Aalto University
School of Science
Master's Degree Programme in Security and Mobile Computing

Siddharth Prakash Rao

# Analysis and Mitigation of Recent Attacks on Mobile Communication Backend

Master's Thesis

Espoo, 25 June 2015

Supervisors: Dr. Tuomas Aura, Aalto University
Dr. Dominique Unruh, University of Tartu

Co-supervisors: Dr. Silke Holtmanns, Nokia Networks
Dr. Ian Oliver, Nokia Networks

Aalto University
School of Science

| | |
|---|---|
| Aalto University<br>School of Science<br>Degree Programme in Security and Mobile Computing | ABSTRACT OF THE MASTER'S THESIS |


Author: Siddharth Prakash Rao


Title: Analysis and Mitigation of Recent Attacks on Mobile Communication Backend


| | | |
|---|---|---|
| Number of pages: 95+9 | Date: 25.06.2015 | Language: English |
| Professorship: Data Communications Software | Code: T-110 | |



Supervisors: Dr. Tuomas Aura, Aalto University
Dr. Dominique Unruh, University of Tartu

Co-supervisors: Dr. Silke Holtmanns, Nokia Networks
Dr. Ian Oliver, Nokia Networks



In the last quarter of 2014, several successful attacks against mobile networks were demonstrated. They are based on misuse of one of the key signaling protocol, SS7, which is extensively used in the mobile communication backend for signaling tasks such as call and mobility management. The attackers were able to locate the mobile users and intercept voice calls and text messages. While most attacks in the public eye are those which exploits weaknesses in the end-device software or radio access links, these recently demonstrated vulnerabilities exploit weaknesses of the mobile core networks themselves. Understandably, there is a scramble in the mobile telecommunications industry to understand the attacks and the underlying vulnerabilities. This thesis is part of that effort.

This thesis presents a broad and thorough overview and analysis of the known attacks against mobile network signaling protocols and the possible mitigation strategies. The attacks are presented in a uniform way, in relation to the mobile network protocol standards and signaling scenarios. Moreover, this thesis also presents a new attack that enables a malicious party with access to the signaling network to remove lost or stolen phones from the blacklist that is intended to prevent their use. Both the known and new attacks have been confirmed by implementing them in a controlled test environment.

The attacks are serious because SS7, despite its age, remains the main signaling protocol in the mobile networks and will still long be required for interoperability and background compatibility in international roaming. Moreover, the number of entities with access to the core network, and hence the number of potential attackers, has increased significantly because of changes in regulation and opening of the networks to competition. The analysis and new results of this thesis will help mobile network providers and operators to assess the vulnerabilities in their infrastructure and to make security-aware decisions regarding their future investments and standardization. The results will be presented to the operators, network-equipment vendors, and to the 3GPP standards body.



**Keywords**: Signaling Protocols, SS7, Mobile Core Network, Security

# CONTENTS

# LIST OF FIGURES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| 2G/3G/4G | 2nd/3rd/4th Generation (wireless telephone technology) |
| 3GPP | 3rd Generation Partnership Project |
| AAA | Authentication, Authorization, Accounting |
| ACM | Address Complete Message |
| AIN | Advanced Intelligent Network |
| API | Application Programming Interface |
| APN | Access Point Name |
| ATI | Anytime Interrogation |
| AuC | Authentication Center |
| BSC | Base Station Controller |
| BSS | Base Station Subsystem |
| BTS | Base Transceiver Station |
| CAMEL | Customized Application for Mobile-network Enhanced Logic |
| CAN | Channel Associated Signaling |
| CAP | Camel Application Part |
| CAS | Channel Associated Signaling |
| CCS | Common Channel Signaling |
| CEIR | Central Equipment Identity Register |
| CLEC | Competitive Local Exchange Carriers |
| CND | Call Number Display |
| CTIA | Cellular Telephone Industries Association |
| DoS/DDoS | Denial Of Service/ Dynamic Denial of Service |
| DPC | Destination Point Code |
| EIR | Equipment Identity Register |
| EMS | Enhanced Messaging Service |
| GGSN | Gateway GPRS Support Node |
| GMLC | Gateway Mobile Location Center |
| GMSC | Gateway Mobile Switching Centre |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| GSM | Global System for Mobiles |
| GSMA | GSM Association |
| gsmSCF | GSM Service Control Function |
| gsmSSF | GSM Service Switching Function |
| GT | Global Title |
| GTT | Global Title Translation |
| HLR | Home Location Register |
| HPLMN | Home Public Land Mobile Networks |
| HSS | Home Subscriber Server |
| IAM | Initial Address Message |

| | |
|---|---|
| IDP | Initial Detection Point |
| IETF | Internet Engineering Task Force |
| ILEC | Incumbent Local Exchange Carriers |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| INIT | Initiation Message |
| IoT | Internet of Things |
| IP | Internet Protocol |
| ISDN | Integrated Services Digital Network |
| ISPC | International Signaling Point Code |
| ISUP | ISDN User Part |
| ITU-T | International Telecommunication Union - Telecommunication Standardization Sector |
| IWMSC | Interworking Mobile Services Switching Center |
| LA | Location Area |
| LCS | Location Services |
| LIDB | Line Information Database |
| LIG | Legal Interception Gateway |
| LNP | Local Number Portability |
| LTE | Long Term Evolution |
| MAP | Mobile Application Part |
| MCC | Mobile Country Code |
| MMS | Multimedia Messaging Service |
| MNC | Mobile Network Code |
| MO/MT | Mobile Originated/Mobile Terminated |
| MS | Mobile Station |
| MSC | Mobile Services Switching Center |
| MSISDN | Mobile Station International Subscriber Directory Number |
| MSRN | Mobile Station Roaming Number |
| MSU | Message Signal Unit |
| MTP | Message Transfer Part |
| NDC | National Destination Code |
| NDS | Network Domain Security |
| NSS | Network Switching Subsystem |
| OPC | Originating Point Code |
| OSI | Open System Interconnection |
| PC | Point Code |
| PDP | Packet Data Protocol |
| PKI | Public Key Infrastructure |
| PLMN | Public Land Mobile Networks |
| PRN | Provide Roaming Number |
| PSN | Public Switch Network |
| PSTN | Public Switched Telephone Network |

| | |
|---|---|
| RA | Routing Area |
| RAN | Radio Access Network |
| RAND | Random Challenge |
| REL | Release Message |
| RRLP | Radio Resource LCS Protocol |
| RTDB | Real Time Database |
| SCCP | Signaling Connection Control Part |
| SCP | Signal Control Point |
| SCRC | SCCP Routing Control |
| SGSN | Serving GPRS Support Node |
| SIGTRAN | Signaling Transport |
| SIP | Session Initiation Protocol |
| SME | Short Message Entity |
| SMLC | Serving Mobile Location Center |
| SMS | Short Message Service |
| SMSC | Short Message Service Centre |
| SRES | Signed Response |
| SRI | Send Routing Information |
| SS | Supplementary Services |
| SS7 | Signaling System No. 7 |
| SSN | Sub System Numbers |
| SSP | Signal Switching Points |
| STP | Signal Transfer Points |
| TCAP | Transaction Capabilities Application Part |
| TCP | Transmission Control Protocol |
| TMSI | Temporary Mobile Subscriber Identity |
| TUP | Telephone User Part |
| UICC | Universal Integrated Circuit Card |
| UMTS | Universal Mobile Telecommunications System |
| USSD | Unstructured Supplementary Service Data |
| VLR | Visitor Location Register |
| VMSC | Visited Mobile Switching Center |
| VoIP | Voice over IP |
| VPLMN | Visited Public Land Mobile Networks |

# 1 INTRODUCTION

With the near-ubiquitous coverage of cellular networks and more affordable smart phones, the number of mobile users is increasing day by day. The telecommunication sector is growing continuously with a total of 3.6 billion unique mobile subscribers at the end of year 2014 [1]. At present, half of the world population is using mobile phones and subscriptions in their day to day life, and it is estimated that an additional of one billion mobile subscribers will be using telecommunication services at the end of year 2020.

In today's world, mobile networks have not only become the most vital part of communication infrastructure but also a major driving force behind global economic progress and welfare. Mobile communication systems have become a crucial part of the daily activities of most people ranging from voice calls, text messages and Internet access to providing emergency call services. In this context, assuring security to all the mobile subscribers has become a major concern of mobile network operators.

In spite the relative security guaranteed by the mobile operators and the advancements in technologies to protect the mobile phone users, attackers have competitively learned to exploit the vulnerabilities in existing mobile network communication to conduct illegitimate activities and gain control over personal information of mobile users. Repeated incidents of private calls, messages or pictures of government officials, celebrities and businessmen being leaked over the Internet have demonstrated concrete evidence about vulnerability of telecommunication systems. These incidents not only question the capability and responsibility of mobile operators, but also agitate common laymen about their personal privacy. While most attacks in the public eye have exploited weaknesses in the end-device software, less known attacks that exploit weaknesses of the mobile network have also become an everyday problem. This thesis focuses on such attacks against the mobile backbone and signaling systems.

Most people consider a mobile telecommunication network as a complex system built with cutting edge technologies. This perception of people leads to a misconception about the security and privacy protection provided by these networks. Most people assume that attacks can be performed only by skillful hackers and sophisticated government intelligence agencies as the

attacks might be cumbersome and expensive to execute. The fact is that the mobile network is indeed quite a complicated system built with multiple subsystems, which in turn might have different underlying technologies. But the security of the whole network is determined by the security level of the weakest subsystem and many points of the modern networks are surprisingly open for professional or institutional attackers.

## 1.1 Motivation

In this era of mass surveillance and cyber espionage, numerous attacks are conducted by government agencies and evil hackers on mobile users. Recent report in the media revealed that one of the major government surveillance agencies is collecting bulk information from the mobile traffic [2]. Yet another leaked report [3] from Ukrainian communication regulators (NKRZ) and Ukrainian Security Services (SBU) disclosed that suspicious mobile network packets from one of the telecommunication partners from Russia was revealing location of mobile users and there were high chances that their voice calls were being intercepted. Investigation of the above mentioned incidents by security experts unveiled the fact that those attacks have been carried out by misusing the technical features of a mobile core network technology known as Signaling System #7 (SS7) protocol. The researchers demonstrated that the SS7 network is vulnerable and the loopholes in SS7 protocol have been utilized for surveillance of mobile communication.

SS7 protocol dates back to 1970s when it was used by a closed community of national telephone network operators and was built based on the trust between those operators. Today, SS7 is also used for interconnectivity between mobile network operator networks and to enable roaming and cellular services across operator domains. Since the access to the mobile core network was initially restricted only to the trusted telecom operators, SS7 was considered to be safe as the physical security of underlying network elements and communication channel was assured. Regardless of the advancement in IP-based mobile technologies, SS7 still continues to dominate the telecommunication world because it has become the backbone of Global System for Mobile Communications (GSM) systems and all new cellular technologies based on it. However, the mobile networks are no longer the realm of a few trusted national operators. Newer technologies like SIGTRAN and Session Initiation Protocol (SIP) have increased the entry points to mobile core network and the opening of the telecommunications market for

competition has increased the number of “trusted” operators far beyond what was originally intended.

In the last quarter of 2014, several successful attacks [4] using the SS7 network such as eavesdropping [5], tracking of user [6], SMS spoofing [7] and SMS redirect [8], have been demonstrated. However, an in-depth technical research of these attacks from the mobile network provider’s point of view to understand the vulnerabilities in the existing systems has been lacking. Single attacks have been publicized mainly for the purpose of marketing consultancy services, and there is no published analysis that would give an overall picture of the vulnerabilities. This knowledge gap has stood as hindrance to implement the necessary security measures.

This thesis addresses the gap between attack discovery and the much needed security implementations from the network providers, by presenting a thorough analysis of attacks against SS7-based mobile network signaling and the possible mitigation strategies. The information in this thesis will help mobile network providers and mobile network operators to assess the vulnerabilities in their infrastructure and to make security-aware decisions regarding future investments. The analysis and new results of this thesis will, in particular, be used to support standardization of security features in the 3rd Generation Partnership Project (3GPP) arena.

## 1.2 Goals

The goal of this thesis is to provide a comprehensive analysis of recent attacks on mobile network communication backend specifically targeting the Signaling System #7 (SS7) protocol. The thesis includes a thorough analysis of signaling-protocol vulnerabilities in the Network Switching Subsystem (NSS) i.e. mobile core network and roaming architecture of telecommunication backend. The background literature review explains the underlying signaling message details, flows and network entity descriptions.

The primary goal is to conduct exhaustive research to analyze the recently published SS7 attacks by elaborating the attack preparation phase and to increase our understanding of the various attack scenarios by inspecting the malicious message flows. This perusal will lead to new information about the outcomes and impact of already known attacks; to potential

countermeasures and mitigation strategies; and finally to the discovery of new attacks. Furthermore, a secondary goal is to briefly consider how the transition to the newer IP-based Long-Term Evolution (LTE)/ Diameter protocol, which is expected to eventually replace SS7 will affect mobile network security.

## 1.3 Brief summary of results

An in-depth inspection of the known attacks on the mobile communication backend was conducted, and the results of this investigation are thoroughly articulated in this thesis. The attacks are analyzed and explained in the context of the underlying signaling architecture and message flows. The attacks analyzed are categorized based on the possible impacts and the underlying modus operandi. Furthermore, some new attack vectors were discovered and documented. For reasons of responsible disclosure, only one of the two new attacks can be explained in this thesis. The results will be presented to the relevant equipment manufacturers and standards bodies, and the new attack in Chapter 5 has been submitted for publication. A brief outline of mitigation strategies and counter measures is also provided.

## 1.4 Scope of the thesis and the author's contribution

The thesis work has been carried out at Nokia Networks Finland under the supervision of Dr. Silke Holtmanns and Dr. Ian Oliver of the Security Research team. The author has implemented most of the attacks surveyed in this thesis (in a protected test environment, to avoid attacking real world systems) and verified that the attacks actually work. The implementations confirm the feasibility of the attacks as described in chapter 4, and constituted a major part of the work in preparing this thesis. Due to company policies and reasons of responsible disclosure, some of the information related to analysis strategy, network traces, actual behaviors, success rates, and codes cannot be revealed in a public document such as this thesis. However, the included information should be sufficient to assure the readers that these are real security issues that also take place in deployed cellular networks.

In the beginning of chapter 4, an executive summary of research methodology has been outlined. The work methods are typical of systems security research and of the type that is commonly used to contribute to security protocol standardization in the 3GPP arena. Thus, instead of writing the analysis methodologies from a security audit point of view, the workflow

of attacks has been outlined in detail with references to the relevant 3GPP specifications and references. This information is of the kind that is needed as background information for the standards body and operators to decide on the countermeasures that will be implemented. The Appendix provides further information to support some of the aspects mentioned as part of the attacks.

Note that frequent use of the word 'analysis' in this thesis might mislead the reader to expect a mathematical model or network traces of verifications. We stress that in our context, analysis means reviewing, structuring, and analyzing the feasibility of the attacks, as is typical in security analysis in the systems security field.

The main part of this thesis has been structured to fit "Review-type study" as mentioned in the official guidelines document of University of Tartu [9]- section 3.1.2. Sufficient references have also been given to the original ideas of different authors, which have been synthesized into one coherent picture. Currently there are no other public document available which provide a similar comprehensive summary of major core network attacks. So this thesis will be, to the knowledge of its author, the first of its kind.

Additionally, the author has also found new attack vectors which has been described in chapter 5. The discovery, thorough description and proof-of-concept implementation of new attacks, inspired by previous literature, is a typical working methods of the systems security area, which justifies the entitlement of the thesis to fit into the category of "Review-type study". In a broad sense, this part of the thesis also fits into the category ‘Solution of Application development task’, although the developed and implemented results of security research are often negative i.e. new attacks.

## 1.5 Structure of Thesis

Chapter 2 provides the essential background regarding the mobile network core network signaling system and the SS7 protocol stack. An outline of the various core network entities and addressing schemes is given.

Chapter 3 articulates various potential entry points of an attacker to the mobile core network. Additionally, this chapter highlights the current status of telecommunication security.

Chapter 4 explains the known attacks against mobile network that exploit SS7 features. The attacks and the exploited signaling features are presented in a uniform way. This chapter also classifies the core network attacks into categories such as location privacy breach, call interception and eavesdropping, and SMS based attacks. Each of these categories elucidates different attack methods.

Chapter 5 illustrates one of the new attack vectors uncovered by the author during the thesis project. This chapter illustrates how an attacker can unblock stolen mobile phones without the mobile operator's cooperation using a loophole in core network signaling.

Chapter 6 proposes potential counter measures against the attacks that have been described in Chapter 4.

The Chapter 7 contains a brief discussion of the newer technologies that will eventually replace SS7 and Chapter 8 concludes the thesis.

# 2 BACKGROUND

## 2.1 Introduction to SS7

Signaling System No. 7 (SS7) is one of the most widely used network architecture and a protocol used in telephony world. It is also known by the name C7 outside North America. SS7 is standardized by International Telecommunication Union Telecommunication Standardization Sector (ITU-T). This standard articulates specific set of protocol about information exchange over a digital signaling network in the public switched telephone network (PSTN) systems. SS7 is widely used in cellular (wireless) and fixed-line (wire line) for call establishment, billing, routing and information exchange. Alongside basic communication functionalities such as setting up and release the telephone calls, SS7 serves as a rich source of meta-data and serves various other purposes within the communications network. It has served its purpose over four decades and has been a substantial source of income for the service providers. Though it is not going to last in the industry for various outdated methods and security vulnerabilities, many aspects of SS7 will be replicated in the signaling networks.

## 2.2 Application of SS7

Being the backbone of Public Switched Telephone Network (PSTN), SS7 protocol suite has its diverse application across the global telecommunication network. It is the signaling protocol used between the control elements in the mobile core network. When a mobile is switched on, the identification, authentication and registration of the Subscriber Identity Module takes place through SS7 based signaling. SS7 is also needed each time we make a telephone call which goes beyond local exchange. Despite being used in daily routine for mobile telephony, many of the end users are unaware of its existence or diverse applications.

Other than those mentioned above, here are the application of SS7 network and protocol:

1. Call establishment, management and release.
2. Short Message Service (SMS)
3. Supplementary services by the mobile operators such as Call Number Display (CND), call waiting and call forwarding.

4. Line Information Database (LIDB) which has information related to subscriber's identification such as name and address along with billing information.
5. Local Number Portability (LNP)
6. Toll-free numbers for telemarketing
7. Televoting
8. Enhanced Messaging Services (EMS) such as logos and ringtone delivery.
9. Call blocking (Do-not-call enforcement)

Besides its applications in telecommunication networks, it also acts as a connection to the data communication world by providing features like Internet call-waiting, games based on locations, services which uses browser based telecommunication, Hotspot billing, etc.

## 2.3 SS7 Network

### 2.3.1 Signaling Network Architecture

Definition of signaling according to ITU-T is as follows "The exchange of information (other than by speech) specifically concerned with the establishment, release and other control of calls, and network management, in automatic telecommunications operations" [10] . Users of PSTN hence exchange many such signals with network elements; the user dialing digits and sending a waiting or dial tone are some examples of it. Telephony signaling can be classified into two categories namely 'subscriber signaling' and 'network signaling'.

As shown in Figure 2.1, subscriber signaling happens on the link between subscribers (end users) and the nearby local switch; whereas the signaling that takes place between the nodes of core network is known as network signaling. The latter means network signaling which takes place between source and destination local switch through the core network. Network signaling is complex compared to subscriber signaling as it supports various database-driven functionalities such as calling plan validation, Local Number Portability and roaming. Since the SS7 protocol stack comes under the network signaling, the rest of this thesis will consider only network signaling.

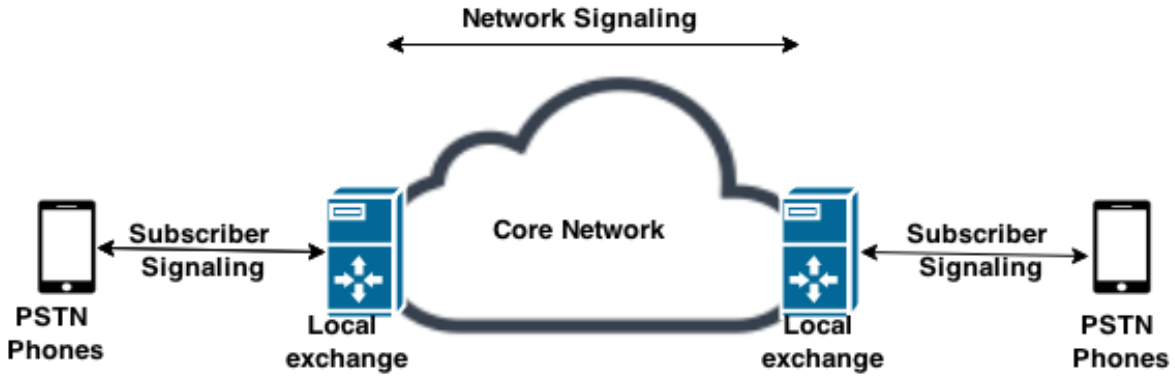



**Figure 2.1: Categories of signaling.**

Implementation of network signaling is possible by two methods namely Channel Associated Signaling (CAS) and Common Channel Signaling (CCS). Predecessors of SS7 such as initial versions of Signaling System Number 6 (SS6) used CAS methods, however currently it is not widely deployed. In CAS systems, most of the signaling takes place in a deterministic manner. For example, a dedicated fixed signaling capacity is pre -allocated for every trunk in a fixed way. This approach was prone to attacks where the subscriber can make free phone calls illegally by generating line signals with the help of handheld tone generator placing it near the mouthpiece of the phone. Major disadvantage of CAS based systems is that signaling cannot be done in the in the call connection phase, which imposed limits on signaling states. Another drawback is that the resource allocation is inefficient because of its deterministic nature.

On the other hand, the resource (signal) allocation in CSS happens in a need-based non-deterministic way, which makes it more efficient than CAS. The signaling capacity here is provided in a common pool and it will be used where and when necessary. SS7 is a purely CCS based protocol and is packet based carrying 200 bytes of information in each SS7 packet. The advantage of being a packet based approach is that it can support two different ways of signaling:

1. Circuit based signaling: This indicates the primary purpose of signaling such as set up, management and dropping telephone calls.
2. Non-circuit based signaling: This type of signaling facilitates data transfer between network entities for purpose other than telephone calls.

Often, the telephone calls are referred to as voice and anything other than voice are referred as user traffic or signaling. Since SS7 is based on CCS, it indeed makes sense to know more about it. CCS supports three different types of *signaling modes.* Signaling mode refers to the type of relationship that the network traffic and signaling path holds. This matters to CCS mainly because of the reason that it is not a fixed path. So the efficiency and performance would matter on the relationship between the signaling modes. The brief description of signaling modes of CCS follows:

1. Associated mode: There are fixed signaling paths between the switches. This mode is less complicated to design, but are less efficient and more expensive in a large network. The requirement of this mode is that the underlying network should have mesh topology connecting all nodes.

As represented in Figure 2.2, the voice and the user traffic transmission happens in the same route.


**Figure 2.2: Associated Mode of Signaling.**

2. Non-associated mode: As the name indicates, there will not be any fixed paths for transmission which results in potentially multiple of paths during a voice call or other user traffic. There is no guarantee that voice and user traffic would reach to the destination at same time as they might take different paths and there is no specific method to re-order the out of sequence messages. This is the reason why non- associated mode is not used in SS7 protocol.

3. Quasi -associated mode: This is more economical way compared to the associated mode mainly because there is no need of fully mesh topology in the underlying network as the signaling can be routed through intermediate nodes avoiding the direct links. It is designed in such a way that voice calls and user traffic arrive simultaneously as the path will be fixed at the beginning of a call based on the need. It differs from non-associated signaling mode by offering a relatively fixed path.

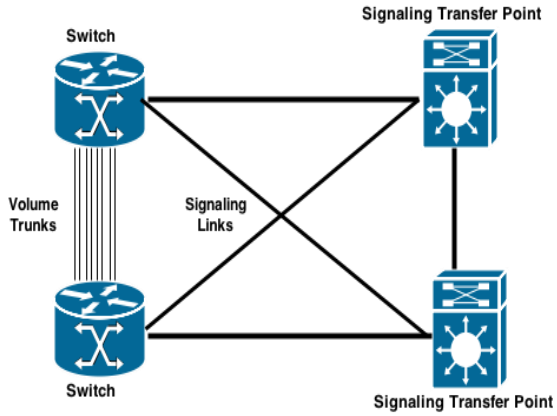



**Figure 2.3: Quasi-associated mode of signaling.**

The advantage of CCS over CAS is that it provides more flexibility and control of signaling. It comparatively less expensive alongside facilitating efficient resource allocation and usage, resulting in faster call set up. It overcomes the security limitations of CAS as an end user cannot generate signals pertaining to the core network.

### 2.3.2 Signaling Architecture

When we have a deeper look into SS7 architecture, it uses bi-directional channels called signaling links where it transfers the messages. These signaling links connect the building blocks of the network known as signaling points. There are three signaling points namely Signal Switching Point (SSP), Signal Transfer Points (STP) and Signal Control Points (SCP). Each of these points is identified by a unique code, and that code will be carried in the signaling message between such the signaling points. This code identifies the source and destination. The signaling path for a message will be chosen by a point using a routing table. The Figure 2.4 shows the visual representation of the SS7 signaling points in the architecture:

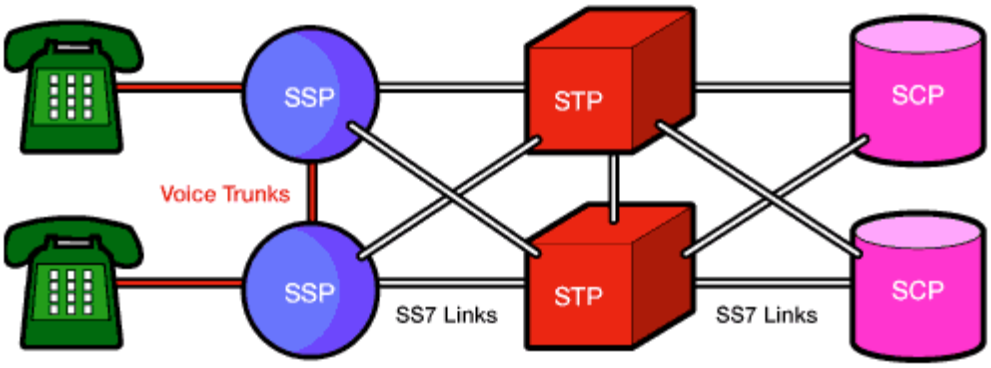



**Figure 2.4: SS7 signaling points [11].**

Brief descriptions of the signaling points are as follows:

1. Signal Switching Point (SSP): These are the telephone switches which initiate, switch or terminate calls. They communicate with other SSPs to establish, manage and release voice circuits. They are capable of communicating with SCP's database to check the routing information in case of a toll-free number.
2. Signal Transfer Points (STP): These are the packet switches which perform routing of incoming signaling message from the source towards the destination based on the information contained in the SS7 message.
3. Signal Control Points (SCP): These are nothing but databases which aid the services that are supplementary to normal calling. Usually SCPs are deployed in pairs with the STPs for reliability.

In accordance with the usage in the network, the links between SS7 signaling points are logically divided into six types - “A” through “F”. Although all these links are either 56Kbps or 64 Kbps bidirectional data links supporting the lower layers of the protocol, they differ by their usage in connecting the signaling points. The Figure 2.6 below shows the different signaling link types:

1. A Links: Access links (A link) interconnects the signaling points (either SSP or STP or SCP). This type of link is used to transmit the messages that are originated or destined to signaling end points. In Figure 2.6, examples of A link are 2-8, 5-12, etc.
2. B Links: Bridge link (B link) interconnects one STP with another. When there are multiple networks, the primary STPs of these networks are connected in a quadrilateral

manner. The links in the Figure 2.6 such as 8-7, 7-11, 11- 12 and 12 -8 makes one such quad.

3. C Links: A Cross link (C Link) interconnects STPs which are performing similar functions with their mated pair. Any message will be transmitted through this type of links only when a specific STP was no other routes to reach the destination such as in the case of link failures and thus enhances the reliability of the signaling network. The links 7-8 and 9-10 represents the C links.
4. D Links: D link stands for 'Diagonal link' which interconnects primary STP pair (such as an inter-network gateway of the quad-linked STPs as explained before) to a local STP pair. This can be used at different hierarchical levels. 8-9 and 7-10 are examples of D link.
5. E Links: An 'extended link' (E link) connects an SSP to an alternate STP which serves as a substitute signaling path when the main or home STP cannot be reached. Simply put, messages will be transmitted from the SSPs to STPs when the A link is not functioning. This kind of links will be deployed only when it makes a marginal difference to the reliability matrix of the network. In the Figure 2.6, 1-11 and 1-12 represents E links.
6. F Links: F link stands for 'Fully associated link'. They connect two signaling end points that are not traditionally included in the network with STPs. As shown in the Figure 2.6, link 1-2 is an F -link. These kind of links are generally not deployed between two networks as they bypass the security measures provided by STPs.

The difference between B and D link is negligible or rather arbitrary and for this reason, those links are termed as 'B/D links'. As we can infer, the difference between all the types is just at a logical level and irrespective of their name, these signaling links carry messages within the SS7 network.

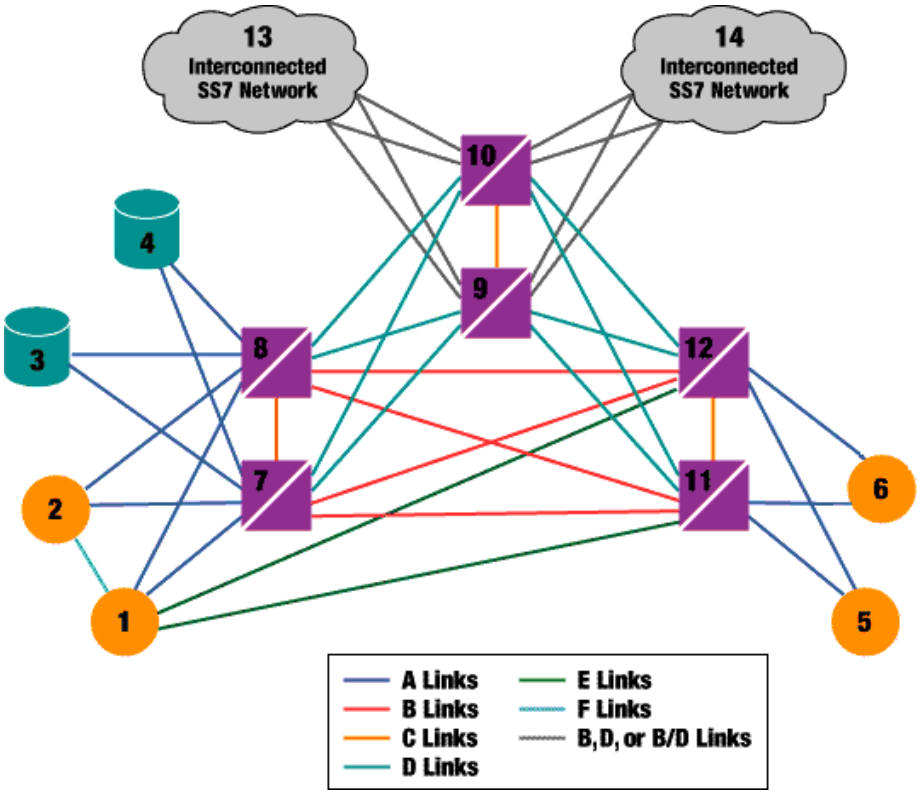



**Figure 2.5: SS7 signaling links [12].**

## 2.4 SS7 Protocol Stack

The hardware and software functionality of the SS7 protocol are divided into functional abstractions called layers. A comparison of Open Systems Interconnection (OSI) reference model along with SS7 protocol stack in given in the Figure 2.7.

**Message Transfer Part (MTP):**

This is divided into three levels – MTP level 1, MTP level 2 and MTP level 3. MTP level 1 being the lowest layer, works similar to that of the physical layer of OSI model as it defines the physical and electrical characteristics of a signaling link. MTP level 2 functions as the data link layer by facilitating flow control, sequence validation and error checking. This layer guarantees the accuracy of message transmission between two signaling points. Similar to that of network layer in OSI model, the MTP level 3 extends the functionality of MTP level 2 with its capabilities such as routing, congestion control and node addressing. When there is a link failure, this level re-routes the network traffic away from the failed parts of the network.

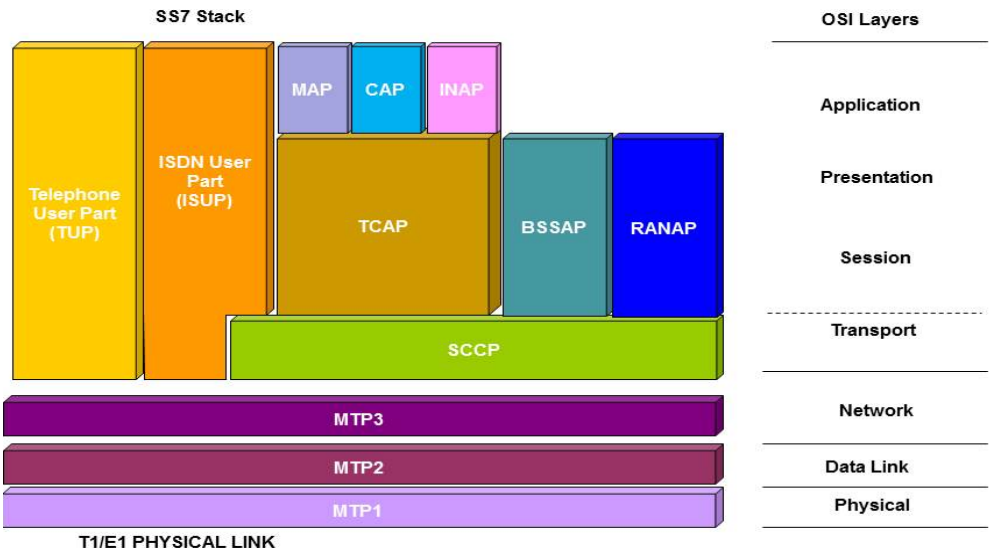



**Figure 2.6: SS7 Protocol Stack [13].**

### Signaling Connection Control Part (SCCP)

SCCP facilitates functionalities such as Global Title Translation (GTT) and network services. Together with TCAP, this layer acts equivalent to that of transport layer of the OSI model. Further details about the functionality of SCCP will appear in the upcoming chapters.

### Telephone User Part (TUP)

In most countries, this level is replaced by ISDN, but it can still be seen in countries like China and Brazil. It supports the basic call establishment and release. This deals only with the analog circuits.

### Transaction Capabilities Application Part (TCAP)

This layer contains the messages and protocols that serves as the communication between applications within the signaling points. This is mainly used in those services which need database support such as Advanced Intelligent Network (AIN) and toll-free numbers. To be more specific, the messages such as queries and responses which are exchanged between SSP and SCP are carried through TCAP messages. This layer also takes care of equipment identification and roaming in mobile networks.

**ISDN User Part (ISUP)**

This layer defines the protocol for voice trunk call establishment, management and termination in which they carry voice and data between the calling and called party. The only calls which do not use ISUP protocol are the calls that originate and terminate in at the same switch. Contrary to the name, along with ISDN calls, ISUP will also be used for non-ISDN based calls over a Public Switched Network.

**Message Application Part (MAP)**

Message Application Protocol (MAP) is one of the applications of the SS7 protocol stack which provides all the additional signaling functionality of the core network. It is responsible for mobility management and such additional services required by mobile networks. MAP is used between many elements of the core network; Home Location Register (HLR), Equipment Identity Register (EIR), Mobile Switching Center (MSC) and Visitor Location Register (VLR), and others. With the release of latest 3rd Generation Partnership Project (3GPP) specifications, MAP supports 81 services [14], which can be categorized as mobility management, operations and maintenance, call handling, short message services, supplementary services, location services, and Protocol Data Packet (PDP) context services. Among the network elements that MAP protocol uses, HLR and MSC are the most important components. These take dynamically the role of MAP-service user or MAP-service provider in the MAP service model. The network elements of the core network are addressed by MAP using Sub System Numbers (SSN) and Global Title (GT) provided by Signaling Connection Control Part (SCCP) of SS7.

As MAP uses the SS7 stack with the help of the Message Transfer Part (MTP), SCCP and Transaction Capabilities Application Part (TCAP) layers, it also facilitates inter-MSC handovers during a call. Alongside subscriber and location management, it is also responsible for mobile terminal validation, fault recovery, and authentication and security. It does not handle the cell level handovers but manages any handovers above that.

## 2.5 Overview of core network entities

Section 2.3 of this chapter provides a logical abstraction of the core network in terms of SSPs, STPs and SCPs. However, the practical implementations of those abstracts are in terms of various network elements. This section gives a brief outline of the overall mobile telephony

network, emphasizing the functionality of the major core network elements. Figure 2.8 outlines the architecture of core network including the Home Public Land Mobile Network (HPLMN) and the Visited Public Land Mobile Network (VPLMN) core network.

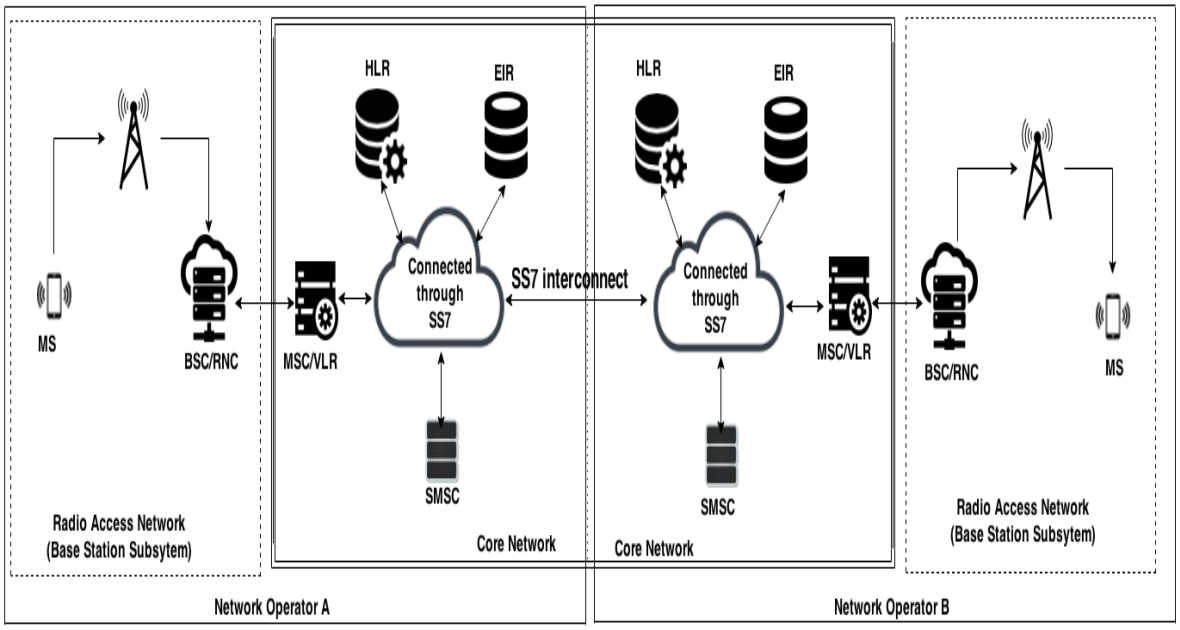



**Figure 2.7: Overview of mobile network architecture.**

The HPLMN is the mobile network to which the mobile users has subscribed. Any network other than HPLMN is considered to be VPLMN. When the mobile users roaming in VPLMN, that network will receive subscription information (such as billing, profile, identities) from the HPLMN. MSC and VLR are typically collocated in each network and will be considered as one unit. The HLR contains the subscriber and service information. EIR is the entity that provides verifies whether a mobile device has been reported as stolen or missing. The EIR stores the list of stolen or missing devices which is queried by HLR. Since the scope of this thesis is limited to the core network, details regarding the Radio Access Network (RAN) are omitted.

As said, the Home Location Register (HLR) is a centralized database which stores subscription related data [15] and service data. It also stores global titles and routing information (e.g. Access Point Name). Subscriber information such as location details is retrievable using the International Mobile Subscriber Identity (IMSI) of the Subscriber Identity Module (SIM) card or the USIM application on a Universal Integrated Circuit Card (UICC). Likewise, service

information such as the operator specific services to which the subscriber has subscribed to are stored in the HLR. An internal mapping is maintained by HLR between IMSI and MSISDN. Network entities like MSC and VLR uses the SS7 MAP protocol to interact with the HLR. The HLR is queried for various purposes such as location updates, routing and authentication. To limit the load on the HLR, the network operator might configure the number of checks regarding subscribers. An adequate level of such checks must be maintained, however, because decrease in such checks increases the risk of unauthorized access to network facilities (e.g. using an invalid SIM).

MSC works as an entry point to core network from the Radio Access Network (RAN). It bridges the Base Station Subsystems (BSS) and core network elements such as HLR using the SS7 MAP protocol [16]. It handles also other operations like managing the interfaces and billing and call processing. It is often collocated with the VLR.

As mentioned, EIR provides features to tackle mobile thefts by preventing stolen or banned mobile equipment from accessing the network [14]. This is facilitated by checking the International Mobile Equipment Identity (IMEI), which is provisioned during mobile manufacturing, against black, white or grey listed sets from the EIR database. The data is retrieved using the mobile device specific IMEI as a key, which is independent of the IMSI, MSISDN or SIM/UICC card identifier ICC_ID [14].

Furthermore, the Short Message Service Center (SMSC) is the core network element responsible for storing and forwarding short messages [17]. Billing center (not shown in the Figure 2.8), which includes gsmSCF, gsmSSF, etc. is responsible for subscriber billing for their calls, SMS and any other value added services. The Authentication center (AuC) is yet another network entity which is responsible for authenticating the subscriber SIM or USIM before allowing the use equipment to connect to cellular services. However, a detailed description of AuC is omitted here because, within the core network, the traffic will be un-encrypted and AuC does not play a major role.

## 2.6 Identifiers and Addressing Schemes

The diverse range of subsystem within mobile network use several different identifiers and addressing schemes to uniquely identify the network elements, applications and subscribers.

The Figure 2.9 illustrates the identifiers and addressing schemes used at some of the key layers of the SS7 protocol stack.

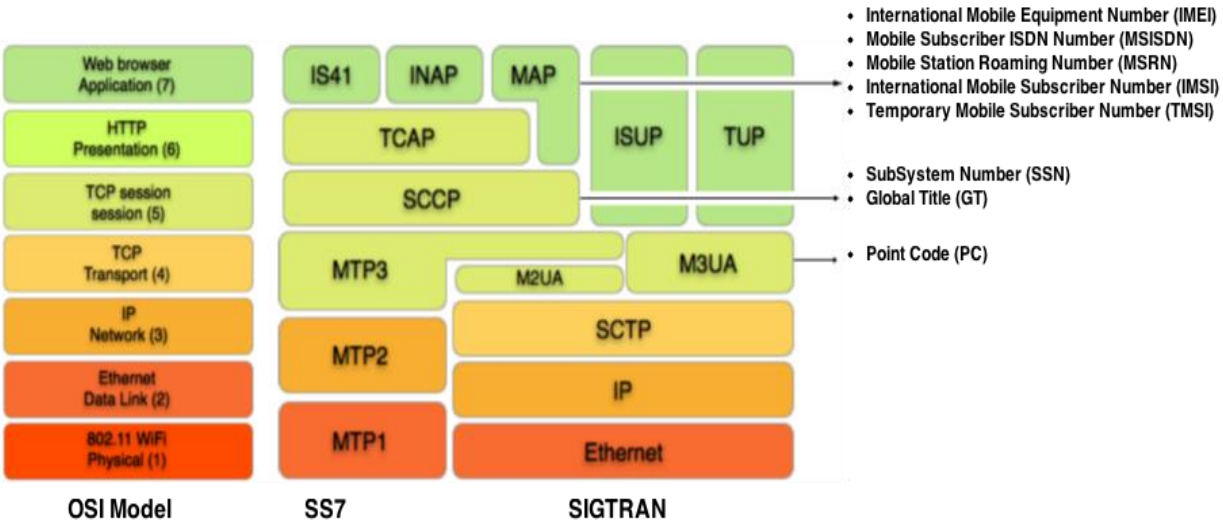



**Figure 2.8: Identifiers and identifiers used at different layers of SS7 [18].**

The purpose of the IMEI [19] is to identify each individual mobile device. IMEI is a unique number to identify mobile phones and satellite phones over the GSM, Universal Mobile Telecommunications System (UMTS) and Long-Term Evolution (LTE) networks [20]. The IMEI consists usually of a 15 digit unique number often complemented by a check digit which is excluded as part of the IMEI check transmission [19]. The IMEI can be up to 17 digits long as some manufactures add a two-digit software version of the device. All mobile manufacturers are mandated to equip any mobile device with an IMEI number and strict measures are taken to make it tamper proof by physical, electrical or software methods. Such genuine IMEI numbers holds all the required information for the network operators to trace a mobile device's origin of production uniquely with the help of EIR when it is required.

International Mobile Subscriber Identity (IMSI) on the other hand uniquely identifies the cellular network subscription and is used by the core network for identifying the mobile's home network and HLR. It is used for obtaining information on network service usage by the subscriber [19]. The IMSI is up to 15 digits long but it can be shorter than that depending on the network operator. The first three digits of IMSI are the Mobile Country Code (MCC), the next two are Mobile Network Code (MNC), which identify uniquely the home operator of the

subscriber, and the following ten digits are the Mobile Subscription Identification Number (MSIN) within the scope of that operator. [21]

To avoid extensive use of IMSI and hence to protect subscriber privacy, a temporary substitution of IMSI called the Temporary Mobile Subscriber Identity (TMSI) is used in mobility signaling. Since TMSIs have just the local significance, it is stored in the MSC/VLR only. Unlike IMSIs, the TMSIs are not stored in HLR.

Mobile Subscriber ISDN number (MSISDN) is simply the phone number of each subscription of the mobile users. It contains a 3 digit Country Code (CC), 2-3 digits National Destination Code (NDC) and a 10 digit Subscriber Number (SN). However, when the user is in roaming (or in VPLMN), the mobile station is recognized by a provisional location dependent ISDN number known as Mobile Station Roaming Number (MSRN). It has the similar format of MSISDN, but all the codes refer to the visited network rather than home network. This number will be used for connecting voice calls to the mobile device in its current location.

Subsystem Number (SSN) [21] is used in the SCCP signaling part to uniquely identify the applications within the core network. Global Title (GT), which we have already referred to, is yet another addressing scheme used in the SCCP protocol [22] for uniquely identifying the network elements for routing purposes. GT can range up to 15 digits. In layman's terms, SSN is equivalent to a TCP ports whereas GT is equivalent to an IP address.

Point Code (PC), on the other hand, is a 14 or 24-digit address similar to a MAC address, used to uniquely identify signaling point nodes in the MTP3 layer in the destination field of Message Signaling Unit (MSU). The three types of point codes according to ITU-T Q.704 standards are the Originating Point Code (OPC), Destination Point Code (DPC) and International Signaling Point Code (ISPC).

Routing of signaling messages within the core network is based on the combination of PC, GT and SSN addressing schemes. IMSI and IMEI are used to identify the subscriber's profiles and mobile terminals.

# 3 SS7 ATTACK SCENARIO

In this chapter, we discuss how an attacker can gain access to the SS7 mobile core network with the help of different entry points. Also it gives a brief outline of the attacks that will be discussed in the rest of this thesis.

## 3.1 Overview of entry points to core network

The number and complexity of interfaces between heterogeneous network entities pose major vulnerabilities to the SS7 mobile core network. Additionally, expanding interdependence and interconnectivity between the telecommunication networks and Internet has elevated the threats. The vulnerabilities in Internet and mobile networks affect each other. However, the key loophole of the SS7 backbone system lies in the lack of authentication procedures, as SS7 was intended for closed telecommunication coteries.

Changes in the regulation and opening of the telephony industry to competition has given rise to easier ways to get into the mobile core network. For example, the United States "Telecommunications Act of 1996" [23] enforces laws to "*let anyone enter any communication business – to let any communication business to enter any market against any other*" [24]. It also mandates the implementation of Legal Interception Gateways (LIGs) [25] which allows government agencies to lawfully intercept mobile communication. The "Telecommunications Act of 1996" allowed the small scale Competitive Local Exchange Carriers (CLECs) to introduce new trends in telecommunication industry by breaking the monopoly business of Incumbent Local Exchange Carriers (ILECs). ILECs have a large scale establishment and hence expertise along with measures to address the security needs. CLECs, on the other hand, being relatively small companies and new entrants to the market, may be more insecure because of the budget constraints and need to compete by cutting costs. Any of the CLECs, including ones established by malicious attackers, can gain access to the SS7 core network at a reasonably low cost [23]. Since STPs and SCPs have human facing frontend systems, an attacker can compromise them in a CLEC environment and thus gain control over the core networks.

Another potential threat to the closed backend core network comes from the relatively inexpensive ISDN connection. By injecting malicious ISDN (ISUP) messages, an attacker can

connect to SSPs, which bridges end users to SS7 entry points and hence enter the core network. The attacker can also execute Distributed Denial of Service (DDoS) attacks by overloading the SSP entities beyond its capabilities and harm interconnection between SSPs and STPS [13].

Yet another threat of attacker gaining access to the core network comes from Local Number Portability (LNP) [26]. The Application Programming Interface (APIs) to SCPs to incorporate LNP has been exploited by the attackers to gain knowledge of secret subscriber information and mobile user location. A compromised femtocell (a small, low-power cellular base station typically used for small business) and GSM-only phones which downgrade the higher cellular specification (such as 3G and 4G) to 2G, can act as a hot hub for attackers to exploit SS7 vulnerabilities. Value added services such as Unstructured Supplementary Service Data (USSD), SMS, General Packet Radio Service (GPRS) and Session Initiation Protocol (SIP) have given rise to more advanced attacks against the SS7 network elements. The Figure 3.1 diagrammatically summarizes the entry points to the SS7 network through the various network elements mentioned in section 2.5.

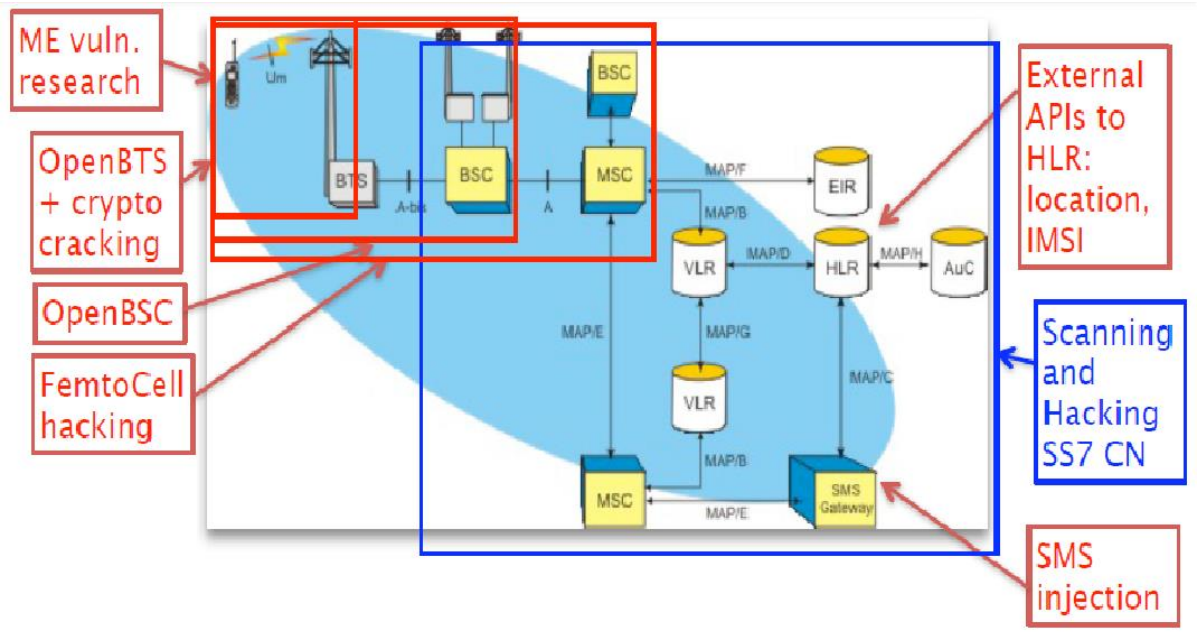



**Figure 3.1: Possible entry points to mobile communication network backend [27].**

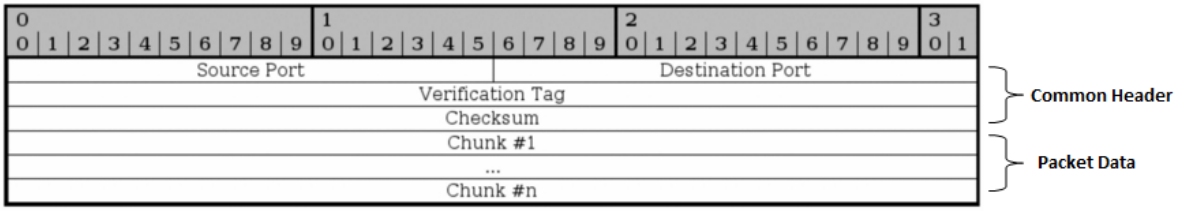
## 3.2 Mapping the SS7 periphery

Attackers extensively use the SIGTRAN protocol [28], an extension to the SS7 family, to exploit the vulnerable entry point (port) and hence map the GSM core network. By this, the attacker not only gains knowledge about the underlying infrastructure but also learns network internal aspects such as Global Title and Point Codes, which he can use for his attacks further.

Being an addendum of SS7 suite, SIGTRAN supports call management and application exemplars of SS7 but over the Internet Protocol (IP) and the transport-layer called Stream Control Transmission Protocol (SCTP) [29]. SIGTRAN facilitates adaptation of Voice over IP (VoIP) networks to the PSTN signaling. An attacker can use SCTP stealth scanning methodologies [27] to explore the vulnerable ports in the SS7 core network.

One of the useful tools to scan SCTP-enabled network elements is SCTPScan [30] which scans machines having major operating systems such as Linux, BSD, MacOS X and Solaris. It allows the attacker to find entry points to the telecom core network infrastructure along with mapping them.

SCTPScan uses the INIT (Initiation) chunk of SCTP packet and listen to the INIT ACK message to learn the live host machines and open ports. Figure 3.2 represents the SCTP message format and the different types of chunks that form the message payload.




(a)

| Chunk Number | Chunk Name |
|---|---|
| 0 | Payload Data (DATA) |
| 1 | Initiation (INIT) |
| 2 | Initiation Acknowledgement (INIT ACK) |
| 3 | Selective Acknowledgement (SACK) |
| 4 | Heartbeat Request (HEARTBEAT) |
| 5 | Heartbeat Acknowledgement (HEARTBEAT ACK) |
| 6 | Abort (ABORT) |
| 7 | Shutdown (SHUTDOWN) |
| 8 | Shutdown Acknowledgement (SHUTDOWN ACK) |
| 9 | Operation Error (ERROR) |
| 10 | State Cookie (COOKIE ECHO) |
| 11 | Cookie Acknowledgement (COOKIE ACK) |
| 12 | Reserved for Explicit Congestion Notification Echo (ECNE) |
| 13 | Reserved for Congestion Window Reduced (CWR) |
| 14 | Shutdown Complete (SHUTDOWN COMPLETE) |
| 15-62 | Reserved for IETF |
| 63 | IETF-defined chunk extensions |
| 64-126 | reserved to IETF |
| 127 | IETF-defined chunk extensions |
| 128-190 | reserved to IETF |
| 191 | IETF-defined chunk extensions |
| 192-254 | reserved to IETF |
| 255 | IETF-defined chunk extensions |

(b)

**Figure 3.2: (a) SCTP Packet format [31] (b) SCTP chunk types.**

The SCTPscan tool does not perform a full 4-way SCTP handshake because, it might establish a real connection to target machine along with slowing down the scan process. Instead it lets the attacker to send repeated INIT messages specific to each port to the network element (server) and waits for a response. If the port is closed, the server responds with the ABORT message. But, if the port is open, the server responds with the INIT ACK message which informs the attacker that the SCTP port is open. The Figure 3.3 below demonstrates the basic SCTP 4-4-way handshake and the stealth scan.

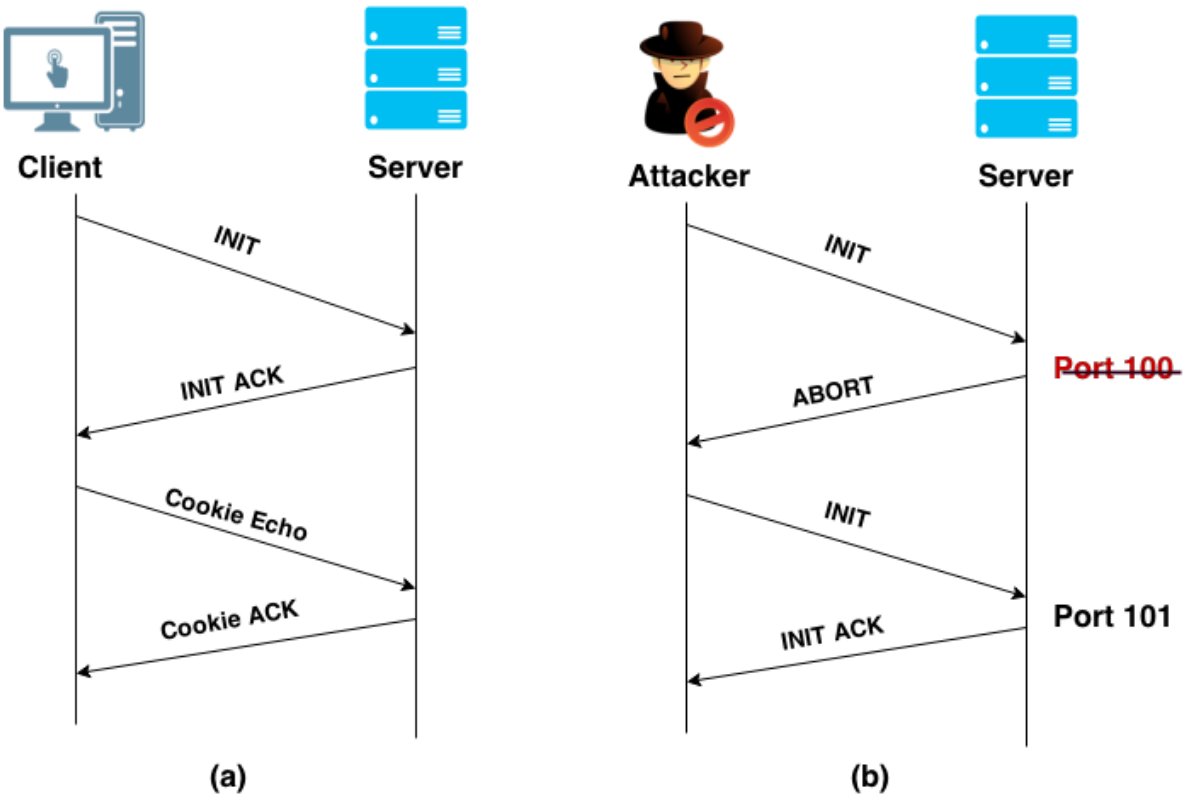



**Figure 3.3: (a) SCTP full 4 way handshake (b) SCTP stelath scan by attacker [27].**

By doing the SCTP scanning, attacker not only gains entry to the SS7 core network (STPs) but also he can perform the following tasks thereafter:

1. He can intercept the traffic routing through STPs and learn Destination Point Codes (DPC) to penetrate deeper into to the network stack.
2. For each DPC learnt, the attacker can perform an SSN scan which allows him to know the applications or services (e.g. call services, SMS services) running on the underlying network elements. Depending on the service that is running the network element, the attacker can classify the network elements into SMSC, HLR, etc.
3. Once the type of the network element is known, the attacker can perform application or service level scan tests (MAP tests, CAP tests, etc.) to further dig into the network stack.

## 3.3 Current status of SS7 vulnerabilities

As mentioned in section 3.1, the vulnerabilities of SS7 telecommunication backbone network would affect the vulnerabilities of the Internet and vice versa. Besides, the attacks of 2G (GSM) SS7 protocol can be extended to higher standards such as 3G and 4G. Enhanced services such as SIP, VoIP and GPRS increase the entry points to the core network and allow malicious hackers to exploit further vulnerabilities of the legacy network backend. Since backward compatibility needs to be maintained within the telecommunication world, a downgrading attack is potentially possible from 4G, 3G to 2G. Figure 3.4 below summaries the number of vulnerabilities found, grouped according to the various network elements.

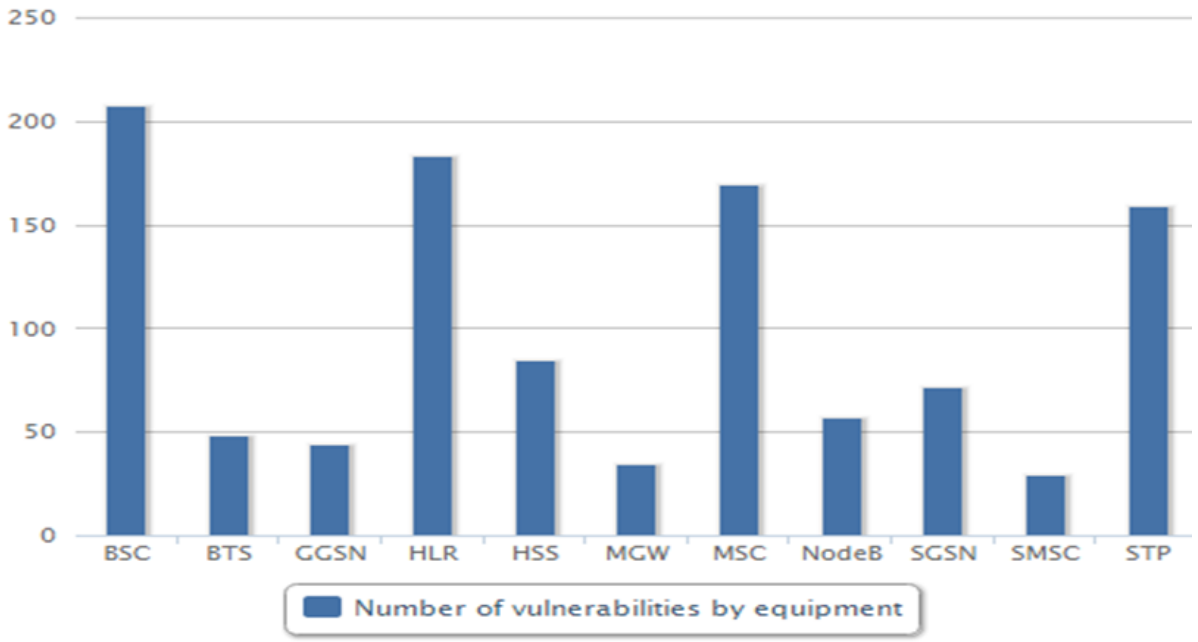



**Figure 3.4: Number of vulnerabilities (on Y-axis) based on different network elements (X-axis) [32].**

Network elements such as BSC and BTS are part of RAN, whereas HSS and Node B are specific to 3G and 4G networks. Though the attacks surveyed in this thesis apply to 3G and 4G elements on a generic level, the focus of this thesis is on the SS7 backbone, with most modern mobile networks are still compatible.

It is clear from Figure 3.4 that the vulnerabilities associated with HLR is exploited on a larger scale mainly because HLR is the central element of the mobile core network hierarchy and

stores a lot of sensitive information. On the other hand MSC is equally exposed as it is the gateway to the core network from the RAN. The high number of attacks on STP infers that the attackers have penetrated the routing mechanism within the telephony backend.

The Figure 3.5 demonstrates the number of vulnerabilities found so far [33] by different underlying protocols of the SS7 stack.

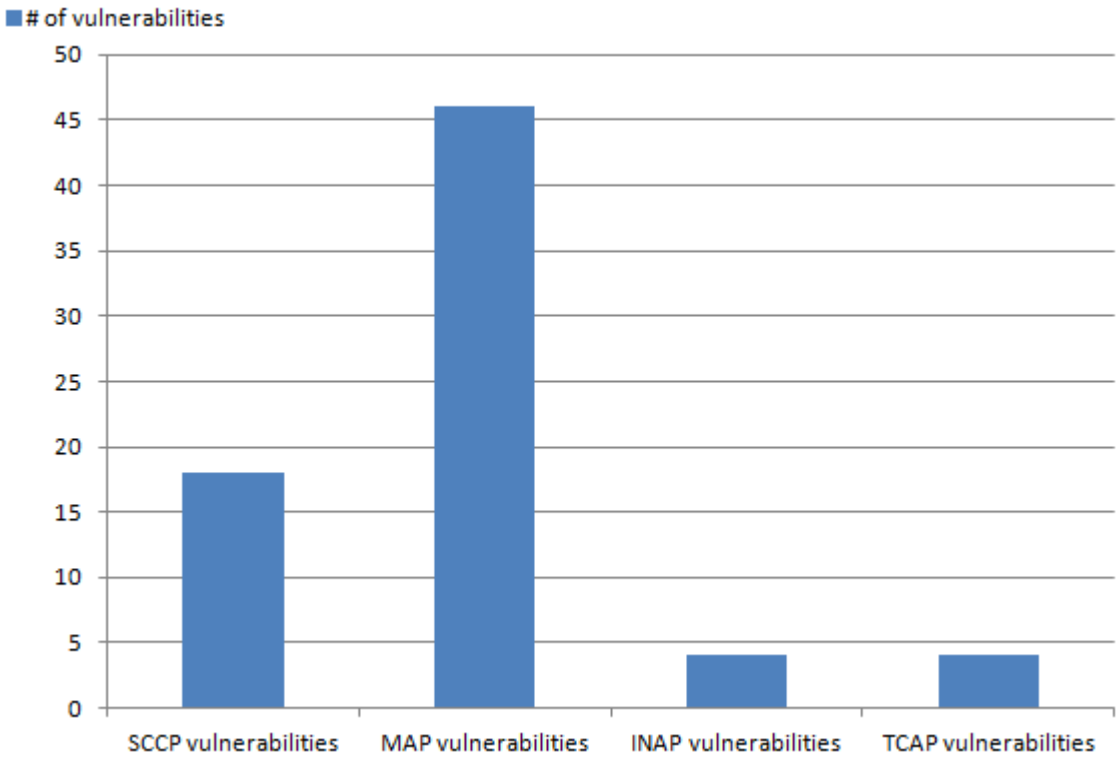



**Figure 3.5: Number of vulnerabilities by internal protocols.**

In comparison with the Diameter protocol [34], the number of vulnerabilities found in SS7 is higher. But this is mainly because of an exposure bias in the sense that the old protocol's (SS7) vulnerabilities are better known than those of the newer protocol deployments. The number of vulnerabilities specific to MAP protocol is explained by the fact that, MAP being an application layer protocol, provides diverse entry points to access core network internal elements such as HLR, VLR, MSC, EIR, SMSC, etc. The high rate of DDoS attacks and other forms of telecommunication network penetration attacks is evident from the higher number of SCCP vulnerabilities as SCCP is responsible for routing, flow control and error correction within SS7 networks.

# 4 ANALYSIS OF ATTACKS

## 4.1 Analysis paradigm

Telecommunication networks support diverse range of services and entities which are connected using various protocol stacks. Attackers take advantage of diversity of such systems to perforate into the system. They use interconnection between protocols (such IP and SCTP) to gain access to the core network entities and go up the protocol stack to unveil different kinds of information (as mentioned in section 3.2). Any device in an IP network is recognized by IP and MAC addresses. Protocols such as TCP, UDP and SCTP offer ports to establish connection within the network hosts. The routing criteria will be based IP addresses. However, in mobile communication systems a diverse profusion of identifiers and addressing schemes (Figure 2.8) are used to identify network hosts, applications or even the subscribers. SS7 networks use combination of PC, GT or SSN for routing purposes. Analysis from an attacker's point of view ('what has to be done to perform a core network attack) is narrated below.

Elements in the core network are connected with each other using SCTP. However, SCTP ports are open to interact with Internet, which actually is the entry point to SS7 stack from IP network. So the attacker who already gained access to the SS7 network can use SCTP sockets to bind to the internal elements using IP stack. Using SCTP client-server applications, the attacker can establish connection with loosely secured network internal elements. One such basic example of client-server connection establishment is presented in Appendix A. While the connection is being established, the attacker can use standard packet monitoring tools such as Wireshark [35] (or tShark) to intercept the traffic. An example of such a traffic intercepted during SMS protocol is also presented in Appendix A. During these interceptions, attacker can learn more information about end points (such as network elements including GT, SSN) which helps him to impersonate as internal network elements and mimic the similar traffic during his attacks.

Whilst intercepting the traffic, attacker can manipulate the message packets with false data using packet manipulation programs such as Scapy [36]. The attacker can use such tools to fake the message packets along with capturing them. These tools are also capable of creating invalid packet data, scanning, probing or trace routing. A sample of Scapy program to send

manipulated SCTP message is given in Appendix B. It gives attacker the privilege to manipulate each fields of network messages of many standard protocols, along with decode the packets, and match requests and replies. It helps him to inject false IMSIs, GTs of MSCs, etc. into normal messages interchanged between network elements.

Though the previous two paragraphs explain how to perform attacks, from security audit point of view, analysis of attacks would be reviewing, structuring and analyzing the feasibility of the attacks. However, from the perspective of security audits, detecting the core network attacks are quite challenging as most of the attacks (frauds) takes place in stealth more. But the impact of such undetected attacks cause frightful financial loss to network vendors. Since telecommunication domain is huge, some of the common mistakes like IP overlaps, misconfiguration of firewalls or any other system configuration has to be audited by vendors. Lack of threat intelligence and mindset of telecommunication engineers are not yet open to adapt aggressive security skillset like that of IP-oriented engineers.

One of the analysis techniques that was adapted by many network providers in cooperation with network operators is by honeypot trapping by setting up a purposeful trap. As a preparation of such analysis, overall data about messages being exchanged within the network has to be gathered. Analyzing such data would be helpful to find trace fingerprints of attackers. Examples of such fingerprints would be same end node trying to use similar false messages (this indicates that the attacker is using a single resource, or stack on same system). Furthermore, error log information would also hint attackers trying to exploit specific protocol or specific network resource. Once such anomalies are detected on purpose they will be fed to the honeypot trap. Being a subdomain of actual working network, the attackers will be trapped without their notice. Now the behavior of such attackers (at this point, it would be some suspicious end nodes) can be studied in detail. Key aspects of such behavior analysis is observing each and every activity of attackers including the resources they are trying to exploit, messages being sent, data which are faked, etc. Based on understanding the purpose of their activities, their requests can be fulfilled or rejected by the honeypot administrator. The interesting fact about most of the standard protocol is usually they are two way communications. So if the attacker can request something using two way protocols, the honeypot administrator or auditor can also request some kind of information to respond to attacker’s messages. The security auditor can also provide response claiming he is responding

to the attacker genuinely, but divert the attack traffic to a trap node. This allows to understand purpose and end-to-end communication of an attacker as each and every information is being monitored in honeypot environments. In case the system cannot respond (fulfil the attackers need), from the analysis the attacking nodes can be blacklisted.

Based on auditing core network attacks on protected test environments, detailed workflow of attacks with relevant 3GPP specifications and references specific to exploited signaling features are articulated in this chapter in a uniform way.

## 4.2 Location privacy breach

With growing number of mobile phone users, number of services that the mobile user demands is increasing. There exists many location based services in which user allows the application vendors to learn about their location. However, the insufficiently protected nodes in mobile communication networks would also disclose the location without user's consent.

Mobile phones have become a major part of our daily lives and hence a vital component of our communication and commutation. Since we carry our mobile phones almost everywhere and any time [37], the location information that can be learnt poses as one of the biggest privacy threats. Government agencies, hackers and advertisement companies spying on mobile end users without their knowledge or the awareness and consent of network operators are a serious issue in context of personal privacy. In this chapter we discuss the known weaknesses in mobile communication backend networks that would disclose location of a user and also outline the common mitigation approaches.

In spite the advancement in mobile communication technology and the security of the air interface, there are very few measures taken to protect location privacy of the users from illegitimate access using the interworking network (i.e. SS7 / SIGTRAN). Location and International Mobile Subscriber Identity (IMSI) are co-related and they are protected from outer world as far as technically feasible. Using IMSI catchers the active attackers can collect IMSIs on Radio Access Network (RAN) or air interface. Besides, home network operator can fully track the user location whereas the visited network operator can partially track user location.

### 4.2.1 Regular Location Disclosure scenarios

Network that the user has currently logged into would know the geo- location of the cell tower and this location information provides an approximate location of user to an attacker. Otherwise, this information is revealed to outer world in two cases as below:

1. "Locate my phone" services –Most often scenario of this use case is when the phone is lost, network operators would provide this information with consent of phone owner.
2. "Law enforcement" – In case of emergencies or when the user has to be tracked down for legal purposes.

As part of law enforcement for Location Services (LCS), "Phase II E911 rules re-quire wireless service providers to provide more precise location information to PSAPs; specifically, the latitude and longitude of the caller. This information must be accurate to within 50 to 300 meters depending upon the type of location technology used." Though it is used for emergency purposes, it mandates the network operators to provide accurate position of the mobile. Unlike the normal location updates during calls or SMS, more precise location information is obtained using Radio Resource LCS Protocol (RRLP) [38] with the help of Gateway Mobile Location Centre (GMLC).

### 4.2.2 Overview of Location Proximity

To serve cellular services to appropriate mobile users, mobile networks have a specific geographic hierarchical structure. Such a structure for GSM consists of cell, Location Area, MSC service area, Public Land Mobile Network (PLMN) service area and GSM Service area [39]. A pictorial representation of these geographic hierarchical structures is shown in Figure 4.1:

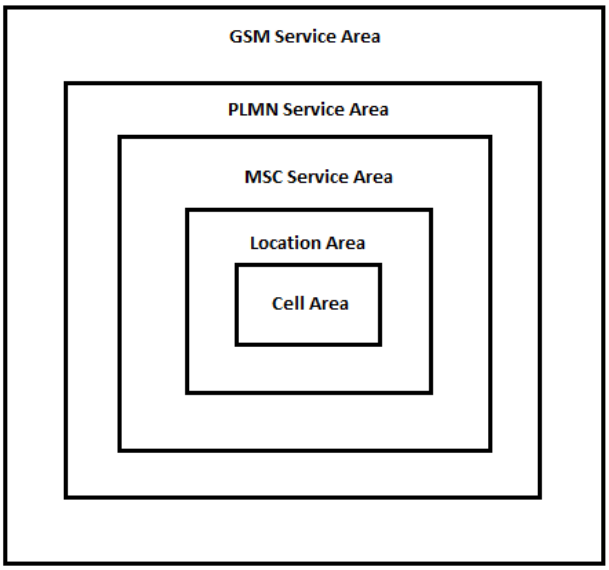



**Figure 4.1: GSM geographic hierarchy structure.**

Cell being the smallest area of GSM location hierarchy, it ranges from 100 meters to 35 Kilometers (which is the radio coverage of a transmitter). Each cell is identified by Cell Global Identity and it is used for positioning. CGI is mapped to geographic co-ordinates by the operators using a pre-defined cell ID database.

Multiples of such cells constitute a Location Area (LA). Every time a mobile user moves to a new LA, it will be updated in the VLR database. An MSC Service Area comprises of many such location areas that the MSC can serve. HLR stores the in-formation about MSC that serves a particular mobile station. MSCs are recognized by Global Title (GT). The whole area a mobile operator covers is identified as PLMN service area and each such area will have many MSCs serving that particular operator network. Overall area with GSM connectivity is considered as GSM Service area. Every network providers have similar structure and this logical mapping can often cross each other.

### 4.2.3 Location disclosure using call setup messages

As part of mobility management, the network operators have to keep track of the MS locations, while it is moving. The location information is often tracked using International Mobile Subscriber Identity (IMSI) which is attached to the network using *IMSI Attach* GSM procedure when a mobile phone is switched on. This is required by the MSC and VLR to keep the MS registered in the network for location updates. Once the mobile is turned on and ready to make

or receive messages/calls (the “idle” state), every time it moves to a new VLR/MSC area the location has to be updated in GSM system. The general network message flow [14] in those cases is as follows:

1. When user places a call using phone number/ MSISDN of another user, an ISUP IAM (Initial Address Message) message which contains the MSISDN is generated. Based on the information contained in MSISDN, the call will be routed in the mobile network through GMSC.
2. GMSC identifies the HLR location based on MSISDN and to locate the called MS, it dispatches the MAP Send Routing Information (*MAP SRI*) towards the HLR.
3. HLR queries the VLR using MAP Provide Roaming Number message (*MAP PRN*) to get Mobile Station Roaming Number (MSRN).
4. VLR responds to HLR with *MAP PRN ack* message which contains the MSRN, a temporary number assigned by the VLR which in turn contains the IMSI.
5. HLR passes the MSRN back to GSMC with MAP Routing Information Acknowledge message. Now the Now the GSMC knows MSC and hence the location of the MS which is served by it. GSMC generates the IAM with MSRN of the called user. Since MSC can map MSRN to IMSI, on arrival of IAM message, it establishes the call connection.

#### 4.2.3.1 Attack using call setup messages

This attack using the normal working message flow of the call set up messages to know the approximate location of the user (or MS). Successful completion of this attack as per [6] would reveal the IMSI (which is supposed to be a secret), global title of the MSC (which identifies the MSC uniquely in the global network and its geo-location) and error messages if the phone is turned off. The Figure 4.2 describes the attack in context.

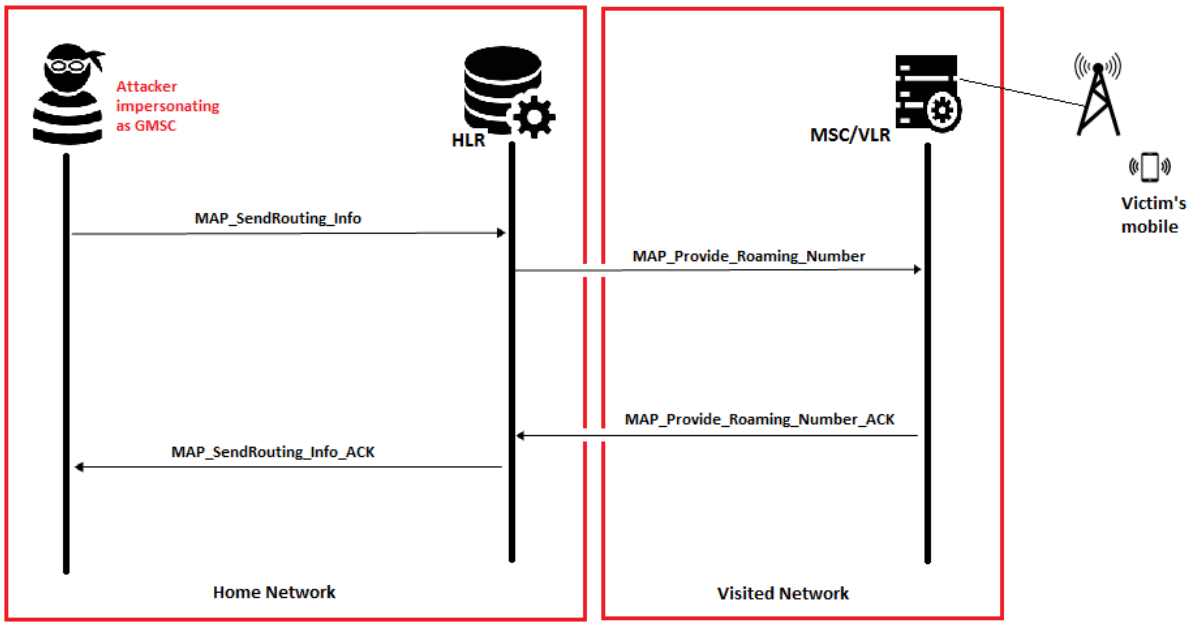



**Figure 4.2: Location disclosure using call setup messages.**

Here the attacker initiates the call set up IAM messages impersonating as GMSC. The attack message flow is as follows:

1. Attacker with SS7 access impersonates as GMSC and initiates the call set up IAM message.
2. He sends *MAP SRI* message enclosing the MSISDN (phone number) to the HLR. Since there is no authentication check made, HLR thinks someone is trying to call to the provided MSISDN and processes the message.
3. HLR sends *MAP Provide Roaming Number* to the corresponding VLR to get the MSRN.
4. The VLR responds with *MAP Provide Roaming Number ACK* containing the MSRN, which in turn contains the IMSI and Global Title (GT) of the MSC/VLR which is serving the MS enquired by the attacker.
5. On arrival of *MAP Provide Roaming Number ACK* message, HLR will remit this information to the attacker impersonating as GMSC with MAP_SRI_ACK message.
6. Attacker would not proceed to initiate the call set up as he has gained the information about user's IMSI and MSC location.

Numbering the MSCs with GT is purely operator specific, though it would reveal the location of mobile user. GT reveals the country (country code field of GT), area (area code) and possibly the network (if mobile networks in a country can be identified by area code). The location details can be further narrowed down by mapping MSC and its approximate geological location, by querying a large set of phone numbers with known location to the network. Since the number of phones that an MSC can serve is limited, the number of MSCs is more in a largely populated area compared to a single MSC serving a larger area in villages. So if the victim is in the city area, there are high chances that the attacker can know his exact location.

### 4.2.4 Location disclosure using SMS protocol messages

Short Message Service (SMS) is transmission of messages up to 140 bytes between mobile stations in a sore and forward mechanism. End to end SMS procedure comprises of two parts – first where the SMS is submitted to Short Message Service Center (SMSC) by the sender; second is the delivery of that message to the recipient from SMSC. Such short messages use signaling channels to accommodate simultaneous voice service over the mobile network [40]. Mobile stations transmit SMS over air interface to the Base Transceiver Station (BTS) and from which it enters the SS7 core network routing over MSC/VLR, SMSC and HLR towards the destination.

Basic message workflow in SMS protocol as per [41] is as follows:

1. Message submission by the sender (Mobile Originating part)
    - The address of SMSC is usually stored in the SIM card.
    - When the sender sends a Short Message (SM), the message along with SMSC address will be transmitted to the MSC.
    - Based on the SMSC address specified, MSC imparts Mobile Originated ForwardSM (*MO ForwardSM*) message to the SMSC.
    - If the SM is successfully delivered (stored in SMSC), it is acknowledged by SMS submit report message i.e. *MO ForwardSM ACK*.
2. Message delivery by SMSC to the destination ( Mobile terminating part)
    - To deliver SM to the destination, SMSC has to know the MSC location and IMSI of the recipient which is stored in the HLR.

– SMSC sends *MAP Send Routing Info For SM* message to the HLR to query the MSC GT/location and IMSI of the recipient.

– HLR encapsulates IMSI and MSC location in *MAP Send Routing Info For SM ACK* message and sends it back to the SMSC. Based on this information, SMSC routes the SM to the recipient MSC which in turns delivers it to the mobile user.

#### 4.2.4.1 Attack using SMS protocol messages

Here the attacker impersonates as SMSC and sends messages to know the MSC GT and IMSI of the victim. The Figure 4.3 describes the attack [6] message flow.

Here the attacker performs following tasks:

1. Attacker impersonates as SMSC and sends *MAP Send Routing Info For SM* message to the HLR by enclosing the MSISDN (phone number) of victim.
2. The HLR thinks that the SMSC needs to send an SM to the provided MSISDN, and replies back with *MAP Send Routing Info For SM ACK* message which contains IMSI of the victim along with GT of the MSC that is serving the victim at that point.

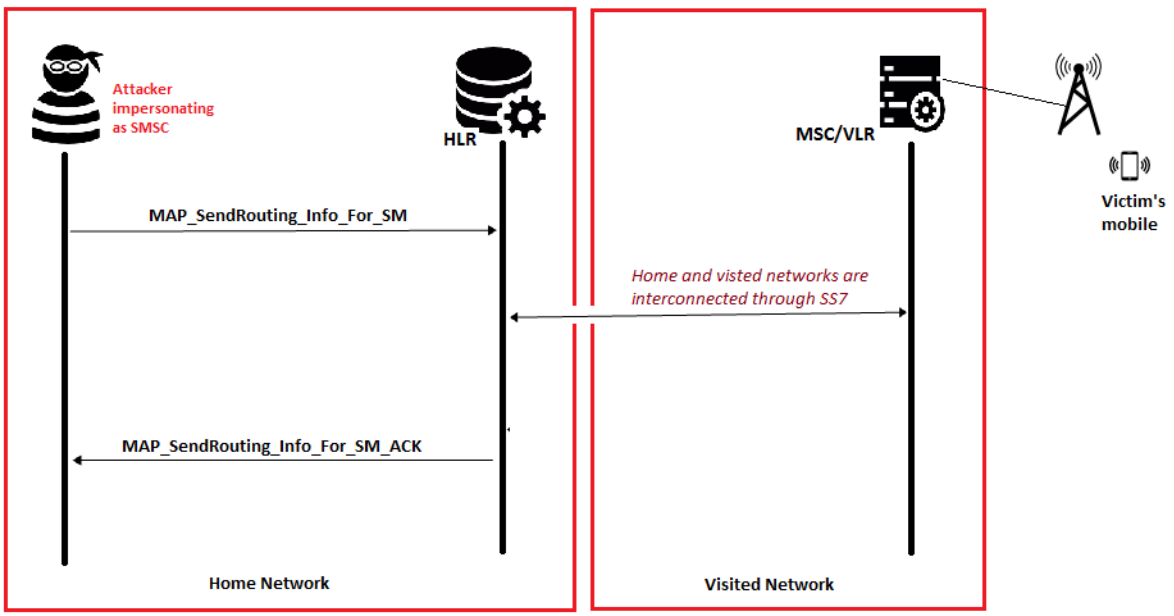



**Figure 4.3: Location disclosure using SMS protocol messages.**

Though MSC GT reveals the approximate location area of the victim, as explained earlier cell level geo-location mapping can be done with predefined set of MSC-Geolocation pairs.

### 4.2.5 Location disclosure using CAMEL Location Management Function Messages

Customized Applications for Mobile Networks Enhanced Logic (CAMEL) [42] is an overlay on MAP logical layer. As part of location management function, the net-work providers can send Any Time Interrogate (ATI) messages to the HLR from CAMEL platforms to obtain the cell ID or location of the user along with which it can provide the subscriber information such as billing data and International Mobile Station Equipment Identity (IMEI). The location information provided here is the last known location of the mobile user. Basic message flow of location management functions is described [43] as below:

1. GSM Service control Function (gsmSCF) element will initiate the *anyTimeInterrogation Request* message by encapsulating the MSISDN and transmitting to the HLR of home network.
2. Based on the provided MSISDN, the HLR will transmit the *Provide SubscriberInfo* message to the MSC/VLR.
3. MSC sends a Paging Request message to the mobile station to look up its current state. If the mobile user is on call, then the age field is set to 0, as the MSC always knows the location. If the mobile user is not on call (which means age field is not 0), MSC would at least know the last location to where it served the MS. The Paging Response message will have cell ID and age information.
4. On arrival of Paging Response, MSC responds to the HLR by sending *Provide SubscriberInfo Response* message which contains the cell ID, IMSI and/or IMEI of the requested MSISDN.
5. HLR will now send the *anyTimeInterrogation response* back to the gsmSCF with the subscriber information from previous step.

#### 4.2.5.1 Attack using anyTimeInterogation messages

Here the attacker with SS7 access will impersonate as gsmSCF and sends the *any-TimeInterrogation* Request message with the MSISDN of victim to HLR. The message flow of this attack [44] is as shown in the Figure 4.4.

1. Attacker impersonates as gsmSCF and sends *anyTimeInterrogation request* message along with the MSISDN of the victim to HLR.
2. HLR treats this as a legitimate message from gsmSCF and initiates the Provide SubscriberInfo request to the MSC/VLR.
3. VLR initiates the Paging request to the MS and in return as part of Paging Response message receives the IMSI and location of the MS.
4. MSC then sends the information from previous step along with MSC GT to the HLR via *Provide SubscriberInfo* Response.
5. HLR forwards this information to the attacker via *anyTimeInterrogation response* message.

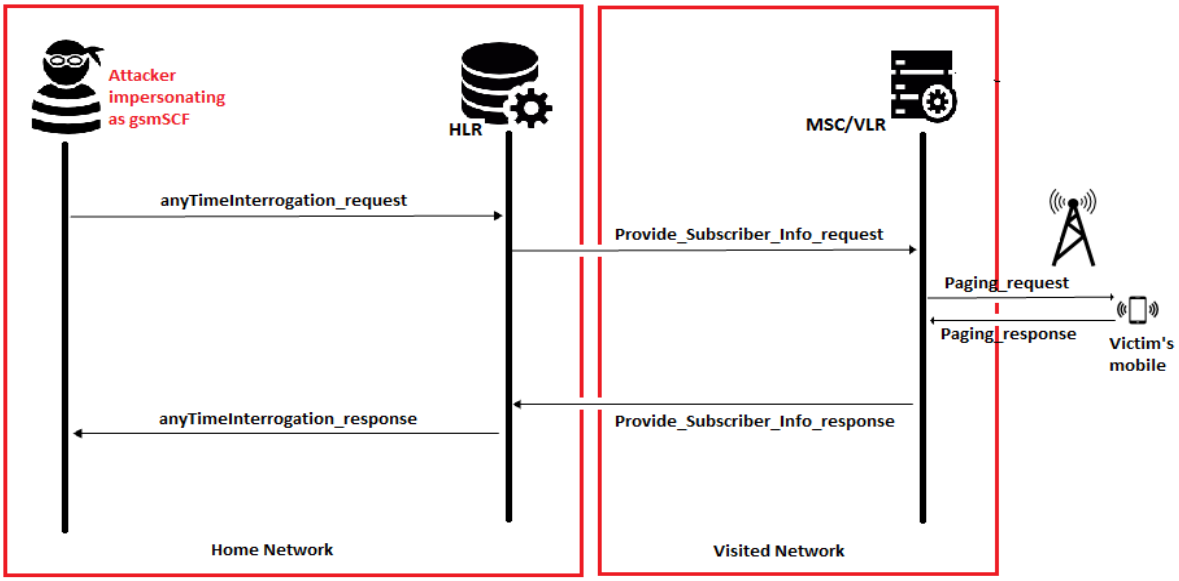



**Figure 4.4: Location disclosure using *anytimeInterrogation* messages.**

Attacker now knows the approximate cell of the victim along with IMSI, GT of the serving MSC and possibly the IMEI number. Here the attacker would know victim's location more accurately as he can gain knowledge about the cell rather than just MSC as in the previously described attacks.

#### 4.2.5.2 Hybrid Attack using SMS and CAMEL messages

Though *anyTimeInterrogation* is part of some of the location finder application services [39], many network operators block (filter) it for security purposes and hence attacker might not get *anyTimeInterrogation request* message in return always. However, we can bypass that using a hybrid attack [44] by directly querying the MSC/VLR. The Figure 4.5 describes such hybrid attacks of circumventing *anyTimeInterrogation* filters imposed by network operators.

Attacker can send Provide Subscriber Info request to the MSC/VLR by impersonating as HLR. However this will be treated by MSC/VLR only if the IMSI is provided by the HLR. Since we assume that the attacker just knows the MSISDN or phone number of the victim, the attacker should get the IMSI first.

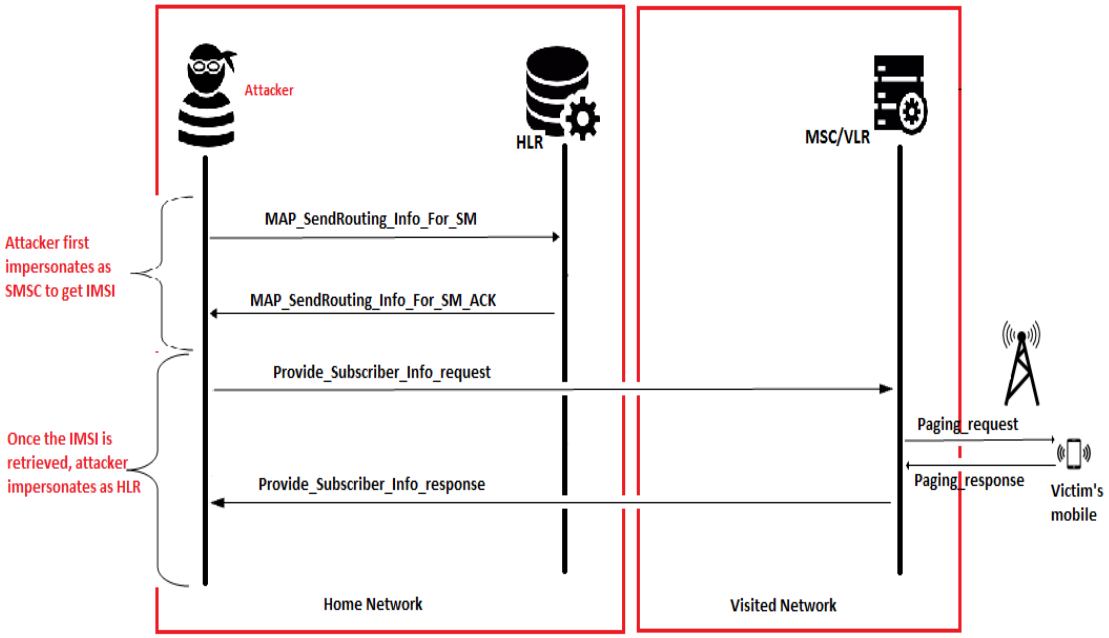



**Figure 4.5: Location disclosure hybrid attack.**

1. Here the attacker performs previously described SMS message attack to know the MSC GT and IMSI. He impersonates as SMSC and sends *MAP Send Routing info ForSM* to HLR by encapsulating MSISDN of victim.
2. HLR in return responds to the attacker with IMSI and GT of MSC in *Send Routing Info ForSM acknowledgement* message.

3. Now since attacker has IMSI of the victim and he knows which MSC to query for cell level location information, he impersonates as HLR and sends *Provide Subscriber Info request* message to MSC/VLR.
4. MSC/VLR will initiate the Paging request to know cell level location details of MS. The MS responds with Paging Response. Through *Pro-vide Subscriber Info response* message, it would reveal the cell information to attacker.

Unlike previous attacks, here the attacker has more chances and accuracy of knowing the victim's location as cell level information provides better location proximity than the location details that a MSC GT can reveal.

### 4.2.6 Location disclosure using emergency location service (LCS) messages

To serve the people in case of emergency situations governmental bodies have mandated [45] three digit emergency numbers such as 911 (in United States of America) and 112 (in Europe). This feature is implemented as per location service guidelines [38]. Dialing 911 or 112 would place a free of charge call on behalf of mobile users and accurate location information is collected to serve the people in emergency quickly. Often the accurate location is calculated either based on Global Positioning System (GPS) technology or based on triangulation between cellular towers by considering angle of arrival and time difference of arrival factors of radio signals. This can either be used from mobile station side (emergency calls) or from the network side (to track criminals, etc.). The attack being discussed here is more related to network side location services. The basic message flow of LCS [45] is as below:

1. An authorized client (e.g. police) can initiate a location service request from a Serving Mobile Location Center (SMLC) client. SMLC is a functional element of Base Station Controller (BSC) used for location detection of mobile phones in GSM networks. The request includes MSISDN.
2. This request is directed to Gateway Mobile Location Centre (GMLC). GMLC bridges external SMLC clients with core network and hence it authenticates the LCS service requests to filter out only legitimate clients. The GMLC can also request HLR for routing information. SMLC and GMLC functions can be parts of a same network entity.

3. GMLC sends *Provide Subscriber Location Request* message to MSC/VLR of visited network (VMSC). Though there is no authentication check for this message, address of the sender will be verified. The MSISDN will be mapped to IMSI and hence this message includes IMSI instead of MSISDN.
4. VMSC (MSC/VLR of visited network) sends location request to the BSC which in turn uses *RRLP requests* to know the exact cell ID location of the mobile.
5. The location report received by VMSC includes the exact location of MS. It is encapsulated in *Provide Subscriber Location ACK* message and sent to GMLC.
6. GMLC then encloses this information in location service response and sends it back to SMLC client.

Here the LCS service response will have accurate location of MS including longitude and latitude. Hence there is no need to separately map the cell ID to respective geo-location coordinates.

#### 4.2.6.1 Attacks using location service (LCS) messages

In this attack [44], attacker bypasses the verification check done by GMLC by impersonating himself as GMLC to VMSC. Since it requires IMSI corresponding to victim's MSISDN, the attacker initially impersonates as SMSC to HLR and retrieves the IMSI as discussed in section 3.2.1. The message flow for this attack is represented in the Figure 4.6.

Communication exchanged during location disclosure attack using LCS messages is described below:

1. Here the attacker performs previously described SMS message attack to know the MSC GT and IMSI. He impersonates as SMSC and sends *MAP Send Routing INFO FOR SM* to HLR by encapsulating MSISDN of victim.
2. HLR in return responds to the attacker with IMSI and GT of MSC in *Send Routing INFO FOR SM* acknowledgement message.
3. Now since attacker has IMSI of the victim and he queries visited network MSC for accurate location information. He impersonates as GMLC and sends *Provide Subscriber Location req* message to MSC/VLR.

4. MSC/VLR will initiate the RRLP request to know precise location details of MS. The MS responds with RRLP Response. Through Provide Subscriber Location Response message, it would reveal the location of victim to attacker.

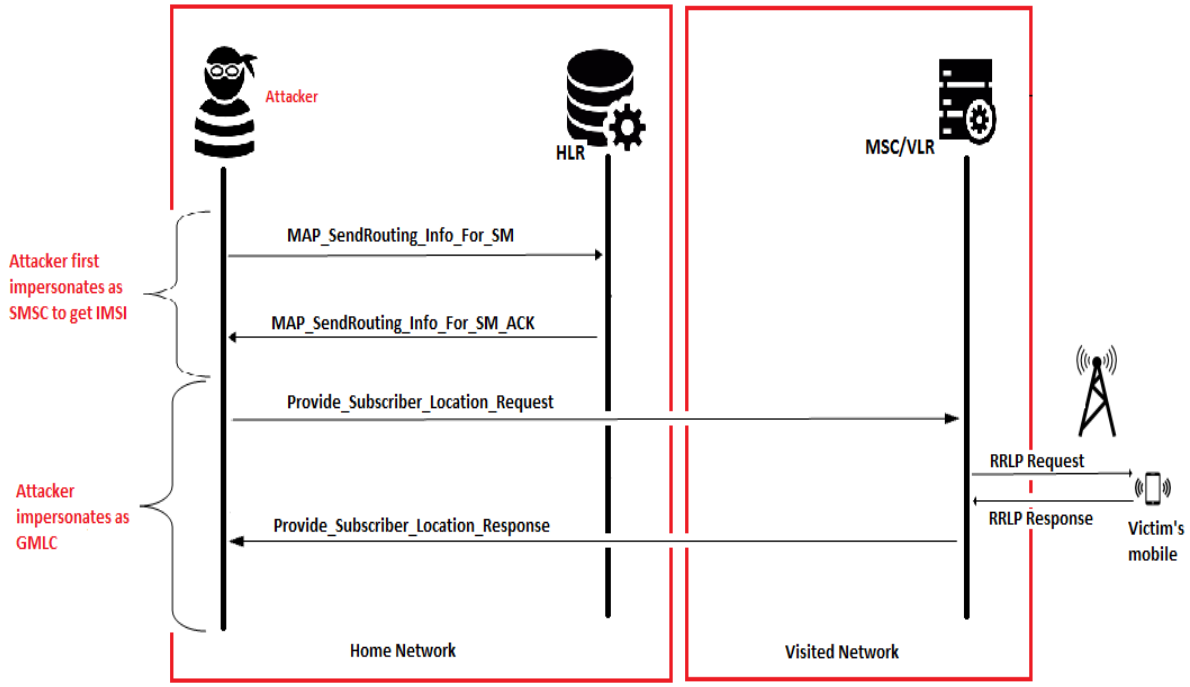



**Figure 4.6: Location disclosure using LCS messages.**

To summarize, the attacks discussed in the sections 4.2.1 to 4.6.1 articulates how an attacker with SS7 access can retrieve IMSI and MSC GT just using MSISDN (phone number). The global location of MSCs can be narrowed down to more accurate locations either by predefined scripts or by querying in public databases such as SHODAN [46] – a computer/network device search engine. The attacks shown in 4.2.5.1 and 4.2.6.1 provide more accurate details of the victim by providing cell ID of the victim MS. Once the cell ID is known, the attacker can use third party APIs [47] to get latitude and longitude of victim's location and also plot them on a map. Some of the examples pertaining to sample trace of a located cell ID and scripts that use the aforementioned APIs are given in Appendix C.

## 4.3 Call interception and eavesdropping attacks

In this section, we discuss how an attacker can intercept a phone call using loopholes in SS7 protocol.

### 4.3.1 Basic call setup workflow during roaming

As part of mobility management services, international roaming facilities are provided using CAMEL [42] specifications. More specifically, mobile operators facilitate international roaming within their network using CAMEL Application Part (CAP). This enables the operators to provide home network services to visiting subscribers.

Assuming that a Finnish subscriber is roaming in Estonia and trying to call a Finnish number, a basic call setup workflow during roaming is pictorially represented in Figure 4.7.

1. When the MS is roaming in a new location (different country), it intimates its whereabouts (MSC area and GT) to HLR of home network (home country). To serve the roaming MS with home network services, the HLR notifies the MSC of visited network using *insertSubscriberData Request* message. This message contains global address of gsmSCF from home network and the list of events that has to be reported to gsmSCF. Example of the events that has to be reported is calls to home network number while roaming.
2. When the roaming MS wants to make a phone call to a Finnish number, it places the call using IAM call setup message toward MSC of visited network. It places the call using Finnish national phone number format (e.g.: 046641….).
3. Since this event has to be reported to gsmSCF as per roaming agreements, the visited MSC initiates the CAP *Initial IDP* message to gsmSCF of home network.
4. Now the gsmSCF converts the Finnish national phone number format to international format as per E.164 specifications [48]. It encapsulates the international phone number format (e.g. +358 46641…..) in *CAP Connect* message and send it across to the visited MSC.
5. Depending on the international phone number format, the visited MSC re-initiates the ISUP IAM call set up message to contact the MSC of called party (in home network) and the call is established.

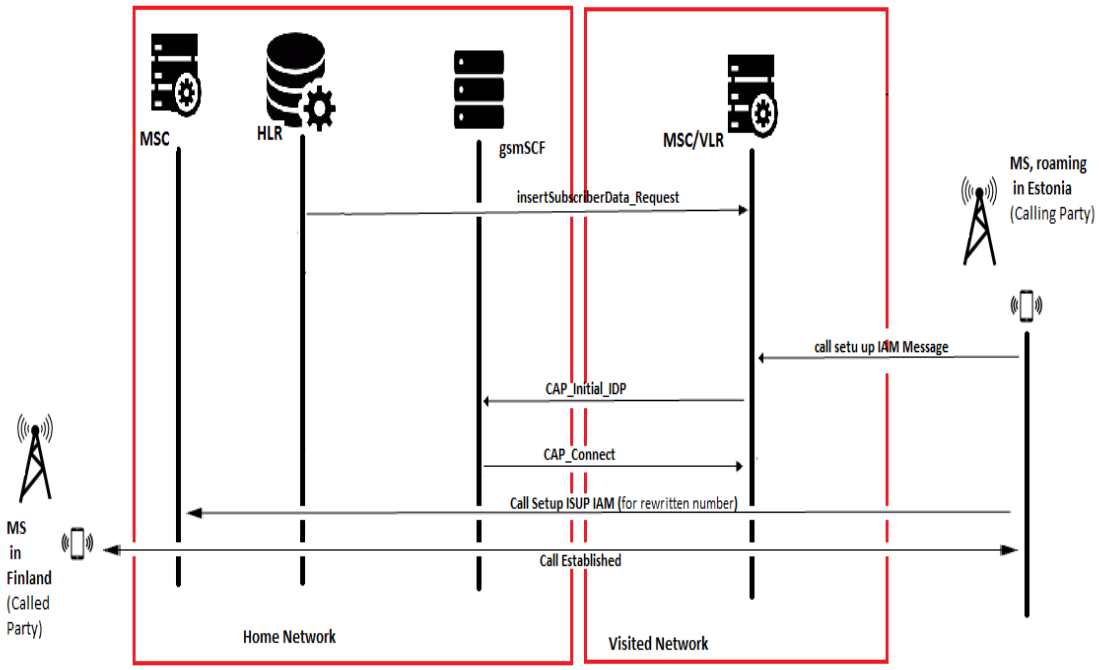
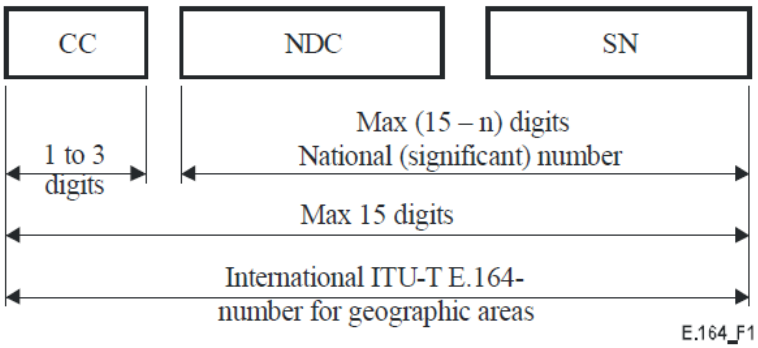



**Figure 4.7: Basic call setup workflow during roaming.**

Various fields of the international phone number format is shown in Figure 4.8:




CC Country Code for geographic area
NDC National Destination Code
SN Subscriber Number
n Number of digits in the country code

NOTE – National and international prefixes are not part of the international ITU-T E.164-number for geographic areas.

**Figure 4.8: International ITU-T E.164 international phone number format [48].**

### 4.3.1.1 Call interception using CAMEL messages

Here the attacker with SS7 access successfully intercepts the calls made by a roaming mobile user by exploiting the loopholes in CAMEL protocol. As a prerequisite for this attack, initially

the attack redeems MSC GT of calling MS using the exploits shown in section 3.2.1. Based on the dialed MSISDN by victim, the attacker also retrieves MSC GT of 'called MS'. Since there are no plausibility checks made by visited MSC while accepting *insertSubscriberData Request*, the attacker impersonates as home network HLR and injects address of fake gsmSCF. This enables the attacker to gain complete control over victim's (calling party) call from roaming net-work. Workflow of call tapping attack [44] is demonstrated in the Figure 4.9:

1. Initially the attacker tracks the location of victim's MS using the location privacy breach attack described in section 4.1.4.1. This allows him to learn the MSC GT and IMSI of calling victim from roaming network.
2. Then the attacker impersonates as HLR from home network and using *insert Subscriber info Request* message, he injects the address of fake gsmSCF to MSC along with list of events to report.
3. When the roaming MS in Estonia wants to place a call to a Finnish phone number (in Finnish phone number format), it contacts the MSC of its visited network using IAM call setup message.
4. Since calling event has to be reported to gsmSCF as per roaming agreements, the MSC contacts the fake gsmSCF address which is injected by the attacker. The MSC sends *CAP initial IDP* message to fake gsmSCF instead of the subscriber's gsmSCF.
5. Once the *CAP initial IDP* message is received, attacker rewrites the MSISDN number to number of his recording proxy (e.g. +358 46541…), instead of provided the international calling number of 'called party' in E.164 format and sends it back to the MSC using *CAP_Connect* message. A recording proxy can be build using open source frameworks such as Astrerisk IP PBX [49], which not only helps to record the telephonic conversation, but also route them to any other destination over IP network.
6. Now, instead of actual called party number (+358 46641 …), the MSC initiates *call setup IAM* messages for attacker's recording proxy (+358 46541…). Attacker bridges the call to original called party number (+358 46641….).
7. Though both parties can talk to each other, since the call is routed through recording proxy, the attack observes/records the conversation.

This attack works fine until the roaming MS uses the malicious MSC or till the HLR resets address of original gsmSFC. However this attack can be carried out only if the international network provider is same for both calling and called parties.

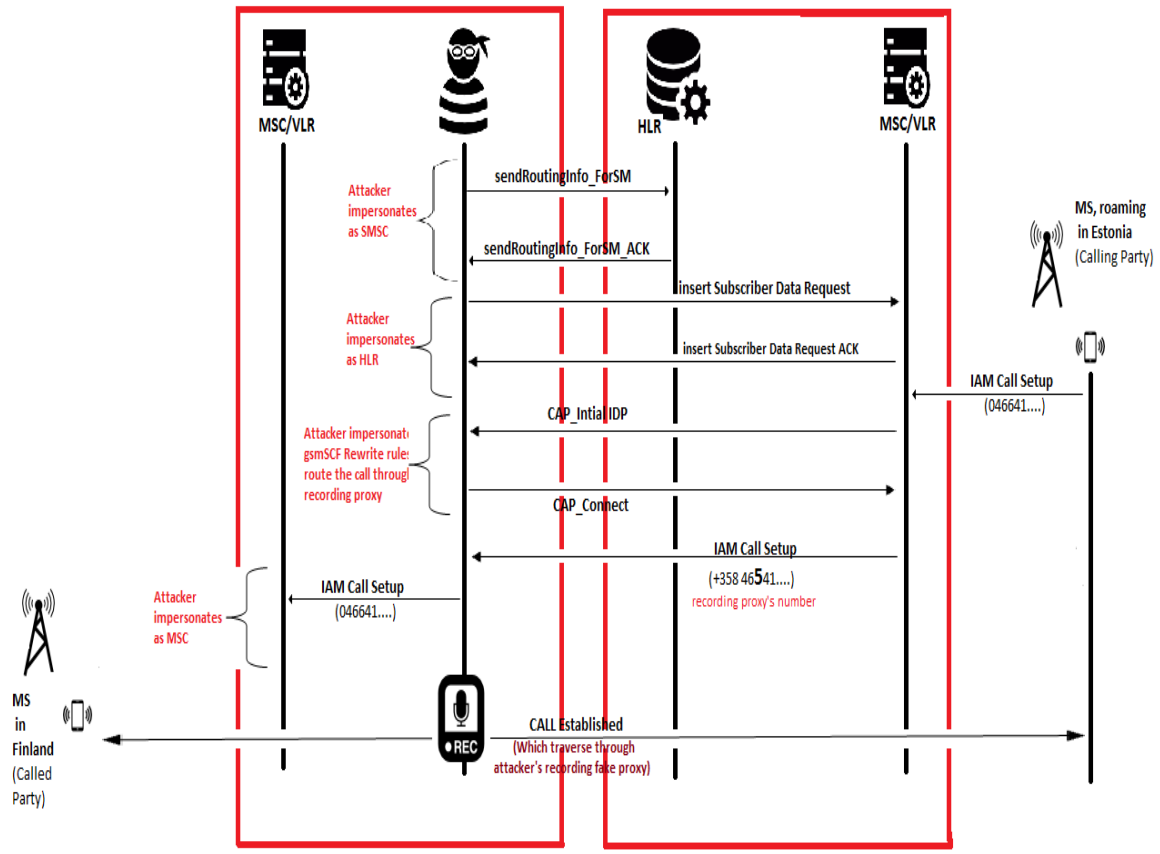



**Figure 4.9: Call interception using CAMEL messages.**

## 4.3.2 Call interception using subscriber profile manipulation

To receive continuous cellular services, the MS has to updates its location when it moves from one location to other. While updating the location, MSC sends its GT along with IMSI (collected from MS) Update Location message to HLR. It turn, the HLR provides the information needed by MSC to provide cellular services to the MS in context. The information sent by HLR mainly includes the subscription profile which allows network operators to charge for the services they provide. For the sake of simplicity gsmSCF and gsmSSF are mentioned

with a generic term “billing platform” in this attack. Basic message flow when an MS updates its location (in presence of a billing platform) is as follows:

1. When a new MS enters a new MSC/VLR area, the MS registers to the VLR through IMSI ATTACH procedures [50].
2. The serving MSC/VLR sends the collected IMSI and its own GT to HLR using Up-date Location message.
3. HLR responds back to MSC/VLR with insert Subscriber Data message which contains the subscriber’s billing profile. Typically, the subscriber pro-file includes allowed and prohibited services; call forwarding settings; billing platform address. Another scenario where HLR sends insert subscriber data is when the subscriber changes his billing plans.
4. MSC saves the subscriber profile in its database and confirms it to the HLR using insert subscriber data acknowledgement message.
5. Hereafter, every time a call or SMS is initiated, it will be routed to billing platform to enable network operators to charge the MS subscriber for their service.

#### 4.3.2.1 Call tapping attack using subscriber profile manipulation

In this attack [8], an attacker can eaves drop over victim’s outgoing calls by injecting a fake billing platform address in the MSC/VLR. The attacker routes the call from victim to its actual destination and meanwhile records or eavesdropping the call conversations. Since the loophole in billing mechanism is used, this attack works only when the victim is placing an outgoing call. Unlike the attack demonstrated in 4.2.1.1, the incoming calls cannot be eavesdropped. The Figure 4.10 demonstrates the attack in context.

1. As part of preparation phase, the attacker tracks the location of victim’s MS using the location privacy breach attack described in section 4.1.4.1. This allows him to learn the MSC GT and IMSI of victim.
2. Now the attacker impersonates as MSC/VLR and sends update location message to HLR by providing victim’s IMSI.
3. HLR considers this to be a legitimate message thinking that the MS have moved to a new location. In return HLR sends *insert subscriber data* message (contains sub-

scriber's profile including billing platform details) to the attacker who is impersonating as MSC/VLR.

4. Once the billing platform address is fetched, the attacker sends another *Location Update* message to same HLR but with GT of actual MSC. By doing this task, the attacker allows the original MSC to handle the calls made by victim.
5. Now the attacker impersonates as HLR and sends *insert Subscriber data* message to original MSC but with a fake billing platform address. This is to manipulate victim's subscriber profile.
6. Since there is no plausibility check made by MSC on *insert Subscriber data* message, the MSC thinks that the victim has updated his subscription plans and hence accepts by sending insert *subscriber data acknowledgement* message to HLR.
7. When the victim wants to make a call, it contacts the MSC serving it using MSISDN of destination MS. Now the MSC sends *Initial IDP* message to billing platform address provided by the attacker. This in real case enables the billing platform (gsmSCF) to start charging for the outgoing call.
8. The attacker who is impersonating as billing platform, using *CAP Apply Charging Report* to MSC by encapsulating a call rerouting address as per [51]. This helps the attacker to impersonate as a fake MSC and route victim's call to its original destination through SS7 network.
9. Original MSC routes the *IAM call set up* message to attacker's fake MSC address after confirming that the billing has begun.
10. Attacker who is impersonating as MSC would now bridge the call from victim's MSC to original destination by initialization another *IAM call set up* message.

Since the call is being routed to its original destination, the victim can converse over the call with MS of destination. However, the attacker who is actually in the middle can record or eavesdrop the call without caller and receiver's knowledge using the recording proxies.

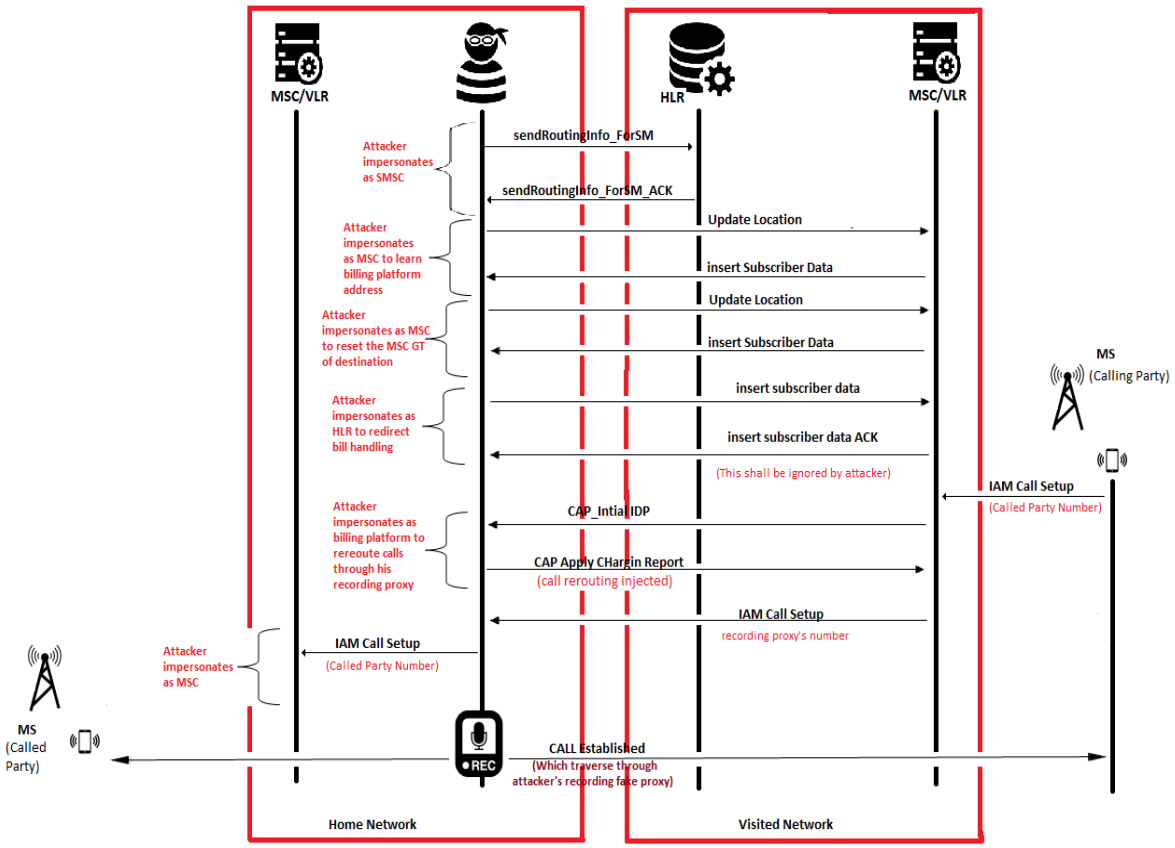



**Figure 4.10: Call interception using subscriber profile manipulation.**

### 4.3.3 GSM/UMTS authentication mechanism

Though it is not a complete attack using SS7 backbone network, some part of the attack utilizes the loopholes of pseudonymity mechanism from core network. However, message exchange over RAN networks is omitted as it is out of scope for the thesis text. According to GSM/UMTS specification [52], "an intruder cannot deduce whether different services are delivered to the same user". Since IMSI is considered to be a decisive secret, a temporary identity (TMSI) is user as a pseudonym to obfuscate IMSI. TMSI is used for encrypting over the air traffic for voice calls. However, a new TMSI should be assigned at each change of location.

The GSM security model relies on a shared secret between HLR and subscriber's SIM. The security mechanism contains following elements:

- A 128-bit key shared secret- *Ki*
- A 32-bit Signed Response- *SRES* (obtained using *ki*)
- A Random challenge - *RAND* (challenge is thrown by MSC)

– A 64-bit session key- *Kc* (for encrypting the communication over RAN)

When a mobile is switched on, it reports to the network. HLR sends one or more authentication triplets <*RAND, SRES, Kc*> to the serving MSC/VLR. Then the MSC chooses a *RAND* and sends it to the mobile. Using *ki* stored in the SIM card, the MS generates *SRES* and sends back to MSC. MSC compares the SRES provided by MS and HLR, and if it matches, session key *Kc* is provided to base station. This key is used for encryption for every cellular activity thereafter. TMSI is used along with the session key instead of IMSI until a next location update is received. Once the location is updated, new TMSI and session keys will generated using the same steps. Session key agreement and provision of TMSI is shown in the Figure 4.11.

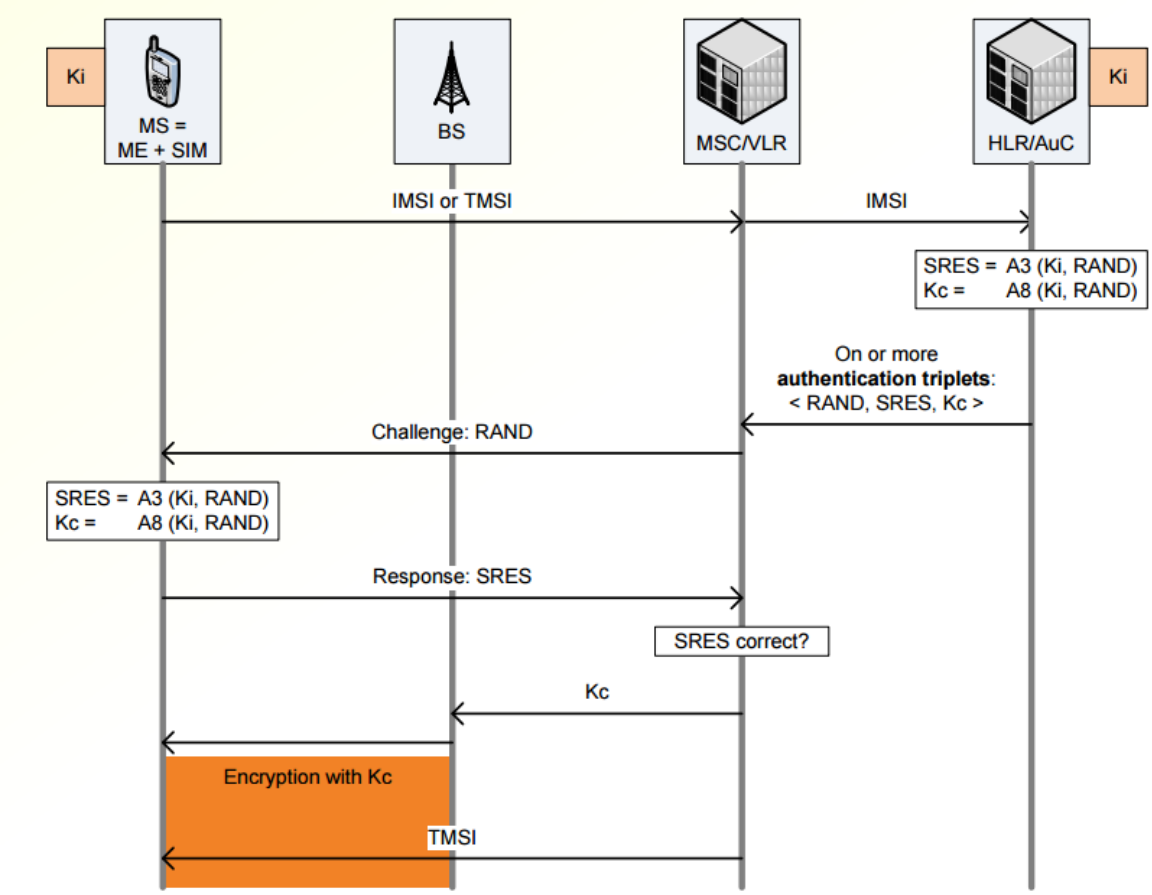



**Figure 4.11: GSM authentication mechanism [53].**

### 4.3.3.1 Call tapping attack using TMSI interception

Research on TMSI usage [54] has revealed that same TMSI will be used repeatedly irrespective of MS location update. The research also revealed that previously established keys are reused

for TMSI reallocation. This enables the attacker to perform replay attack and decrypt the communication using reused session keys.

Using OsmocomBB [55], an open Source GSM Baseband software implementation an attacker can capture TMSI over the air in RAN. Once the TMSI is captured, pro-vided the same TMSI is used for session identification, he can request the HLR to provide session keys by impersonating as MSC. The attack [44] workflow is explained in the Figure 4.12.

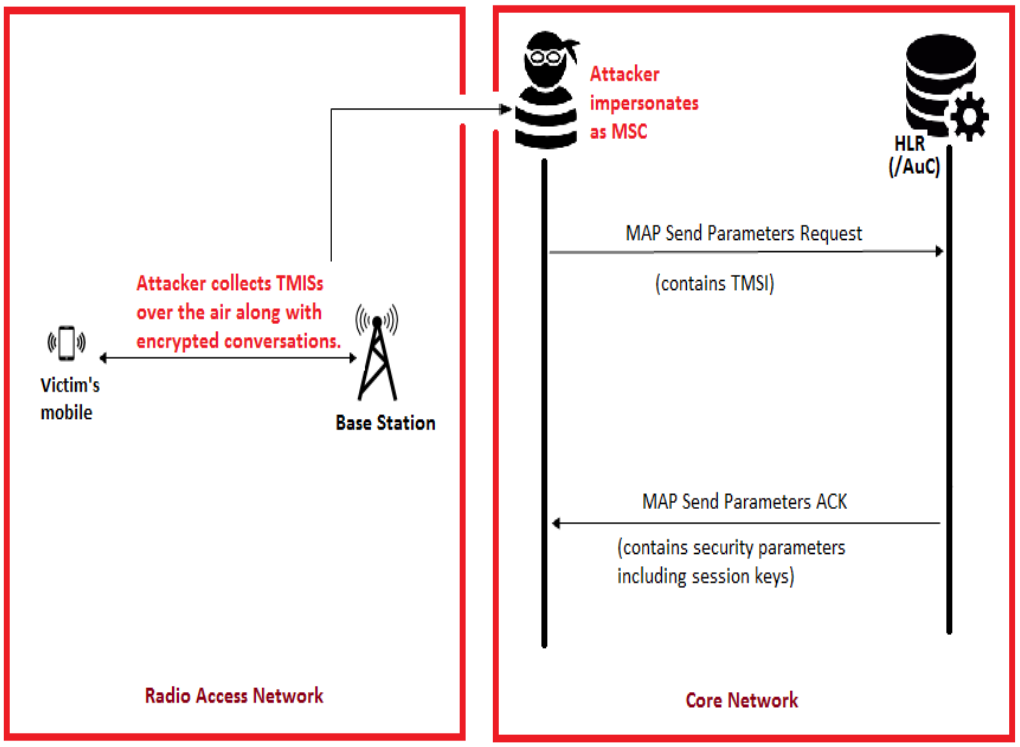



**Figure 4.12: Call interception using TMSI replay attack.**

1. Attacker catches TMSI over air (as it is frequently exchanged compared to IMSI) using OsmocomBB.
2. By impersonating as MSC, the attacker sends *MAP send Parameters Request* message to HLR by encapsulating TMSI.
3. The HLR/AuC replies back with *MAP Send Parameters Response* which contains the session keys [56].
4. The attacker can capture encrypted GSM/UMTS calls and decrypt them using the session keys obtained.

This is a passive attack and it works fine until new session key and TMSI is generated.

## 4.4 SMS based attacks

In this section, we discuss different types of SMS based attacks that can be done using loopholes in SS7 core network. Although there have been plenty of SMS frauds reported, we discuss only the attacks which utilizes SS7 completely.

As described in section 4.1.4.1 (location disclosure using SMS protocol messages), SMS protocol includes two parts [57]. When an SMS is initiated from subscriber A, the MS will contact its MSC which in turn connects to SMSC using Mobile Originated ForwardSM message. SMSC looks up for MSC GT and IMSI of the SMS receiver, and dispatches Mobile Terminated ForwardSM message towards destination MSC. The Figure 4.13 explains the two faceted SMS mechanism.

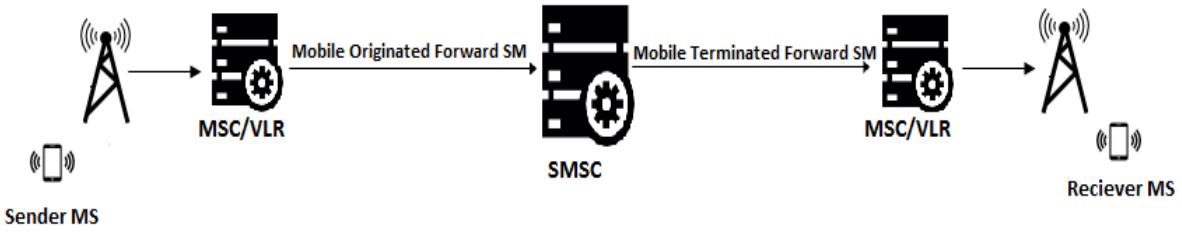



**Figure 4.13: SMS mechanism in a nutshell.**

Since Mobile Originated ForwardSM and Mobile Terminated ForwardSM messages are not checked for their authenticity, loophole in the SMS protocol leverages the chances of SMS based attacks.

### 4.4.1 SMS interception using fake MSC

In this attack [8], the attacker impersonates to HLR as an MSC that is serving the victim. Since SMSC inquires HLR for destination MSC details during Mobile Terminated ForwardSM procedure, attacker can successfully intercept all the SMS messages intended for victim. This attack is represented in the Figure 4.14:

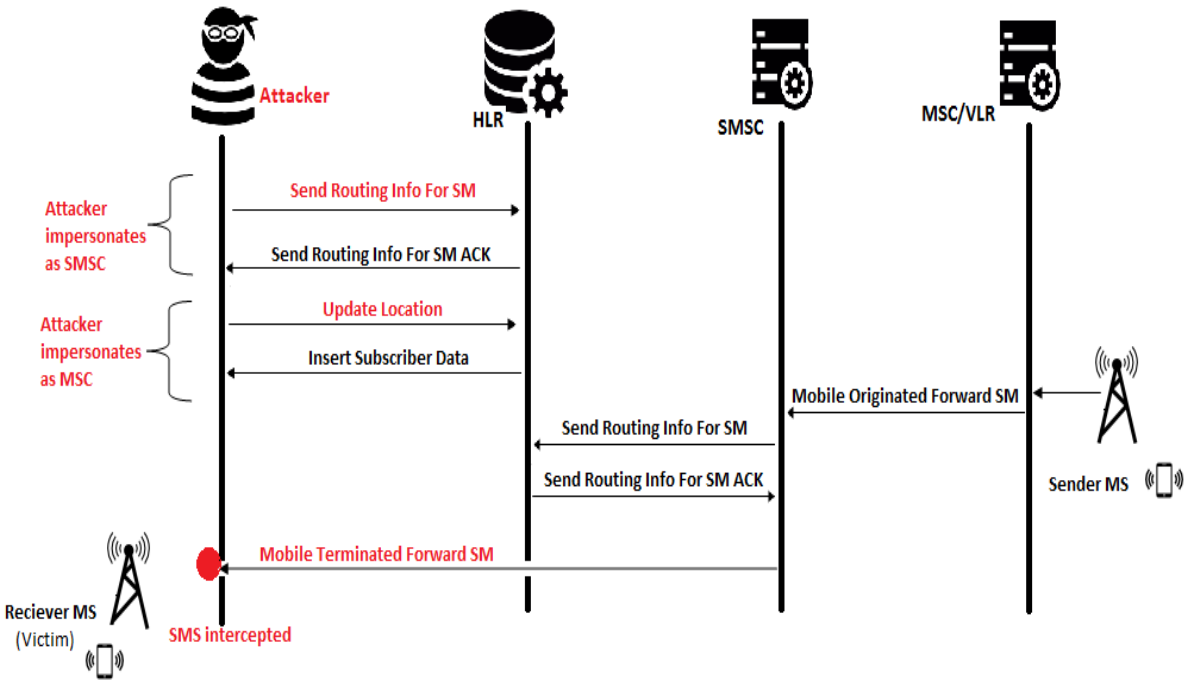



**Figure 4.14: SMS interception on the receiver end using fake MSC.**

1. As pre-requisite for this attack, the attacker impersonated as SMSC as described in section 4.1.4.1 to learn the MSC GT and IMSI of victim.
2. Once the MSC GT and IMSI of victim is known, attacker impersonates as an MSC serving the victim and sends update location message to HLR by providing victim's IMSI.
3. HLR responds back to the attacker with insert subscriber data message and this shall be ignored.
4. Now assume that subscriber A is sending an SMS to the victim (subscriber B), the MSC serving MS A will dispatch Mobile Originated ForwardSM to SMSC.
5. SMSC contacts the HLR using send Routing info for SM message to know MSC GT and IMSI of subscriber B.
6. Since HLR has stored the attacker as the MSC responsible for subscriber B, it sends attacker's MSC GT to SMSC using send Routing info for SM ACK message.
7. SMSC thinks that is the legitimate MSC of subscriber B and hence dispatches the SMS message using Mobile Terminated ForwardSM message.
8. Attacker can now receive all SMS message that is destined to subscriber B, the victim.

This attack is valid until the victim changes his location area. However as long as HLR stores attacker's fake MSC as the legitimate MSC serving the victim, the attacker can intercept all the SMS chats, one-time passwords, confirmation codes and password recovery messages which increases the threats to personal privacy.

## 4.4.2 Illegitimate SMS messages

As mentioned earlier, *Mobile Originated ForwardSM* and *Mobile Terminated ForwardSM* messages are not checked for their authenticity. This allows an attacker to send illegitimate SMS messages using various methods as follows.

### 4.4.2.1 Sending SMS using Mobile Originated ForwardSM messages

An attacker with access to SS7 network can send SMS messages using loopholes in SMS delivery mechanism. This method can be used to perform following tasks:

- Fake SMS: An SMS can be sent to any subscriber within the network by faking sender's MSISDN. Here an attacker can also spoof as some legitimate subscriber.
- Spam messages: Unsolicited SMS containing commercial advertisement, bogus contents can be sent by an attacker.
- SMS flooding: An attacker can send large number of messages to one or more destinations. The sole purpose of attacker is to slow down the network or to jam mobile stations.

To perform SMS attacks using *Mobile Originated ForwardSM* message, the only information the attacker has to know is MSC GT and IMSI of destination MS. A basic flow of such an attack is represented in the Figure 4.15.

1. To know MSC GT and IMSI of destination, the attacker uses location privacy breach attack described in section 4.1.4.1.
2. Attacker now impersonates as MSC and sends MSISDN of sender in *Mobile Originated ForwardSM* message to SMSC.
3. If SM is successfully stored in SMSC, an acknowledgement is sent back to attacker with *Mobile Originated ForwardSM ACK* message.
4. To deliver SM to the destination, SMSC has to know the MSC location and IMSI of the recipient which is stored in the HLR.

5. SMSC sends *MAP Send Routing Info For SM* message to the HLR to query the MSC GT/location and IMSI of the recipient.
6. HLR encapsulates IMSI and MSC location in *MAP Send Routing Info For SM ACK* message and sends it back to the SMSC. Based on this information, SMSC routes the SM to the recipient MSC which in turns delivers it to the mobile user using Mobile Terminated Forward SM message.

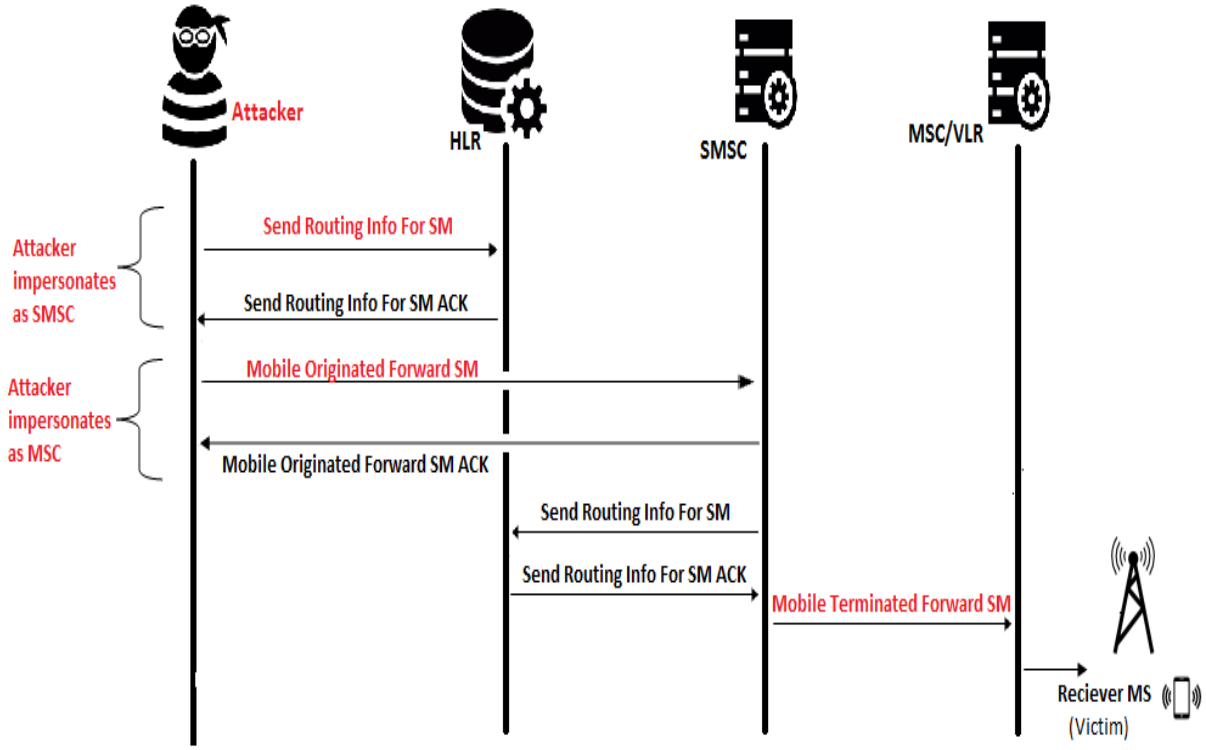



**Figure 4.15: Sending illegitimate SMS using *Mobile Originated Forward SM*message.**

This enables the attacker to successfully send an SMS to desired destination. The SMS will be billed to the sender, which can be any legitimate MSISDN that the attacker has chosen.

### 4.4.2.2 Sending SMS without inter-network agreement

Attack mentioned in section 4.3.2.1 works fine within the same network. For this attack to work outside home network, a roaming agreement should be present between the networks. In presence of roaming agreement amongst networks, SMSC of HPLMN would contact the HLR of VPLMN with *MAP Send Routing Info For SM* to know the whereabouts (MSC GT along with IMSI) of destination MS.

However, when there is no roaming agreement amongst the operator, the HLR of VPLMN simply ignores Mobile Originated Forward SM message sent by SMSC of HPLMN.

But the attacker can just execute the mobile terminated part of SMS protocol. In which he can just send Mobile Terminated Forward SM message to the destination MS by impersonating as SMSC of VPLMN. The Figure 4.16 demonstrates how an attacker can abuse internetwork SMS communication.

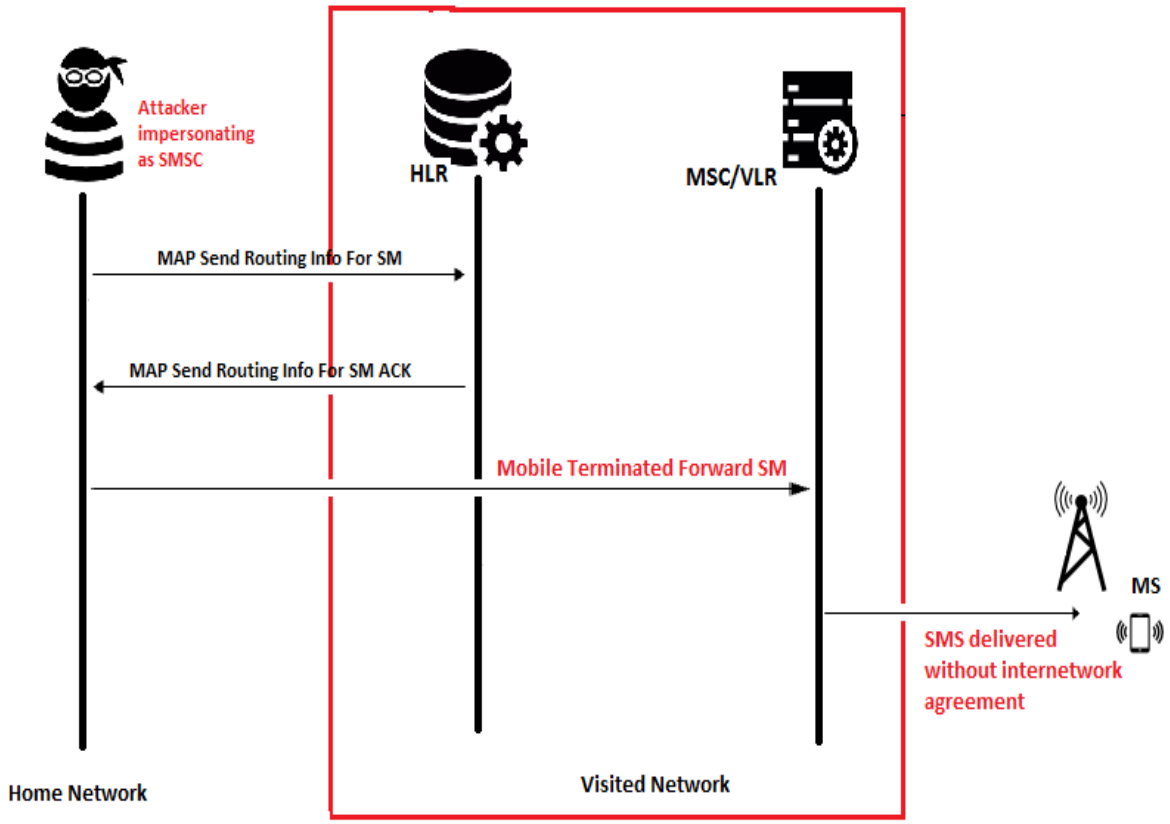



**Figure 4.16: Sending illegitimate SMS using *Mobile Terminated ForwardSM* message.**

1. Attacker learns destination MSC GT and IMSI based on location privacy breach attack described in section 4.1.4.1.
2. Attacker impersonated as SMSC of VPLMN encapsulated destination IMSI and SM in Mobile Terminated Forward SM message.
3. He sends this message to MSC serving the destination and it will be delivered to MS.

Though the attacker has violated inter operator agreements, the SMS will be success-fully delivered to desired destination. However, this incident will be logged in visited network and

it will bill the home network for SMS services. This enables the attacker to send free spam messages across the network.

# 5 NEW ATTACK TO UNBLOCK STOLEN MOBILE DEVICES

Increase in usage of mobile phones and the relative increase in the number of mobile phone thefts have imposed an overhead on securely retrieving the stolen or missing devices. While the mobile security researchers try to figure out various mechanisms to track such devices, attackers on the other hand are trying to exploit weaknesses in the mobile network system to dissipate into the dark side with stolen devices. In this chapter, one of the new attacks proposed by the author is described. The following sections explain how the SS7- MAP protocol can be misused to help an attacker to unblock the mobile device from the stolen list and use it normally.

## 5.1 Current status of mobile thefts

With advancement of recent mobile manufacturing technologies the number of mobile users is increasing day by day as mobile phones are becoming more affordable. According to the World Bank's report [58] in 2012 close to three-quarter of world's population including the developing countries have access to mobile phones. With the increase in mobile phone users, flourishing business in the black market is rising substantially. In United States, 113 phones per minute are stolen or lost; which amass about $7 million worth of smart phones on a daily basis. Recent survey [59] by Lookout, Inc. - a mobile security company revealed that about 25% of the missing phones are left in a public place, where 14% are taken from house or vehicles. Surprisingly the numbers of phone thefts happen through pickpocketing which represents 28% of missing devices.

However, mobile telephony industry and regulatory organizations take the issue with device theft seriously. In 2004, GSM Association (GSMA) has started a Central Equipment Identity Register (CEIR) for methodical recovery or tracking of stolen devices. CTIA -The Wireless Association in United States has passed compulsion on equipping remotely operated kill-switch technology in all the smartphones manufactured after mid-2015. In spite these advancements by technologists to fortify the mobile phone users, attackers have competitively grown to exploit the vulnerabilities in existing mobile network communication backend to gain illegal

control over stolen/missing devices and the private information on them. There exists a growing black market [60] where such devices are sold with least possibility of tracing them.

## 5.2 Working principle of EIR

The EIR stores IMEI which is mobile handset specific. Other identities like IMSI, MSISDN and SIM/USIM are subscription specific and they move along with the subscriber when he puts purchases a new mobile handset and start using his old card in a new device. Since IMEI uniquely identifies individual mobile devices irrespective of subscriber's network, it eventuates for EIR to store the IMEI to track the mobile device. To do so, EIR maintains a database [14] e.g. Real Time Database (RTDB) [61] to store the white, black and grey listed IMEI numbers. The blacklist contains IMEIs of all those mobile devices which are banned to access the network, the grey list contains IMEIs of devices which are allowed to use the network with the contingency that they can be tracked for malicious activities; and white list has all those devices which are allowed to access the network. The database also facilitates the association between IMEIs and IMSIs in many cases.

Below are the typical interactions [14] that take place when a mobile is switched on or when the subscriber moves to a new location. The pictorial representation of this mechanism is shown in the Figure 5.1.

1. The Mobile handset begins the registration process with the Base Station.
2. Base Station initiates the registration process with MSC/ VLR.
3. MSC triggers *MAP CHECK IMEI* message to the EIR before allowing the mobile device to register on the network and updating it to HLR. The EIR receives the required information (only IMEI or IMEI with IMSI) from the *MAP CHECK IMEI* message and searches in the database for its presence in three different lists that are present there.
4. Based on the result from the list matching in previous step, *MAP CHECK IMEI ACK* message containing the equipment status specifying whether the IMEI is in blacklist, greylist or whitelist. Depending on this, MSC takes appropriate decision about registration of the mobile device.

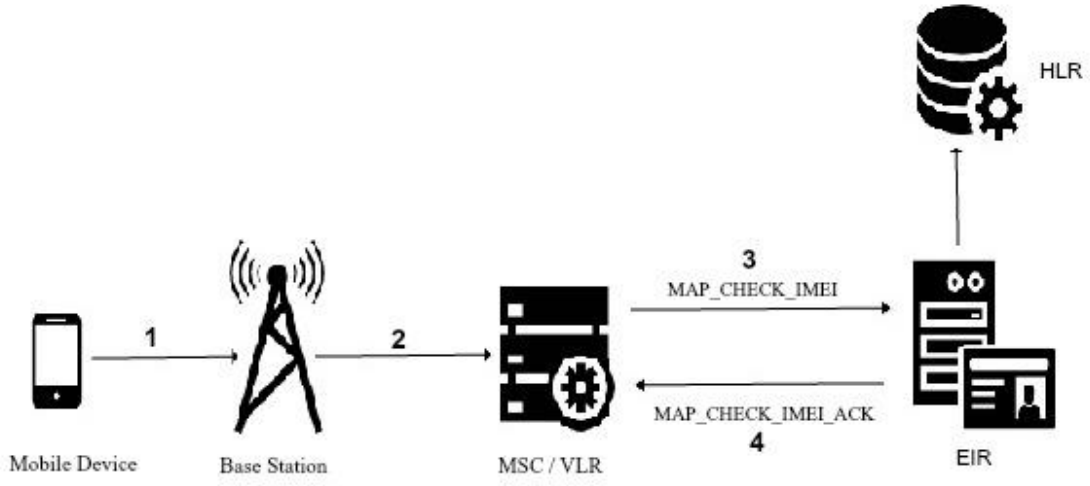



**Figure 5.1: IMEI check performed by MSC.**

Device detection by EIR is carried out in different methods since this is left to the specific implementations and not standardized. Because of this the logic behind such detection is completely network operator specific, this attack may not apply to all systems. Often the duplet of IMEI and IMSI is sent from the MSC to EIR through *MAP CHECK IMEI* message. However many cases IMEI, IMSI and MSISDN triplet is sent for further security scrutiny in modern day implementations. Since only IMEI is mandatory for this operation, it can be assumed, that many systems support IMEI-only messages.

## 5.3 Attack to unblock stolen mobile devices

Though there have been guidelines from the telephony regulatory authorities to utilize the provision of global level IMEI database through Central Equipment Identity Register (CEIR), there is no enforcement of this requirement in most countries. Since a complete real-time global centralized EIR is not fully operational as of now, mobile stolen in one country can still be used in other countries in most of the cases. The attack we present is independent of the database type. The attack presented is based on the following conditions:

- Attacker has a stolen phone which is blacklisted and he knows the IMSI which was associated with it while blocking or last use by the victim. The attacker does not need to have the original SIM as it is sufficient to have just the IMSI. The IMSI can be obtained by active attacks using IMSI catchers while it is in use or using *MAP SendIMSI*

command from the network side (for details see [5], [8] and [44]). We assume that the attacker is putting his own SIM card into the phone, which contains a new IMSI.

- Attacker has access to SS7 core network. This is possible through a compromised edge device such as femtocell or badly configured core network node e.g. [62]. Other possibilities of getting into SS7 networks are if the attacker is a gaining connection through an existing provider with insufficient security checks when renting out their SS7 access or through roaming hubs which are insufficiently protected.
- The Global Title (GT) of the EIR is required, so that the attacker can pose as the MSC. The knowledge of the MSC GT is not necessary, but increases the chances of success of the attack. The GT can be obtained e.g. GT scanning [7], since operators tend to assign GT addresses in blocks; the success rate of such a scan is quite high. If the attacker has pre-knowledge of some GT of the targeted operator e.g. obtaining roaming interworking confidential material, then this is much quicker.

We restrict the scope of our attack by defining attacker's motive at this point is to use the stolen device without risk of blocking.

Now we elaborate on the attack on the EIR which exploits the underlying mechanism when MSC sends IMEI along with IMSI during *MAP CHECK IMEI*. The relationship between those two is leveraged for unblocking a mobile device from the stolen list in the database. In such cases initially the IMEI is checked to know the list it belongs to. If it is found on the black list, an additional check of IMSI is made. If there is a match between IMSI provisioned with IMEI in the EIR database (This is the ISMI-IMEI pair in the EIR before the victim blocks his stolen device.) with the IMSI found in *MAP CHECK IMEI* message then this would override the blacklist condition [61]. It brings the blacklisted mobile to whitelist and hence allowing the registration process to continue.

This is a sensible feature implemented in EIR to automatically unblock devices that are added to blacklist by mistake or by system errors or to reset a device that has gone missing and is found again. It logically proves that the victim who blocked the device (through network operator) has now got it back and hence the IMEI –IMSI pair now is matching with the last entry before blocking. In some EIRs this is maintained to avoid unnecessary blocking in the case of mobile handset sharing (e.g. same handset is used with different SIM /UICC cards.) in

developing countries. The Figure 5.2 illustrates attack environment along with interaction between MSC and EIR. Since this is a focused extension of Figure 5.1; for the sake of clarity, interactions beyond MSC in the RAN are excluded.

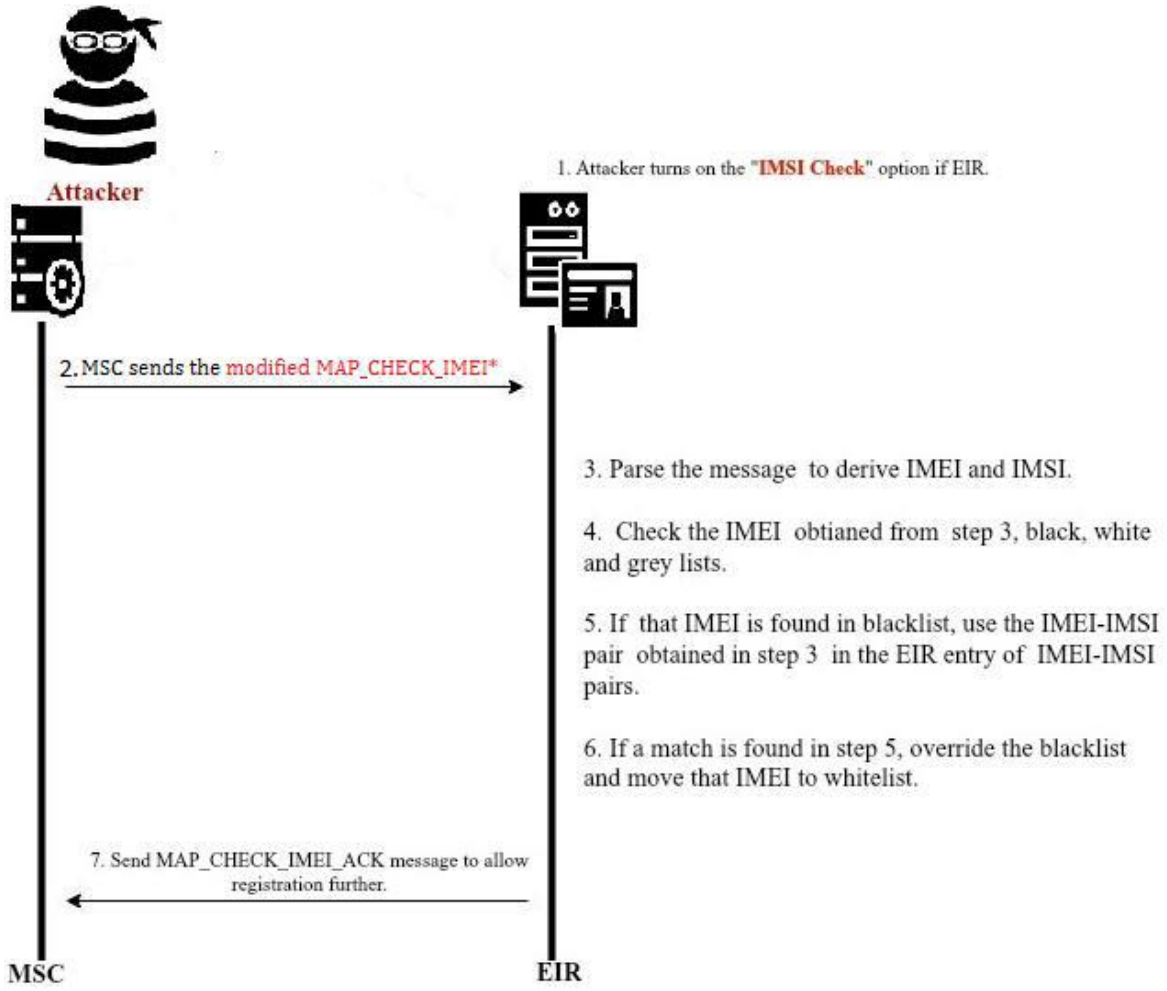



**Figure 5.2: Unblocking using modified MAP Check IMEI message.**

The steps illustrated in Figure 5.2 are explained as follows:

1. We assume that the check is switched on by default, or the attacker just sends a bunch of requests (e.g. if only every 10th time the check is invoked), or he may send his request during a low-load period (e.g. nighttime) or the attacker turns on the IMSI Check option of EIR. The last one can be done using modern device detection utilities such as [63] without disturbing the existing network topology or operation.

   Without any additional authentication check made by EIR while turning on this feature, attacker can perform this task. The IMSI Check option mandates the EIR to check IMSI if IMEI is found on the blacklist.

2. The attacker has access to the original IMSI of victim. The attacker now poses as MSC (depending on filtering level at EIR this may require knowledge of MSC GT). When attacker-MSC tries to contact EIR, the attacker sends a modified *MAP CHECK IMEI* message where his new IMSI is added and the IMEI is send to the EIR.

3. Now the EIR parses the attacker's message from step 2 to derive IMEI and IMSI from Message Signal Unit (MSU) [14]. Since each operator can place IMSI information in any desired location of the message, the
ASN1 decoder will searches the IMSI in multiple locations.

4. Now EIR checks the IMEI derived from step 3 in the EIR database black, grey and white lists. Since the IMEI is of stolen device, it will be in the blacklist as we have mentioned in the scenario that the victim has blocked his stolen phone.

5. Since the IMSI Check is activated in the beginning by attacker in context and since IMEI is found in blacklist, it uses the IMEI-IMSI pair obtained in step 3 and matches against the existing entry of IMEI-IMSI pair for the corresponding IMEI in the EIR database.

6. Since the attacker has replaced his IMSI with original IMSI of victim in step 2, a match is found in the RTDB. Hence the IMEI is overridden from the blacklist and moved to whitelist. This was only possible since the IMSI was sent in step 2.

7. Since the IMEI is there in the whitelist, EIR sends *CHECK IMEI ACK* message back to MSC to allow the IMEI to register to the network and use it. That message the attacker does not need to receive, it is only a confirmation that the attack worked.

Now the attacker has unblocked a stolen phone and he can use it without any difficulties. Since there is no check on the number of such attempts that we could find, he can run this operation every time his mobile is added to the blacklist. Even more simple method is to have his custom script running in SS7 network associated with that specific IMEI to replace his IMSI with victim's IMSI every time MSC initiates a CHECK-IMEI procedure.

A comparison of ASN1 encoding structure of *MAP CHECK IMEI* message without-IMSI [14] and that of with-IMSI (as found in the implementation of [64] is considered for illustration) is given in Figure 5.3.

```
CheckIMEI-Arg ::= SEQUENCE {
        imei                    IMEI,
        requestedEquipmentInfo  RequestedEquipmentInfo,
        extensionContainer      ExtensionContainer      OPTIONAL,
        ...}
```

**(a) When IMSI is not attached**

```
EnhancedCheckIMEI-Arg ::= SEQUENCE {
        imei                    IMEI,
        requestedEquipmentInfo  RequestedEquipmentInfo OPTIONAL,
        imsi                     [PRIVATE 1] IMSI OPTIONAL,
        locationInformat         [PRIVATE 3] OCTET STRING (SIZE (1..7))
OPTIONAL,
        extensionContainer      ExtensionContainer      OPTIONAL,
        ...}
```

**(b) When IMSI is attached**

**Figure 5.3: Variation of MAP Check IMEI message structure [14] [64].**

The attack proposed in this section is articulated with GSM and UMTS specific terminologies. However, EIR is used in higher specifications like LTE and the same attack is possible with no or minimum modification. We have demonstrated that the attacker with SS7 network privileges can gain unlawful access to use stolen (blocked) mobile phones.

Some operators ask for a monetary compensation to unblock a mobile device which serves the purpose of generating revenue and reimbursement of the additional costs from subscribers, which can be avoided if the attacker offers this service in the black market for a lower cost. Hence, alongside illegitimate access, the attacker can gain monetary benefits using the SS7 MAP vulnerability exposed in this attack.

## 5.4 Potential countermeasures

Even with the newer specifications, vulnerabilities that are specific to SS7 are still remained as there are functions with similar functionalities in Diameter, but there the usage of IPSec or TLS may prevent this attack. Another issue is that often backward compatibility needs to be maintained and therefore a downgrading type of attack is potentially possible. The suggested potential countermeasures are:

1. Access control for switching on IMEI validation.
2. Logging of the activation of the validation feature.

3. Filtering on MAP level that the *CHECK IMEI* request is coming from a known internal source (HLR, MSC).

4. Layer crosschecks; in particular, in particular the source address information in "transport layer" SCCP and MAP layer is consistent with each other.

5. If SS7 is run over IP (SIGTRAN), then the usage of IPSec should be considered, according to NDS/IP security [65].

Other countermeasures are also possible and above only give a brief outline of a potential protection strategy.

# 6 MITIGATION OF ATTACKS

In this section we discuss various mitigation strategies to secure the system against attacks described in Chapter 4.

## 6.1 Generic approach for mitigation

Since mobile core network consists of assorted protocols, applications, platforms and implementations, a concrete amalgamation between the underlying systems is required to build a defense mechanism against the attacks. A heterogeneous attack management system to protect the distributed architecture of telecommunication core network should facilitate secure communication infrastructure through authentication, encryption and access control mechanisms [13]. A pictorial representation of a strategic infrastructure to defend against SS7 based attacks in given in the Figure 6.1. The attack management system should incorporate tunneling or traffic encryption similar to Virtual Private Network (VPN), for enabling secure communication between multiple network entities.

On the grounds that SSPs are the entry points to SS7 core network from the RAN network, an authentication component deployed at each every SSP will restrict the attacks that try to gain core network access. A certificate signature mechanism obligated at these components defends the system against spoofing attacks which involves impersonation (of MSC/VLR) of core network gateways, by filtering only the certified entries to SS7 network.

On the other hand, since attackers can learn the network infrastructure and take control over the entities by intercepting the traffic between SSPs and STPs, positioning a dedicated firewall that filters the SS7 interconnection messages would be useful. These firewalls could filter the traffic based on well-known attack signatures or behavior based analytics. Alongside, if traffic between STPs is re-analyzed with the help of packet analyzer placed after the SS7 firewalls, it provides yet another layer of protection to the core telephony network. A dexterous packet analyzer module should passively monitor all the traffic between STPs and the information gathered from these analyzers can be used to review the firewall filtering policies. Since these packet analyzers can seize the malicious SS7 messages that have bypassed the firewalls at SSPs.

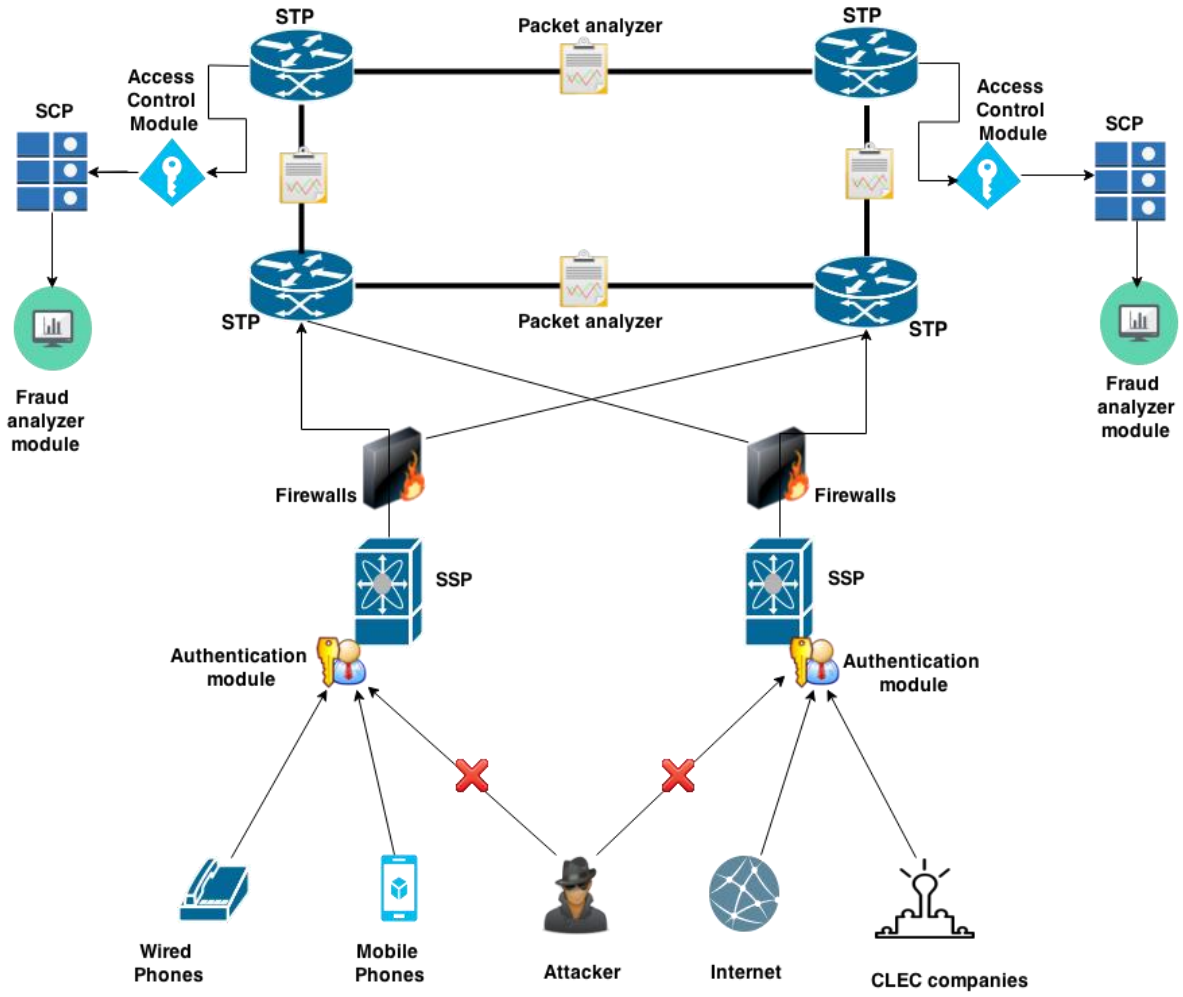



**Figure 6.1: SS7 attack management system [13].**

Since SCPs deal with sensitive data, the messages addressed to SCPs have to be scrutinized carefully for their authenticity. An access control module situated just before SCPs can control restrict illegitimate messages from unauthenticated network entities. Furthermore, a real-time fraud analyzer interfaced with SCPs in conjuncture with the access control module can be useful to analyze doubtful messages that have bypassed the access control mechanisms. These measures can help to protect the subtle subscriber information residing in the SCPs (such as HLR and EIR) from illegitimate accesses.

For obvious reasons that the above mentioned attack management system has to be implemented uniformly throughout all the global SS7 partners, the mitigation strategy may not completely protect the core network from all possible attacks. Although, by providing another

layer of security, the attack management system discussed in this section can be useful to tackle some of the attacks. More concrete mitigation strategies are discussed in the succeeding sections.

## 6.2 SMS Home Routing

As articulated in Chapter 4, one of the most common core network message used by the attackers involve flaw in the original SMS mechanism. Often the attackers use Send Routing Info For SM message as a preparation step for more sophisticated attacks alongside learning MSC GT and location of the victim. In original GSM specification [57] for SMS routing, an SMSC from HPLMN as well as VPLMN will contact the HLR of home network to know the location of MS, so that the SMSC can directly deliver the short message. However, the location and MSC GT information provided to an external network operator can be avoided which restricts the attacker to use *Send Routing Info For SM* message for his trickery.

Instead of relinquishing MSC GT and IMSI of MS directly to the SMSC of VPLMN (or to malicious host), the *Mobile Terminated Forward SM* message from an interconnection (roaming partners, other network operators, unknown hosts including attackers) will be routed through an SMS service platform (SMS home router) in the home network. This mechanism is termed as 'SMS home routing'. Rather than using IMSI of receiving MS, *Send Routing Info For SM* message request to HLR will only provide MSISDN of the MS and a 15 digit MT-SMS Correlation ID [66]. This correlation ID establishes a mutual relationship between *Send Routing Info For SM* and *Mobile Terminated Forward SM* messages. Structure of MT-SMS Correlation ID is given in the Figure 6.2.

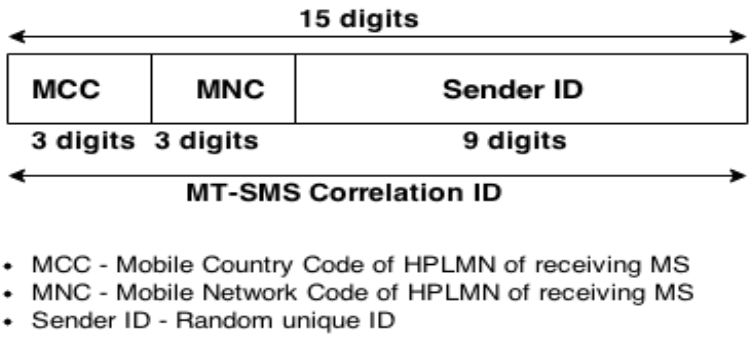



**Figure 6.2: MT-SMS correlation ID [66].**

The MCC and MNC are retrieved by the SMS home router using IMSI of receiving MS, whereas Sender ID is chosen randomly for security reasons.

The Figure 6.3 demonstrates the comparison between SMS mechanism with and without home routing.

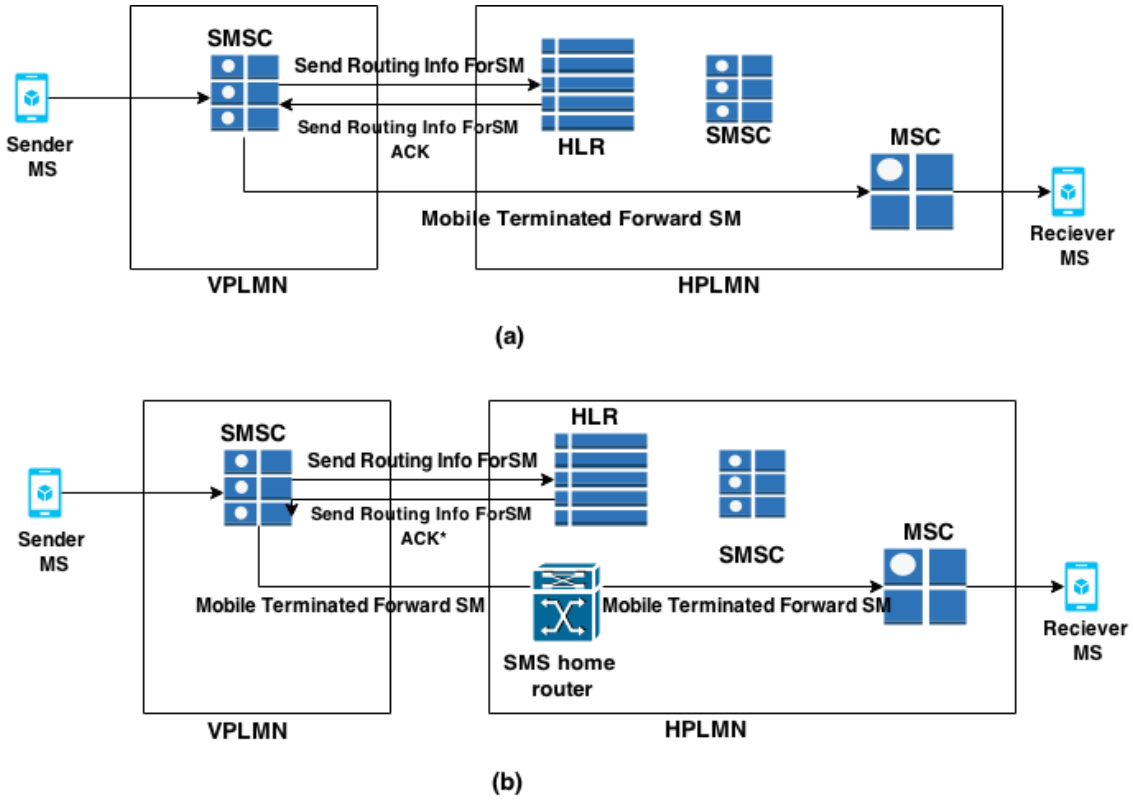



**Figure 6.3: (a) SMS delivery without home routing (b) with home routing.**

SMS home routing defends the mobile core network against spoofed or fraud SMS, illegitimate location privacy breaches. Furthermore, it also enables value added services between multiple network operators and lawful interception of SMS message sent while in another country. 3GPP TR 23.840 [67] has included the SMS home routing in two modes– non transparent mode (enabled where only MT-SMS correlation ID is disclosed to roaming partners) and transparent mode at a higher price roaming agreement (where IMSI of the receiver MS is also disclosed after authentication checks). Some of the global operators had issued with IMSI non-disclosure for billing purposes and it has been added to the specification lately. However since it is not mandated yet, practical implementation roll out is still under progress as it is considered to be an advanced feature of SMSC.

## 6.3 STP firewalls

While studying the attacks abusing mobile core network, it was evident that attackers misuse the interconnection between multiple operators at STPs. Attackers often masquerade as roaming partners and try to establish connection to target STPs by their GT or SSN, and then exploit the system by issuing unexpected network internal commands. Such malicious activities can be stopped by implementing a sophisticated STP firewall system [5] to monitor the interconnection.

An intuitive firewall can be overlaid onto the existing network; by situating the firewalls at SS7 interconnect points. An advanced analysis and reporting module accompanying the firewall can perform real-time inspection and report it to the firewall for policy changes. Heuristic detection and node finger printing can be used to filter out the legitimate core network messages. A pictorial representation of STP firewall architecture is given in Figure 6.4.

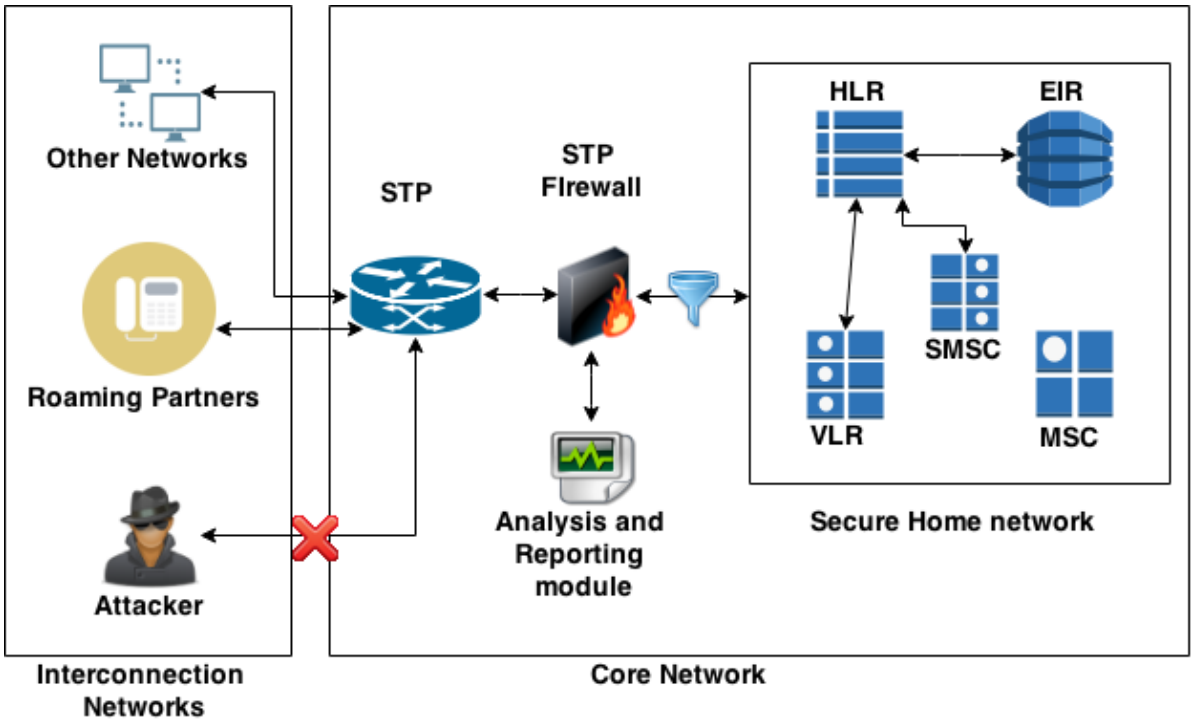



**Figure 6.4: STP Firewall Architecture.**

## 6.4 Best Practices

Some of the best practices that can be incorporated by both mobile network operators and providers are enlisted below:

1. High priority messages like *Any Time Interrogation* and *MAP Send Parameters* is purely internal. Hence any such message from an external network should be filtered out.
2. Mobile network operators should completely remove dependency on handing over subscriber IMSI and MSC GT to external networks. This mechanism can be adapted using proper implementation of SMS home routing and optimal routing within the network. This forbids the attackers at first place from executing interception and fraudulent attacks as they cannot locate their victims.
3. Messages like *Insert Subscriber Data* should be processed only after authenticating the origin of the message. In case if they are originated from external networks or APIs, such requests should be denied.
4. During handovers, it is observed that the attacker exploits the system by intercepting network internal messages before the completion of TCAP handshake. By enforcing MSC/VLR to prosecute the changes requested by the MSCs only after the TCAP handshake completion [68].
5. Any information being sent out of HLR should be filtered based on checking the origin of requester. Messages such as *Update Location* have to be checked with the previous MSC/VLR to confirm the legitimacy of new VLR.
6. Network operators without roaming agreements should be blocked at interconnect STPs. Transport layer firewalls (Layer 2 firewalls) as part of SCCP Routing Control (SCRC) to enforce legitimate GT and SSN routing [69] can be implemented to provide more security to the system. This firewall can also be accompanied with application level firewalls (Layer 7 firewalls) to filter out malicious MAP, CAP and supplementary (SS) service messages.
7. Mobile operators should educate their subscribers to be aware of RAN network attacks such as IMSI catchers, fake base stations and silent SMS by enforcing them to use user applications such as ‘SnoopSnitch’ [70] and ‘Darshak’ [71].

# 7 FUTURE RELEVENCE OF THE ATTACKS

## 7.1 3G, 4G and beyond

Mobile phone attacks have become very common these days with the end of walled garden era where only a select few could access the telecommunication backbone. In spite the advancement in mobile standards, GSM is still the most widely deployed cellular standard in the world, as the newer 3GPP standards maintain backward compatibility with it. Though the four decades old SS7 is slowly being replaced by the newer Session Initiation Protocol (SIP) and Diameter protocols, the old protocol is still used and supported in the majority of telecommunications networks. The attacks analyzed as part of the thesis have proved that SS7 vulnerabilities will serve as tool for attackers against the backward-compatible networks. Earlier chapters provide a detailed analysis of multiple attack vectors against the mobile core network. An attacker can exploit the interconnection between multiple network operators, and disrupt the cellular services, as well cause significant losses to the telecommunication industry. Just with the victim's phone number, the attacker can trace his location, interrupt the cellular services to which the victim has subscribed, and intercept the communication without being noticed by the operators or the victim. A strong requirement for preserving personal privacy of the mobile subscribers has become top priority of mobile operators.

Some of the publicly available documents such as [72], [73] and [74] demonstrate the protection capabilities of mobile networks along with the global risk to the telecommunication sector and to the users. These documents rate the mobile network in terms of their protection capabilities (against the attacks analyzed in the thesis) relative to a reference mobile network [74] that implements all the protection or mitigation measures that have been outlined in chapter 6. It is evident from this analysis that the telecommunication networks have not implemented the latest security measures to protect their subscribers. As we have also seen in this thesis, such measures would be urgently needed.

Though SS7 protocol seems to be outdated, vulnerabilities in SS7 have affected newer standards such as UMTS and LTE. SS7 enables the exchange of encryption keys and, hence, even the UMTS encrypted communication over RAN can also be decrypted by mounting the attack analyzed in section 4.2.3. The fact that SS7 enables a 3G IMSI catcher is quite significant

[5]. Contrary to all the attacks analyzed in this thesis against the mobile core network, there exist a large number of attacks that exploit other vulnerabilities in SIM cards [75] and the mobile Internet (GPRS) [76] as well as enable sniffing the RAN traffic [77]. Even with the implementation of the latest cryptography standards, mobile phones are still prone to clandestine surveillance programs, as the encryption keys used at the root level (SIM cards) are too short [75] to resist cyber espionage.

As explained in chapter 4, the attackers exploit basic cellular service workflow such as voice calls and text messages, and hence not all the SS7 attacks can be blocked with simple filtering as it might affect the regular working mechanisms of telecommunication systems. Furthermore, attacks on value-added services such as Unstructured Supplementary Service Data (USSD), which is used for monetary transactions can incur considerable financial loss to the victim [8] or wipe out personal data from the phone [78]. Since banks and other governmental agencies are also involved [77] besides the mobile phone subscribers, USSD-based attacks can be catastrophic to a larger community. Considering the features with wide range of service subscriptions, USSD is going to be the target of telecommunication fraud. Additionally, Multimedia Messaging Services (MMS) ports the design specification of SMS protocol and, hence, most of the SMS based attacks (section 4.3) can be potentially be extended to the MMS protocol.

## 7.2 Diameter protocol replacing SS7

Newer standards such as 4G are moving towards 'all-IP' connections and the IP based Diameter protocol [34]. Since the IP-based signaling protocols by default use IPsec to authenticate connections, they have higher chances of providing sufficient security than SS7, which has no such protection. However, there is also the possibility that the IP-based attacks from the Internet could be replicated in the telecommunication networks.

Diameter addresses a broader range of emerging technologies than just cellular access, such as Mobile IP and the Internet of Things (IoT). Diameter was designed to resolve the issues with its predecessor, Radius, by improving the authentication, authorization and accounting (AAA) functionality. Since any node within the Diameter system can initiate a request, Diameter is considered to be a peer-to-peer (P2P) communication protocol. The AAA functionality is

incorporated with the help of a Network Authentication Server (NAS) and a shared authentication server [34]. Being a P2P network, every node within the Diameter system can act as a client or a server depending on the network deployment. Every peer within the system uses dynamic peer discovery strategies including peer tables [79], which removes the need for the manual configuration of the NAS. Diameter can use the SCTP or Transmission Control Protocol (TCP) as the transport layer protocol.

One of the key measures to protect the core telecommunications network against network breaches is by hiding the critical elements from outside exposure. In SS7, the Global Title Translation (GTT) functionality [4] helps to achieve network exposure by reducing the need of disclosing the entire network's element addresses in the routing tables of each and every node of the network. GTT hides the critical infrastructure such as HLR and EIR, as STPs can resolve the actual addresses of these elements using internal routing tables. This concept in Diameter protocol is implemented by default in the Home Subscriber Service (HSS) which takes care of GTT as well as mutual network terminal authentication. GTT and mutual terminal authentication jointly can protect the system against SCTP port scanning (section 3.2) and impersonation attacks.

Another concern of the GSM/UMTS core networks is mapping the boundaries of the core network by an attacker by penetrating deeper into the network using vulnerable ports exploiting the interconnection gateways. The Diameter protocol prevents such penetration by topology hiding [67] in terms of critical infrastructure as well as routing paths. When an internetwork message is sent outside the HPLMN, the STP router replaces the internal (actual) address of the network entity with a generic address which can only be resolved by that STP. This helps hide global IP addresses from the view of an attacker who is trying to gain access to mobile core network. This not only prevents the attacker from accessing internal elements but also prevents man-in-the middle (MitM) attacks. As part of backward compatibility, mobile operators have to support interconnection of GSM/UMTS to LTE systems. Address resolution during roaming between the 2G/3G MAP protocol and LTE Diameter is handled by the Interworking Function (IWF) interfaces [80].

Contrary to SS7, the Diameter protocol ensures secure connection between the entities of the core network by IP Security (IPSec) or Transport Layer Security (TLS) that authenticate and

encrypt the internal traffic. Diameter uses the TLS handshake protocol [81], which utilizes X.509 [82] certificates and asymmetric cryptography to authenticate the peers which are part of communication. Since the traffic is encrypted, an attacker who has already gained access to the core network cannot intercept the transmission between network entities [83]. Authentication between the peers in the Diameter protocol makes it comparatively more secure than SS7. Diameter uses Network Access Identifier (NAI), Challenge Handshake Authentication Protocol (CHAP), Extensible Authentication Protocol (EAP) and Password Authentication Protocol (PAP) for authentication [84]. The option of specifying Hop-by-Hop and End-to-End identifiers [85] in the message packets ensures a secure routing path as well as end to end security.

With the AAA mechanism in place, Diameter appears to be more secure than SS7 whose purpose was communication within trusted network. One of the key issues with the Diameter specifications is that, though it standardizes the use of IPSec and TLS in mobile communication, using them is not mandatory [34]. Also, there is no procedure to verify whether IPSec or TLS have been used underneath the Diameter implementation [18] of VPLMN. Moreover, being a P2P protocol, Diameter is application based. The rate at which Diameter can send or handle messages and the disclosure of interconnected peers or routes are dependent on the application. The packets that a Diameter system can send depend on the application that generates them rather than network settings. In such application driven environments, if there is insufficient traffic to piggyback the acknowledgement messages [84]; the underlying TCP or SCTP protocols may cause more traffic with encrypted data. Furthermore, the application decides the penetration or reachability of the signaling messages [18]. The attacker can impersonate at the application level and penetrate deeper into the core network. Hence Diameter cannot completely ensure the core network security against spoofing and interception during interconnection.

Additionally, Diameter uses the X.509 certificate and Public Key Infrastructure (PKI) for authentication; the common the problems of PKI such as distribution of public keys, management of certificates and verification of certificate revocation continue to create the security administration overhead in core networks [34]. Yet another issue with Diameter protocol is that, it does not secure the system against DoS attacks. Though the peers can recognize the malicious flooding messages, the failover algorithms within Diameter

implementation try to respond to the attacker with error messages. The attacker can exploit this vulnerability to submerge the target peer with flooding messages and hence execute a successful DoS attack.

Many of SS7 design features including some flaws have been replicated in the Diameter protocol. GSM/UMTS systems take most of the market share (in terms of inter-operator roaming) compared to hardly a handful of LTE roaming implementations. Since GSM/UMTS along with SS7 will continue to rule the core network domain for probably the next couple of decades, the positive changes that Diameter could affect to the core network are not huge.

# 8 CONCLUSION

Telecommunication network is an intricate system made up of diverse subsystems built on different technologies. While legacy systems are there to survive for the years to come, the security of the whole system can be defined by the security level of the weakest link and partner. The SS7 protocol was built for signaling between a handfuls of trusted telecommunication partners, but it is still being used in the backbone of mobile communication with an open market for new operators to serve more than half of the world population. Even though the walled garden era of trusted partners has been ended with advancement of technologies, SS7 may still continue to dominate mobile core network system for at least the next few years. Moreover, integration of Internet technologies with telecommunication systems have produced new ways for attackers to penetrate into the system. Popular hardware, software and operating systems on personal computers provide the same functionality as sophisticated equipment used in earlier day's telecommunication environment, which means that the attacks no longer limited by access to hardware or software.

The thesis introduced the problem and goals in chapter 1. Chapter 2 gave a brief description of signaling systems, the various internal components of the core network, and the addressing schemes used within the mobile core network. This chapter provided an insight to the real life components of telephony network, rather than just providing a logical abstraction of the underlying architecture. Furthermore, chapter 3 established a connection from the core network architecture to attack strategies that can be used to get into the system. It also outlined how an attacker can penetrate to the SS7 backbone using the advanced features of SIGTRAN and SCTP protocols. Since an outside attacker can exploit open entry points and map the periphery of core network, the risks of such attacks are worth researching. Additionally, chapter 3 also summarized the relaxations of the telecommunication laws which allow anyone including fraudsters to lawfully enter the mobile communication backend.

Chapter 4 explained various methods to manipulate mobile traffic for different types of attacks ranging from tracking the victim in real-time to intercepting all of his mobile communication. With the help of various flow diagrams, it was explained that, by just having victim's phone number, an attacker can breach the privacy and cause financial loss to the victim as well as to

mobile operators. Chapter 5 demonstrated one of the new attacks found by the author, using which a core network attacker can unblock stolen phones for selling them into the black market. The attack exploits the relationship between the mobile phone identifier (IMEI) and the subscriber identity (IMSI) to gain illegitimate access to the equipment identity register (EIR) module. Since this type of exploitation has so far been ignored by the telecom operators, a recommendation to GSMA was made (based on the analysis of this thesis) to filter-out the malicious attack messages.

Chapter 6 articulated several mitigation strategies to defend the core network against the attacks explained in chapter 4. This chapter explained a security architecture and mechanisms to block malicious messages from an attacker at suitable gateways without affecting the normal functioning of the underlying system. Since most of the attacks use message which are part of basic cellular services, a malfunctioning mitigation mechanism could incur a huge financial loss to the network operators.

As part of the discussion, chapter 7 emphasizes how a protocol specific to an older cellular standard can cause catastrophic degradation of security measures incorporated in newer standards. An overview of state of the art security is outlined by describing numerous different attack vectors which are out of scope of the thesis. In chapter 7, limitations and advantages of the Diameter protocol, the successor of SS7 in LTE standards, was explained. Though Diameter appears to be more appealing in terms of security, the potential extension of the known attacks in chapter 7 highlighted the need for strict scrutiny of Diameter specifications before it is implemented on a global scale.

Complexity of network layers and diversity of protocols in the telecommunication field makes it more difficult to find all loopholes in the systems. Even with in-depth knowledge and expertise, providing complete security solutions to end users as well as to mobile operators is a major challenge. However, if the telecommunications operators ignore the early stage disclosures of core network attacks, such as the new attack presented in this thesis, undoubtedly many end subscribers or even entire nations can become victims of attackers.

# REFERENCES


[1] G. Association, "The Mobile Economy 2015," [Online]. Available: http://bit.ly/1Gh19cQ. [Accessed 10 February 2015].

[2] A. &. G. B. Soltani, "New documents show how the NSA infers relationships based on mobile location data.," Washington Post, [Online]. Available: http://wapo.st/1hrSi9F. [Accessed 10 February 2015].

[3] "Taking up the Gauntlet: SS7 Attacks," Adoptive Mobile, 16 December 2014. [Online]. Available: http://bit.ly/13VDJdi. [Accessed 01 May 2015].

[4] M. Mimoso, " Cellular Privacy, SS7 Security Shattered at 31C3.," Threatpost, 30 December 2014. [Online]. Available: http://bit.ly/1dadB2U. [Accessed 22 January 2015].

[5] K. Nohl, "Mobile self-defense," December 2014. [Online]. Available: http://tinyurl.com/n85sxyl. [Accessed 10 March 2015].

[6] T. Engel, "Locating mobile phones using signalling system 7," in *25th Chaos communication congress*, 2008.

[7] A. De Oliveira and P.-O. Vauboin, "Worldwide attacks on SS7 network," April 2014. [Online]. Available: http://tinyurl.com/m6rsa7u. [Accessed 10 January 2015].

[8] D. Kurbatov and S. Puzankov, "Cell Phone Tapping: How It Is Done and Will Anybody Protect Subscribers.," 08 April 2014. [Online]. Available: http://bit.ly/1Gh33Kr. [Accessed 10 January 2015].

[9] University of Tartu, "Recommendations for theses writing," 2014. [Online]. Available: http://www.cs.ut.ee/sites/default/files/2014/l6put88d/Recommendations_2014.pdf. [Accessed 20 May 2015].

[10] INTERNATIONAL TELECOMMUNICATION UNION, "Vocabulary of switching and signaling terms".

[11] Performance Technologies, "Tutorials on Signaling Sytem 7(SS7)," [Online]. Available: http://www.eurecom.fr/~dacier/Teaching/Eurecom/Intro_computer_nets/Recommended/ss7.pdf. [Accessed 12 May 2015].

[12] "Signaling System 7," [Online]. Available: http://www.cs.rutgers.edu/~rmartin/teaching/fall04/cs552/readings/ss7.pdf. [Accessed 11 May 2015].

[13] T. Moore, T. Kosloff, J. Keller, G. Manes and S. Shenoi, "Signaling system 7 (SS7) network security," in *The 2002 45th Midwest Symposium on Circuits and Systems, 2002. {MWSCAS}-2002.*, 2002.

[14] 3GPP, "3GPP specification: TS 29.002; Mobile Application Part (MAP) specification (Release 12)," 3rd Generation Partnership Project.

[15] B. Gabelgaard, "The (GSM) HLR-advantages and challenges," in *Universal Personal Communications, 1994 Third Annual Conference*, 1994.

[16] M. Mouly and M. Pautet, The GSM system for mobile communications, Palaiseau, France, 1992, pp. 100-472.

[17] 3GPP, "3GPP TR 23.039; Interface Protocols for the Connection of Short Message Service Centers (SMSCs) to Short Message Entities (SMEs)," 3rd Generation Partnership Project..

[18] L. Philippe, "Diameter vs SS7 from a security perspective," P1 Labs, 13 July 2013. [Online]. Available: http://labs.p1sec.com/2013/07/28/346/. [Accessed 10 May 2015].

[19] 3GPP, "TS 22.016; Technical Specification Group Services and System Aspects; International Mobile International Mobile station Equipment Identities (IMEI)," 3rd Generation Partnership Project .

[20] . Y. Shui, K. Sood and . X. Yong, "An Effective and Feasible Traceback Scheme in Mobile Internet Environment," *IEEE Communications Letters*, vol. 18, no. 11, pp. 1911-1914, 2014.

[21] 3GPP, "TS 23.003; Numbering, addressing and identification," 3rd Generation partnership Project.

[22] G. Sidebottom, L. Coene, G. Verwimp, J. Keller and B. Bidulock, "Signalling Connection Control Part User Adaptation Layer (SUA)," {RFC} Editor, 2004.

[23] "Telecommunications Act of 1996," US government Publication Office, Public Law 104-104 section 301, 104th Congress, 1996.

[24] "Telecommunications Act of 1996," Federal Communications Corp, 1996. [Online]. Available: https://transition.fcc.gov/telecom.html. [Accessed 3 May 2015].

[25] "ETSI TR 101.943: Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture," European Telecommunications Standards Institute.

[26] 3GPP, "3GPP TS 23.066: Support of Mobile Number Portability (MNP); Technical realization; Stage 2".

[27] P. Langlois, "Getting in the SS7 Kingdom: hard technology and disturbingly easy hacks to get entry points in the walled garden," 2010. [Online]. Available:

http://www.hackitoergosum.org/2010/HES2010-planglois-Attacking-SS7.pdf. [Accessed 20 May 2015].

[28] L. Ong, I. Rytina, M. Garcia, H. Schwarzbauer, L. Coene and H. Lin, "Framework Architecture for Signaling Transport," RFC editor, 1999.

[29] R. Stewart, "Stream Control Transmission Protocol," RFC Editor, 2007.

[30] "Sctpscan: SCTP Network And Port Scanner," P1 Security, [Online]. Available: http://www.p1sec.com/corp/research/tools/sctpscan/. [Accessed 10 May 2015].

[31] "SCTP Headers," security.maruhn.com, [Online]. Available: http://security.maruhn.com/iptables-tutorial/x1736.html. [Accessed 17 May 2015].

[32] "P1 Vulnerability Knowledge Base (VKB).," P1 Security, [Online]. Available: http://www.p1sec.com/corp/products/vulnerability-knowledge-base-vkb/. [Accessed 15 May 2015].

[33] P. Langlois, "Diameter vs SS7 from a security perspective.," P1 Labs, [Online]. Available: http://labs.p1sec.com/2013/07/28/346/. [Accessed 9 May 2015].

[34] V. Fajardo, J. Arkko, J. Loughney and G. Zorn, "Diameter Base Protocol," RFC Editor, 2012.

[35] "'Wireshark'- a network protocol analyzer for Unix and Windows," Wireshark Team, [Online]. Available: Wireshark is a network protocol analyzer for Unix and Windows. [Accessed 10 February 2015].

[36] P. Biondi, "'Scapy'- a packet manipulation program," [Online]. Available: http://www.secdev.org/projects/scapy/. [Accessed 22 January 2015].

[37] Y.-C. Hu and H. J. Wang, "A framework for location privacy in wireless networks," in *ACM SIGCOMM Asia Workshop*, 2005.

[38] 3GPP, "3GPP specification TS 04.31: Location Services (LCS); Mobile Station (MS) - Serving Mobile Location Centre (SMLC) Radio Resource LCS Protocol (RRLP)," 3rd Generation Partnership Project.

[39] L. Ostman, "A study of Location-Based Services including design and implementation of an enhanced Friend Finder Client with mapping capabilities," *Lulea Tekniska Univeritet*, 2001.

[40] Shri, *SMS in GSM Network.*

[41] 3GPP, "3GPP TS 03.40: Technical realization of the Short Message Service (SMS)," 3rd Generation Partnership Project.

[42] 3GPP, "3GPP TS 23.078: Customized Applications for Mobile network Enhanced Logic (CAMEL)," 3rd Generation Partnership Project.

[43] C. Pudney, "3GPP TSG-SA WG2 meeting #22, 2002: Liaison Statement on Restoration of R'96 Any Time Interrogation functionality," 3rd Generation Partnership Project.

[44] T. Engel, "SS7: Locate. Track. Manipulate," December 2014. [Online]. Available: http://tinyurl.com/krvmuxk. [Accessed 15 March 2015].

[45] 3GPP, "3GPP TS 03.71: Location Services (LCS); Functional description; Stage 2.," 3rd Generation Partnership Project (3GPP).

[46] Shodanhq.com, *SHODAN - Computer Search Engine*, 2015.

[47] "Unwired Labs," [Online]. Available: http://unwiredlabs.com/api. [Accessed 10 May 2015].

[48] ITU-T, "The International Public Telecommunication Numbering Plan," ITU-T, 2011.

[49] Asterisk, "Asterisk - an open source framework for building communications applications," Asterisk, [Online]. Available: http://www.asterisk.org/get-started/applications/pbx. [Accessed 10 May 2015].

[50] 3GPP, "3GPP TS 03.12: Location Registration Procedures," 3rd Generation Partnership Project.

[51] 3GPP, "3GPP TS 23.031: 3G Security; Fraud Information Gathering System (FIGS); Technical realization; Stage 2," 3rd generation Partnership Project.

[52] 3GPP, "3GPP TS 33.102: 3G security; Security architecture," 3rd Generation Security Project.

[53] T. Aura, *Lecture notes: Network Security- GSM and 3G Security*, Aalto University, 2010.

[54] M. Arapinis, L. I. Mancini, E. Ritter and M. Ryan, "Privacy through Pseudonymity in Mobile Telephony Systems," in *Proceedings 2014 Network and Distributed System Security Symposium*, 2014.

[55] OsmocomBB, "OsmocomBB," [Online]. Available: http://bb.osmocom.org/trac/. [Accessed 12 May 2015].

[56] Dialogic, *MAP Programmer's Manual*, Dialogic DSI Protocol Stacks, 2014.

[57] 3GPP, "3GPP TS 23.040: Technical realization of the Short Message Service (SMS)," 3rd Geneartion Partnership Project.

[58] World Bank, "Information and Communications for Development 2012: Maximizing Mobile," World Bank, Washington, DC., 2012.

[59] "Phone Theft in Europe: What Really Happens When Your Phone Gets Grabbed," Lookout, Inc, May 2014. [Online]. Available: https://www.lookout.com/resources/reports/phone-theft-in-UK. [Accessed 20 April 2015].

[60] "The secret world of stolen smartphones, where business is booming," Wired.com, December 2014. [Online]. Available: http://www.wired.com/2014/12/where-stolen-smart-phones-go/. [Accessed 12 April 2015].

[61] Tekelec, "Feature Manual - Equipment Identity Register," 2012. [Online]. Available: https://docs.oracle.com/cd/E52590_01/doc.440/910-6272-001_rev_a.pdf . [Accessed 12 April 2015].

[62] Positive Technologies, "Signaling System 7 (SS7) security report.," December 2014. [Online]. Available: http://tinyurl.com/pkrbae3. [Accessed 10 April 2015].

[63] MobileThink, "Instant Identification of All Devices," [Online]. Available: http://mobilethink.com/products/device-detection/. [Accessed 22 April 2015].

[64] *Attachment #8973 for bug #7648,* Bugs.wireshark.org.

[65] 3GPP, "3GPP TS 33.210 3G security; Network Domain Security (NDS); IP network layer security," 3rd Generation Partnership Project.

[66] 3GPP, "3GPP TR 23.840 V7.0.0: Technical Specification Group Core Network and Terminals; Study into routeing of MT-SMs via the HPLMN (Release 7)," 3rd generation Partnership Project.

[67] 3GPP, "3GPP TR 23.840: Study into routing of MT-SMs via the HPLMN," 3rd Generation Partnership Project.

[68] 3GPP, "3GPP TS 33.204: 3G Security; Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) user security," 3rd Generation Partnership Project.

[69] Informit.com, *Signaling System No. 7 | SCCP Routing Control (SCRC) | InformIT*.

[70] SR Labs, "SnoopSnitch," Security Research Lab.

[71] S. Udar and R. Borgaonkar, "Understanding IMSI Privacy," Blackhat USA 2014.

[72] "SS7 Map," P1 Security, [Online]. Available: http://ss7map.p1sec.com/. [Accessed 15 May 2015].

[73] P1 Security, "niffmap: Map of probable Internet network interception," P1 Security, [Online]. Available: http://sniffmap.telcomap.org/. [Accessed 15 May 2015].

[74] Security Research Labs, "GSM Security Map," Security Research Labs, [Online]. Available: http://gsmmap.org/. [Accessed 15 May 2015].

[75] Security Research Labs, "SIM Card Exploitation," [Online]. Available: https://srlabs.de/blog/wp-content/uploads/2013/08/130803.SRLabs-SIM_card_exploitation-OHM.pdf. [Accessed 15 May 2015].

[76] D. Kurbatov , S. Puzankov and P. Novikov, "Vulnerabilities of Mobile Internet," [Online]. Available: http://www.ptsecurity.com/upload/ptcom/Vulnerabilities_of_Mobile_Internet.pdf. [Accessed 17 May 2015].

[77] K. Nohl and S. Munaut, "GSM Sniffing," [Online]. Available: http://events.ccc.de/congress/2010/Fahrplan/attachments/1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf. [Accessed 15 May 2015].

[78] B. W. Nyamtiga, A. Sam and L. S. Laizer, "Security Perspectives for USSD versus SMS in conducting mobile transactions: A case study of Tanzania," *international journal of technology enhancements and emerging engineering research,* vol. 1, no. 3, 2013.

[79] J. Liu, S. Jiang and H. Lin, "introduction to Diameter," IBM Developerworks, [Online]. Available: http://www.ibm.com/developerworks/library/wi-diameter/. [Accessed 9 May 2015].

[80] 3GPP, "3GPP TS 29.305: InterWorking Function (IWF) between MAP based and Diameter based interfaces," 3rd Generation partnership Project.

[81] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC Editor, 2008.

[82] M. Cooper, Y. Dzambasow, P. Hesse, S. Joseph and R. Nicholas, "Internet X.509 Public Key Infrastructure: Certification Path Building," RFC Editor, 2005.

[83] Oracle Communications, "The Value of Diameter Signaling in Security and Interworking Between 3G and LTE Networks," Oracle Communications, [Online]. Available: http://www.oracle.com/us/industries/communications/value-diameter-signaling-wp-2106564.pdf. [Accessed 11 May 2015].

[84] A. Hoisa, "Comparision between RADIUS and Diameter," [Online]. Available: http://www.tml.tkk.fi/Studies/T-110.551/2003/papers/11.pdf. [Accessed 12 April 2015].

[85] P. Calhoun, J. Loughney, E. Guttman, G. Zorn and J. Arkko, "Diameter Base Protocol," RFC Editor, 2003.

[86] R. Borgaonkar, *Dirty use of USSD codes in cellular networks*, 2013.

[87] 3GPP, "3GPP TS: Functional stage 2 description of Location Services (LCS)," 3rd Generation Partnership Project.

# APPENDIX A

**Client-server communication using SCTP sockets.**

#SCTP_client.py

```
import sctp
import socket
import binascii
soc = sctp.sctpsocket_tcp(socket.AF_INET)
soc.bind(('127.0.0.1', 2906))
soc.connect(('127.0.0.1', 2905))
print("****************************************")
print("********* This is SCTP Client **********")
print("****************************************")
print("\n")
print("* Sending M3UA ASPUP")
soc.send(binascii.unhexlify('0100030100000008'))
buf = soc.recv(1024)
print("* Received: %s" % binascii.hexlify(buf))
print("\n")
soc.close()

# M3UA_Server.py

import sctp
import socket
import binascii
soc = sctp.sctpsocket_tcp(socket.AF_INET)
soc.bind(('127.0.0.1', 2905))
soc.listen(5)
ear, (ip, port) = soc.accept()
buf = ear.recv(1024)
print("****************************************")
print("********* This is M3UA Server **********")
print("****************************************")
print("\n")
print("* Received: %s" % binascii.hexlify(buf))
print("* Sending M3UA ASPUP ACK")
ear.send(binascii.unhexlify('0100030400000008'))
print("\n")
ear.close()
soc.close()
```

**Recorded interactions between SCTP client and M3UA_Server**

```
sid@buddha:~/Desktop/Thesis_Samples$ python M3UA_Server.py
**************************************
********* This is M3UA Server **********
**************************************


* received: 0100030100000008
* sending M3UA ASPUP ACK
```

```
sid@buddha: ~/Desktop/Thesis_Samples
sid@buddha:~/Desktop/Thesis_Samples$ python SCTP_client.py
**************************************
********* This is SCTP Client **********
**************************************


* sending M3UA ASPUP
* received: 0100030400000008
```

**4-way Handshake**

```
sid@buddha:~/Desktop/Thesis_Samples$ sudo tshark -ni lo sctp
tshark: Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled du
e to running Wireshark as superuser. See http://wiki.wireshark.org/Captur
eSetup/CapturePrivileges for help in running Wireshark as an unprivileged
 user.
Running as user "root" and group "root". This could be dangerous.
Capturing on 'Loopback'
  1   0.000000    127.0.0.1 -> 127.0.0.1    SCTP 82 INIT
1   2   0.000058    127.0.0.1 -> 127.0.0.1    SCTP 306 INIT_ACK
  3   0.000088    127.0.0.1 -> 127.0.0.1    SCTP 278 COOKIE_ECHO
  4   0.000133    127.0.0.1 -> 127.0.0.1    SCTP 50 COOKIE_ACK
  5   0.000290    127.0.0.1 -> 127.0.0.1    M3UA (RFC 3332) 70 ASPUP
  6   0.000325    127.0.0.1 -> 127.0.0.1    SCTP 62 SACK
  7   0.000497    127.0.0.1 -> 127.0.0.1    M3UA (RFC 3332) 70 ASPUP_ACK
  8   0.000521    127.0.0.1 -> 127.0.0.1    SCTP 62 SACK
  9   0.000587    127.0.0.1 -> 127.0.0.1    SCTP 54 SHUTDOWN
 10   0.000607    127.0.0.1 -> 127.0.0.1    SCTP 50 SHUTDOWN_ACK
 11   0.000625    127.0.0.1 -> 127.0.0.1    SCTP 50 SHUTDOWN_COMPLETE
11
```

Connection Established (SCTP 4 way handshake)

Connection Shutdown

## Intercepting SMS protocol messages in wireshark

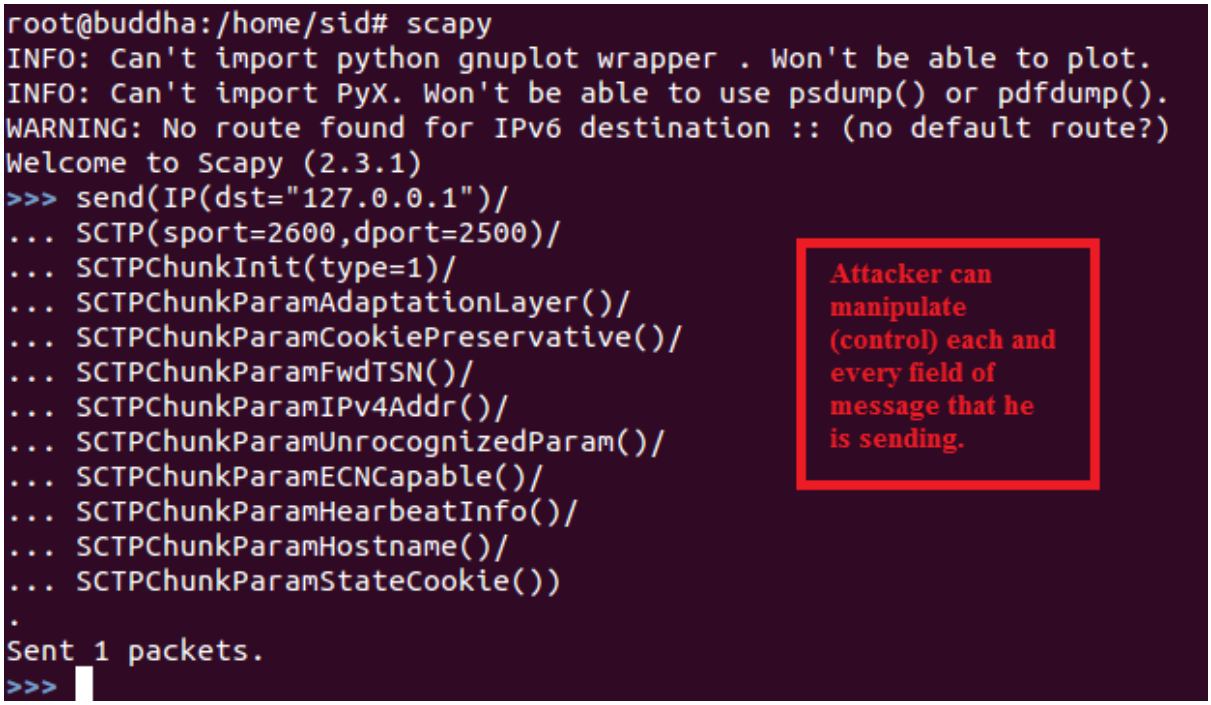
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 18 | 10 | ANSI MAP | 158 | SMS Delivery Point to Point Invoke |
| 2 | 0.026269 | 10 | 18 | ANSI MAP | 146 | SMS Delivery Point to Point ReturnResult |
| 3 | 1.075391 | 18 | 10 | ANSI MAP | 162 | SMS Delivery Point to Point Invoke |
| 4 | 1.099866 | 10 | 18 | ANSI MAP | 122 | SMS Delivery Point to Point ReturnResult |
| 5 | 2.145694 | 18 | 10 | IS-683 | 158 | SMS Delivery Point to Point Invoke |
| 6 | 2.353945 | 10 | 18 | IS-683 | 130 | SMS Delivery Point to Point ReturnResult |
| 7 | 3.395905 | 18 | 10 | IS-683 | 154 | SMS Delivery Point to Point Invoke |
| 8 | 3.673986 | 10 | 18 | IS-683 | 186 | SMS Delivery Point to Point ReturnResult |
| 9 | 4.726220 | 18 | 10 | IS-683 | 170 | SMS Delivery Point to Point Invoke |
| 10 | 4.955802 | 10 | 18 | IS-683 | 130 | SMS Delivery Point to Point ReturnResult |
| 11 | 4.996212 | 18 | 10 | IS-683 | 166 | SACK SMS Delivery Point to Point Invoke |
| 12 | 7.056524 | 10 | 18 | IS-683 | 126 | SMS Delivery Point to Point ReturnResult |
| 13 | 7.096607 | 18 | 10 | ANSI MAP | 178 | SACK SMS Delivery Point to Point Invoke |
| 14 | 7.124739 | 10 | 4 | ANSI MAP | 190 | Registration Notification Invoke |
| 15 | 7.271600 | 4 | 10 | ANSI MAP | 182 | SACK Registration Notification ReturnResult |
| 16 | 7.309235 | 10 | 18 | ANSI MAP | 122 | SMS Delivery Point to Point ReturnResult |
| 17 | 47.276736 | 10 | 4 | ANSI MAP | 166 | Location Request Invoke |
| 18 | 47.479719 | 4 | 10 | ANSI MAP | 186 | SACK Location Request ReturnResult |
| 19 | 63.272333 | 10 | 4 | ANSI MAP | 158 | Transfer To Number Request Invoke |
| 20 | 63.377972 | 4 | 10 | ANSI MAP | 170 | SACK Transfer To Number Request ReturnResult |
| 21 | 63.427134 | 10 | 4 | ANSI MAP | 166 | Location Request Invoke |
| 22 | 63.533011 | 4 | 11 | ANSI MAP | 186 | SACK Routing Request Invoke |
| 23 | 63.536519 | 4 | 11 | ANSI MAP | 170 | Routing Request Invoke |
| 24 | 73.905023 | 4 | 10 | ANSI MAP | 142 | Location Request ReturnResult |

# APPENDIX B

Message manipulation using Scapy.

#Sample code in Scapy to control every field of SCTP message

```
send(IP(dst="127.0.0.1")/
SCTP(sport=2600,dport=2500)/
SCTPChunkInit(type=1)/
SCTPChunkParamAdaptationLayer()/
SCTPChunkParamCookiePreservative()/
SCTPChunkParamFwdTSN()/
SCTPChunkParamIPv4Addr()/
SCTPChunkParamUnrocognizedParam()/
SCTPChunkParamECNCapable()/
SCTPChunkParamHearbeatInfo()/
SCTPChunkParamHostname()/
SCTPChunkParamStateCookie())
```

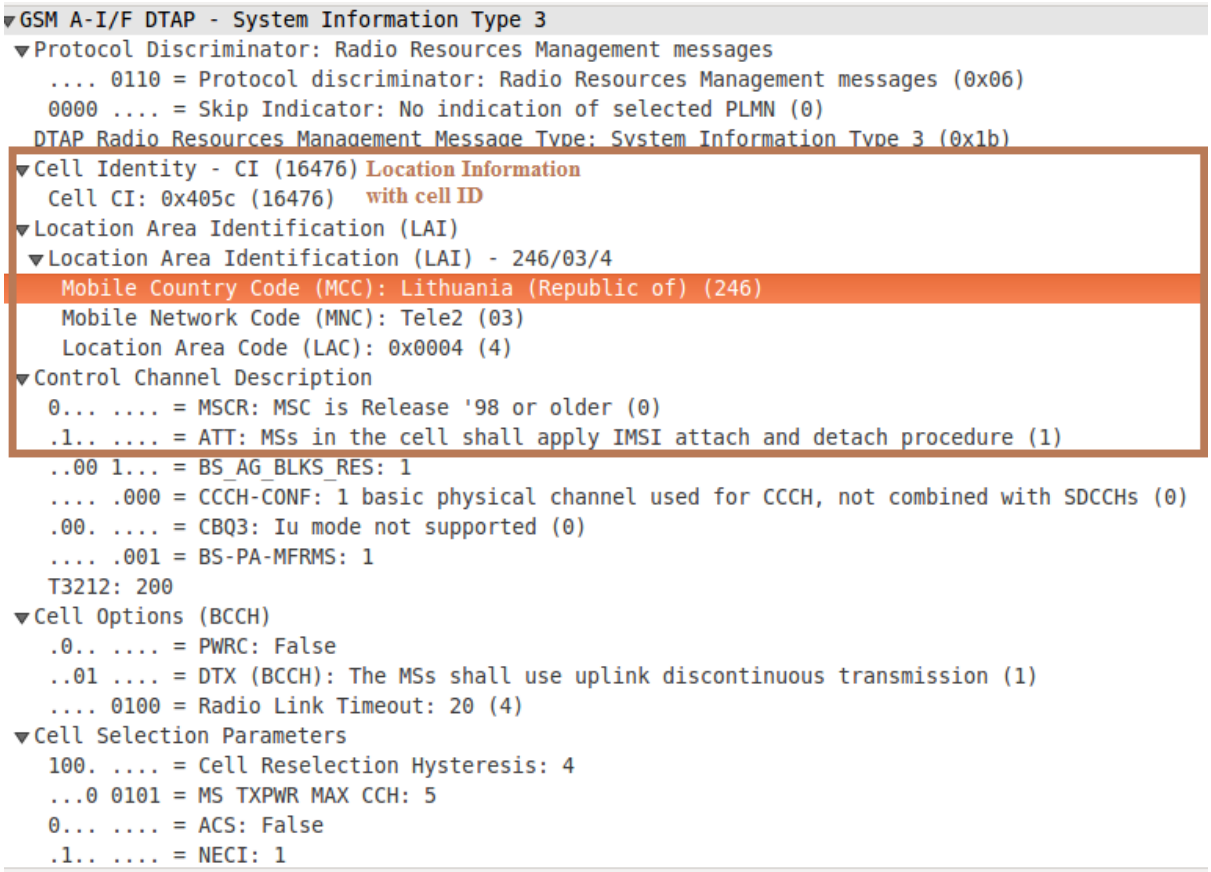


# APPENDIX C

### Disclosure of MSC monitored in Wireshark.

```
▸Frame 1: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits)
▸Ethernet II, Src: AudioCod_03:b3:ef (00:90:8f:03:b3:ef), Dst: Oracle_0a:1a:b0 (00:03:ba:0a:1a:b0)
▸Internet Protocol Version 4, Src: 172.16.128.154 (172.16.128.154), Dst: 172.16.128.51 (172.16.128.51)
▸Stream Control Transmission Protocol, Src Port: m2ua (2904), Dst Port: m2ua (2904)
▸MTP 2 User Adaptation Layer
▸Message Transfer Part Level 3
▾Signalling Connection Control Part
  Message Type: Unitdata (0x09)
  .... 0000 = Class: 0x00
  0000 .... = Message handling: No special options (0x00)
  Pointer to first Mandatory Variable parameter: 3
  Pointer to second Mandatory Variable parameter: 7
  Pointer to third Mandatory Variable parameter: 11
 ▾Called Party address (4 bytes)
  ▾Address Indicator
    0... .... = Reserved for national use: 0x00
    .1.. .... = Routing Indicator: Route on SSN (0x01)
    ..00 00.. = Global Title Indicator: No Global Title (0x00)
    .... ..1. = SubSystem Number Indicator: SSN present (0x01)
    .... ...1 = Point Code Indicator: Point Code present (0x01)
   ..00 0000 0000 1010 = PC: 10
   SubSystem Number: MSC (Mobile Switching Center) (8)
   [Linked to TCAP, TCAP SSN linked to GSM_MAP]
 ▾Calling Party address (4 bytes)
  ▸Address Indicator
   ..00 0000 0001 0010 = PC: 18
   SubSystem Number: Reserved for international use (ITU only) (12)
   [Linked to TCAP]
▾ANSI Transaction Capabilities Application Part
```

### Disclosure of location ID




### Sample codes of unwired labs location API

```
# Sample Request of MS1

{
    "token": "101472503351",
    "radio": "gsm",
    "mcc": 244,
    "mnc": 12,
    "cells": [{
        "lac": 123,
        "cid": 1650204
    }],
    "address": 1
}

# Sample Response for the requested cell information

{
```

```
    "status": "ok",
    "balance": 44,
    "lat": 60.187519,
    "lon": 24.838402,
    "accuracy": 959,
    "address": "Unnamed Road, 02150 Espoo, Finland"
}
```


```
# Sample request for MS2 using 3rd party API

import requests

url = "http://eu1.unwiredlabs.com/v2/process.php"

payload = "{\"token\": \"101472503351\",\"radio\": \"gsm\",\"mcc\":
244,\"mnc\": 5,\"cells\": [{\"lac\": 29120,\"cid\":
278766}],\"address\": 1}"
response = requests.request("POST", url, data=payload)

print(response.text)
```