e.V., 2014. https://media.ccc.de/v/31c3_-_6122_-_en_-_saal_1_-_201412271830_-_mobile_self-defense_-_karsten_nohl#t=1957

[15] Dmitry Kurbatov, *"Five Nightmares for a Telecom"*. Positive Technologies, 2013.
https://www.slideshare.net/phdays/d-kurbatov-5-nightmaresfortelco

[16] M. Kacer, P. Langlois, *"SS7 Attacker Heaven turns into Riot: How to make Nation-State and Intelligence Attackers' lives much harder on mobile networks"*. P1 Security, 2017.
https://www.blackhat.com/docs/us-17/wednesday/us-17-Kacer-SS7-Attacker-Heaven-Turns-Into-Riot-How-To-Make-Nation-State-And-Intelligence-Attackers-Lives-Much-Harder-On-Mobile-Networks.pdf

[17] Sharyn Alfonsi, *"Hacking Your Phone"*. CBC News, 60 Minutes, 2016. https://www.cbsnews.com/news/60-minutes-hacking-your-phone/

[18] Pierluigi Paganini, *"New security flaws in the SS7 protocol allow hackers to spy on phone users"*. Security Affairs, 2014. https://securityaffairs.co/wordpress/31262/hacking/flaws-ss7-protocol-spy-on-phone.html

[19] Pierluigi Paganini, *"Surveillance – How to secretly track cellphone users position around the globe"*. Security Affairs, 2014. https://securityaffairs.co/wordpress/28397/hacking/surveillance-solutions.html

[20] Pierluigi Paganini, *"SS7 Protocol: How Hackers Might Find You"*. Security Affairs, 2016. https://resources.infosecinstitute.com/ss7-protocol-how-hackers-might-find-you/

[21] Kim Zetter, *"The Critical Hole at the Heart of Our Cell Phone Networks"*. Wired, 2016. https://www.wired.com/2016/04/the-critical-hole-at-the-heart-of-cell-phone-infrastructure/

[22] Olivier Dubuisson, *"ASN.1, Communication between Heterogeneous Systems"*. France Telecom R&D, 2000. http://www.oss.com/asn1/resources/books-whitepapers-pubs/dubuisson-asn1-book.PDF

[23] Rauf Akram, *"SMS Tutorial"*. Rauf's Knowledge Portal, 2013. https://raufakram.wordpress.com/2013/12/17/sms-tutorial/

Appendix A: List of MAP messages

Taken from [12]:

- activateSS
- activateTraceMode
- alertServiceCentre
- anyTimeInterrogaton
- authenticationFailureReport
- anyTimeModification
- anyTimeSubscriptionInterrogation
- cancelLocation
- checkIMEI
- deactivateSS
- deactivateTraceMode
- deleteSubscriberData
- eraseCC-Entry
- eraseSS
- failureReport
- forwardAccessSignalling
- forwardCheckSsIndication
- forwardGroupCallSignalling
- mt-forwardSM
- mo-forwardSM
- getPassword
- informServiceCentre
- insertSubscriberData
- interrogateSs
- istAlert
- istCommand
- noteMsPresentForGprs
- noteSubscriberDataModified
- prepareGroupCall

- prepareHandover
- prepareSubsequentHandover
- processAccessSignalling
- processGroupCallSignalling
- processUnstructuredSS-Request
- provideRoamingNumber
- provideSubscriberLocation
- provideSubscriberInfo
- purgeMS
- readyForSM
- registerCC-Entry
- registerPassword
- registerSS
- remoteUserFree
- reportSmDeliveryStatus
- reset
- restoreData
- sendGroupCallEndSignal
- sendGroupCallInfo
- sendEndSignal
- sendAuthenticationInfo
- sendIMSI
- sendIdentification
- sendRoutingInfoForSM
- sendRoutingInfoForGprs
- sendRoutingInfoForLCS
- sendRoutingInfo
- setReportingState
- statusReport
- subscriberLocationReport
- ss-Invocation-Notification

- unstructuredSS-Notify
- unstructuredSS-Request
- updateGprsLocation
- updateLocation
- NoteMM-Event
- updateVcsgLocation
- cancelVcsgLocation

Appendix B: List of InserSubscriberData parameters

Taken from [12]:

- Invoke Id
- IMSI
- MSISDN
- Additional MSISDN
- Category
- Subscriber Status
- Bearer service List
- Teleservice List
- Forwarding information List
- Call barring information List
- CUG information List
- SS-Data List
- eMLPP Subscription Data
- MC-Subscription Data
- Operator Determined Barring General data
- Operator Determined Barring HPLMN data
- Roaming Restriction Due To Unsupported Feature
- Regional Subscription Data
- VLR CAMEL Subscription Info
- Voice Broadcast Data
- Voice Group Call Data
- Network access mode
- GPRS Subscription Data
- EPS Subscription Data
- VPLMN LIPA Allowed
- Roaming Restricted In SGSN/MME Due To Unsupported Feature
- North American Equal Access preferred Carrier Id List
- SGSN CAMEL Subscription Info
- LSA Information

- IST Alert Timer
- SS-Code List
- LMU Identifier
- LCS Information
- CS Allocation/Retention priority
- Super-Charger Supported In HLR
- Subscribed Charging Characteristics
- Access Restriction Data
- ICS Indicator
- CSG Subscription Data
- VPLMN CSG Subscription Data
- UE Reachability Request Indicator
- SGSN Number
- MME-Name
- Subscribed Periodic RAU-TAU Timer
- Subscribed Periodic LAU Timer
- MDT User Consent
- PS and SMS-Only Service Provision
- SMS in SGSN Allowed
- CS-to-PS-SRVCC-Allowed-Indicator
- P-CSCF Restoration Request
- Adjacent Access Restriction Data
- IMSI-Group-Id List
- UE Usage Type
- User Plane Integrity Protection Indicator
- DL-Buffering Suggested Packet Count
- Reset-IDs
- eDRX-Cycle-Length List
- Regional Subscription Response
- Supported CAMEL Phases
- Offered CAMEL 4 CSIs
- Supported Features
- User error