

**DETECTION OF SIGNALING SYSTEM NO.7 (SS7)
ATTACKS, TRAINING SNORT-NIDS OVER
MALICIOUS TRAFFIC PATTERNS FROM SS7 ATTACK
SIMULATOR IN WIRESHARK**



By

Lt Hafiz Muhammad Shafeeq PN

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfilment of the requirements for the degree of MS in Information Security

September 2019

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere

Dedication

This research is dedicated to the martyrs of Pakistan Navy

Acknowledgement

Foremost, I would like to convey my humble gratitude to my mentor and supervisor, Brig Imran Rashid, PhD, for his kind supervision and continuous supportive guidance. His immeasurable patience, prudent approach and practical knowledge helped me steer in the right direction. Also, I am grateful for support and insightful comments from my committee members; Asst Prof Dr Shahzaib Tahir and Asst Prof Mian Muhammad Waseem Iqbal.

I am indebted to my seniors Lt Cdr Zafran Khan PN and Lt Cdr Kaleem Ullah PN for being a positive source of motivation and guidance during different phases of this degree. Furthermore, my sincere regards to Ms Syeda Kinza Saeed Kazmi for her priceless support, unfailing encouragement and strengthening faith in myself during difficult times at the college.

Last but not the least, I would like to acknowledge the endless support and prayers from my wife Dr Kinza Hayat.

Abstract

In 1970s, roaming interconnection for cellular networks was designed for a few trusted parties without considering security as a major concern. Today same decades-old SS7 (Signalling System No 7) is a pillar for many roaming interconnections. Walled technology of SS7 has been proven as vulnerable to serious threats due to deregulation, expansion and confluence with IP-based LTE networks. Security researchers have recently demonstrated that vulnerabilities of roaming interconnections are being widely misused for gaining access to the core network. Although, LTE (Long Term Evolution) and Diameter Signaling promised high-speed data roaming and enhanced security over the air to keep abreast with the latest attack vectors, inherent flaws of roaming interconnection are still there. This thesis gives an insight of common attacks on SS7/Sigtran and compares SS7 with its successor Diameter protocol focusing security. It provides analysis of SS7 attack traffic in Wireshark (packet capture tool) for malicious patterns to create rules in Snort IDS (Intrusion Detection System) for detection of common attacks.

Contents

1	Introduction	1
1.1	Evolution of Mobile Telecommunication	1
1.2	Signaling and SS7	2
1.3	Motivation	3
1.4	Problem Statement	4
1.5	Research Objectives	5
1.6	Contributions	5
1.6.1	Relevance of the Topic to National/Military Needs	5
1.6.2	Advantages	6
1.7	Thesis Outline	6
1.8	Summary	7
2	Literature Review	8
2.1	Background	8
2.1.1	How SS7 Network became Vulnerable?	9
2.1.2	How Vulnerable is the SS7 Network?	10
2.2	Related Research	11

2.2.1	Limited Research by Academia	11
2.2.2	Less Attention by General Public	12
2.2.3	Summary of Related Work	13
2.3	Summary	17
3	SS7 and Diameter - A Comparison	18
3.1	SS7 Signaling	18
3.1.1	SS7 MAP Message Classification	20
3.2	Diameter Signaling	21
3.2.1	Considering Security in Diameter Design	22
3.2.2	Limitations in Diameter Security	24
3.3	Comparing Protocol Stacks	27
3.4	Comparing Attack Ratio in Diameter and SS7 [89]	28
3.5	Summary	28
4	Implementation of Malicious Traffic Filter with Snort and Wireshark	29
4.1	Intrusion Detection Systems	29
4.1.1	Introduction	29
4.1.2	Intrusion Detection Systems (IDS) Types	30
4.1.3	Detection Based on Anomalies	30
4.1.4	Signature-Based Detection	31
4.1.5	Snort-IDS	31
4.2	Packet Sniffing and Analysis	32
4.2.1	Wireshark	33

4.3	Simulation and Testing Environment	33
4.4	SS7 Attack Simulator	34
4.4.1	Simple Mode	34
4.4.2	Complex Mode	35
4.5	Proposed Detection Scheme	35
4.5.1	Attack No 1: Interception of SMS Attack	35
4.5.2	Attack No 2: anyTimeInterrogation Attack	42
4.5.3	Attack No 3: provideSubscriberInformation Attack	43
4.6	Results	44
4.7	Summary	45
5	Conclusion	46
5.1	Future Work	48
5.1.1	Extending Functionality of Attack Simulator	48
5.1.2	New Snort Rules with Real SS7 Traffic	48
5.1.3	Integration of SCTP in Snort	48
	References	49

List of Figures

1.1	Evolution of Mobile Phone Technology	1
3.1	SS7 Network Components	20
3.2	Comparison of SS7 & Diameter Stack	27
4.1	Sample of a basic Snort Rule for ICMP attack detection	32
4.2	Intercept SMS Attack Traffic Simulation by SS7 Simulator	35
4.3	Identification and Analysis of Attack Packets captured in Wireshark . . .	36
4.4	Signatures Derivation from Attack Packets after analysis in Wireshark .	37
4.5	Addition of Custom Rules to Snort Configuration File	37
4.6	SS7 Normal SMS Delivery Procedure	38
4.7	SS7 SMS Interception Attack	38
4.8	Wireshark Captured Sequence of Attack Packets	39
4.9	Validating Snort Configuration after the addition of new Rules	40
4.10	Parallel listening of Snort and Attack Simulation on Lo Interface	41
4.11	Parallel Attack Simulation and Detection	41
4.12	How <i>ATI</i> signaling message is exploited	42
4.13	SS7 Attack using <i>ATI</i> signaling message	43

4.14 How <i>PSI</i> signaling message is exploited	43
4.15 SS7 Attack using <i>PSI</i> signaling message	44

List of Tables

2.1	Summary of related work	13
3.1	Categorization of MAP Messages used in attacks	21
3.2	Percentage of Vulnerable Networks (2017)	28
4.1	Comparing results for all attacks detected	44

List of Abbreviations and Symbols

Abbreviations

2/3/4/5G	2nd/ 3rd/ 4th/ 5th Generation
3GPP	3rd Generation Partnership Project
AAA	Authentication-Authorization-Accounting
AT&T	American Telephone & Telegraph
ATI	Any Time Interrogation
AVP	Attribute Value Pairs
CAMEL	Customized Applications for Mobile networks Enhanced Logic
CAP	CAMEL Application Part
CCS	Common Channel Signaling
CHAP	Challenge Handshake Authentication Protocol
COO	Change-Over Order
DoS	Denial of Service
DNS	Domain Name System
EAP	Extensible Authentication Protocol

GSM	Global System for Mobile
GT	Global Title
GTT	Global Title Translation
GUI	Graphical User Interface
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IAM	Initial Address Message
ICMP	Internet Control Message Protocol
IMSI	International Mobile Subscriber Identity
INAP	Intelligent Network Application Protocol
IP	Internet Protocol
IPSec	IP Security
ISUP	Integrated Services Digital Network User Part
ITU-T	International Telecommunication Union - Telecommunication
IWF	Interworking Function
LTE	Long Term Evolution
MAP	Mobile Application Part
ML	Machine Learning
MS	Mobile Station

MSC	Mobile Switching Center
MSISDN	Mobile Subscriber Integrated Services Digital Network
MTP	Message Transfer Part
MVNO	Mobile Virtual Network Operators
NAI	Network Access Identifier
NCAS	Non-Call Associated Signaling
NDS	Network Domain Security
NFAS	Non-Facility Associated Signaling
NIDS	Network Intrusion Detection System
OS	Operating System
P2P	Peer-to-Peer
PAP	Password Authentication Protocol
PKI	Public Key Infrastructure
PSI	Provide Subscriber Information
PSTN	Public Switched Telephone Network
SCP	Service Control Point
SCCP	Signaling Connection and Control Part
SCTP	Stream Control Transmission Protocol
SIGTRAN	Signaling Transport
SIP	Session Initiation Protocol

SRVLOC	Service Location Protocol
SMS	Short Message Service
SMSC	Short Message Service Centre
SP	Signaling Point
SS7	Signaling System No.7
SSH	Secure Shell
SSP	Service Switching Point
STP	Service Transfer Point
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
Telnet	Teletype Network
TFP	Transfer Prohibit
TLS	Transport Layer Security
TSTF	Telecom Security Task Force
TUP	Telephone User Part
UMTS	Universal Mobile Telecommunication System
USSD	Unstructured Supplementary Service Data
VLR	Visitor Location Register
VM	Virtual Machine
VoIP	Voice-over IP

Introduction

1.1 Evolution of Mobile Telecommunication

Mobile networks grew significantly and importantly over the last three decades and became an integral part of today's communication infrastructure. Since the beginning, small-size hand-held devices, seamless roaming, affordable and low rates with wide coverage area are the prime factors for their greater popularity. It has become the most basic necessity of life and without a mobile device in pocket, life seems unimaginable. Four decades ago, it was a luxury to have a 1G mobile phone and now a 4G device is a must-to-carry item in our daily life.

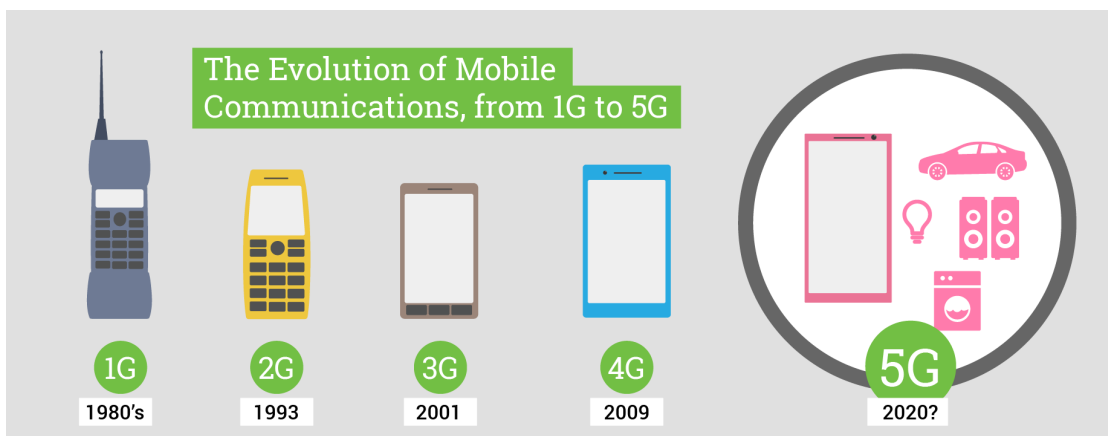


Figure 1.1: Evolution of Mobile Phone Technology

Mobile telecommunication technology is the foundation of business needs, emergency services, public requirements, military and rescue operations. Affordable, low-priced and attractive smart phones with millions of new applications led to the vast increase in the number of mobile users. Mobile broadband subscriptions surpassed 5 billion globally by the end of 2017 [1]. The number of 4G subscriptions are predicted to reach 3.1 billion in number by the end of 2019 [2].

1.2 Signaling and SS7

In telecommunication networks, function of a signaling system is to set up a call, manage the communication process and then tear down it once two devices try to disconnect over the air. It is regarded as the back bone technology of mobile telecommunications which makes it possible to connect and handle the two connecting ends [3][4]. SS7 is the main Signaling System globally, designed five decades ago dating back to 1970s, when only a few national/ multinational operators were providing telecommunication services and had core network access [3][4]. Since then, SS7 is in use for: [5][6][7]

- Number translation
- Call establishment and termination process
- Mobility management (MM)
- User security information
- Short message service (SMS)
- Billing information and prepaid billing
- Access/service authorization
- And other intelligent services

Considering the mutual trust between operators which were already very few in number, no inherent security or authentication controls were incorporated in SS7 core network at the time of designing [8]. Operators being national/ multinational corporations were considered and assumed to be trustworthy, making SS7 network as a walled-park [9][10]. Merger of IP networks based on packet-switching and telephone networks based on circuit-switching, attracted more subscribers, brought more competition and expansion creating high demands and allowing new competitors to enter the market. Due to expansion and introduction of newer technologies to support the increasing demands of the users, number of entry points to core network and interfaces with legacy SS7 network increased as an explosion, which multiplied number of operators entering the network [11].

Throughout the world, major national/ multinational corporations maintained their control over the provision of telecommunication services for two decades till the end of 90s. With the rolling out of 2G, Mobile Virtual Network Operators (MVNO) and smaller companies started offering their services to customers after being legally allowed to be a part of the game with the help of de-regulation in United States and Europe in 1996 and 1998 respectively [12]-[14]. Motive behind the de-regulation was to remove restrictions on the network and help it expand further to accommodate the flooding numbers of users on daily basis.

1.3 Motivation

The real motive behind choosing of this research direction is the continuously pressing performance requirements that modern networks impose on security devices. Hackers can exploit the signaling vulnerabilities to [24]:

- Intercept messages/ tape and redirect calls
- Track a subscriber's location

- Steal information about network and subscribers

An average script-kiddie has access to such techniques, what to talk of intelligence agencies [16]. These techniques have put public privacy, safety, security and money at stake. GSM and UMTS is based on SS7 network [18]. As 4G/LTE is replacing older technologies and telecommunication networks are using newer protocols like Diameter, the question is whether efforts to secure SS7 are still required? [19] As of 2017, SS7 network makes 87% of the total telecommunication networks throughout the world, supporting backward compatibility for newer technologies [9]. Signaling system number 7 is expected to continue playing an important role for the next ten to fifteen years as this type of signaling will only be substituted when all the global trunks will start using VoIP protocols like SIP and DIAMETER or when TCP / IP will provide voice services of end-to-end connectivity.

Keeping in view the current cyber threat environment and state of SS7 vulnerabilities, there is a dire need to carry out further research and focus this issue to help protect the privacy of general public and ensure safety of individuals. Attackers can bring losses to network operators amounting to billions, it is equally important for operators to help close these holes of the once "walled-garden".

1.4 Problem Statement

Switching to the IP technology and deregulation has made it reasonably trouble-free for third parties to gain a way-in to the once protected SS7 network. Inherently absent security controls paved way for severe attacks for subscribers such as tracking of their location and their calls and SMS interception. SS7 will remain as a backbone of telecommunication for a long time as it will be replaced with the world wide usage of VoIP protocols. Considering the above statement, a never-ending process of counter-measures, needs to be deployed.

1.5 Research Objectives

Objectives and goals for this research work are:

- Identification of common attacks in Signaling System No.7 (SS7).
- Review newer signaling protocol Diameter and its predecessor SS7 with respect to security and inherent flaws.
- Detection of malicious SS7 traffic configuring Snort-NIDS and Wireshark.

1.6 Contributions

Contributions of this work is summarized as under:

- It reviews all the available literature with respect to SS7 security issues and countermeasures.
- This research work gives a brief introduction of Signaling System Number 7 and Diameter Signaling protocols, comparing both with respect to security.
- It discusses Intrusion detection and Packet sniffing in detail with the help of examples of Snort and Wireshark, the tools used in this work.
- It proposes a methodology for rule based filtration of specific SS7 MAP messages with the help of Wireshark and Snort over simulated SS7 traffic dataset.

1.6.1 Relevance of the Topic to National/Military Needs

This work is in relevance to the National/Military needs of the hour considering the following:

- Location tracking can harm all troops deployed at seas especially of the Naval Fleet, at land guarding important sites or airmen deployed on air surveillance.
- SMS interception can leak information of classified nature.
- Law enforcement agencies can face problems w.r.t apprehension of criminals.
- Personal subscriber information can be stolen using these vulnerabilities.
- This work can help counter all such threats to National/ Military assets.

1.6.2 Advantages

Following are few of the advantages of this work:

- Law enforcement agencies can plug these communication holes for improved security.
- Armed forces may secure their troops deployment and information assets.
- Operators can work on the implementation and security flaws to help improve their subscribers data.

It is need of the hour to gear up ourselves against signaling vulnerabilities and help understand major attacks recently carried out using these exploits. These exploits need safeguard before our enemies use them for a catastrophic attack. We should prepare ourselves to use it in our advantage at state level rather than falling prey to it. This thesis will help us understand vulnerabilities of SS7 and design safeguards against these vulnerabilities.

1.7 Thesis Outline

This research work has been divided into five chapters:

- Chapter 1: This chapter introduces the topic and problem statement, describes research objectives and importance to national military needs. It also highlights contributions of this research.
- Chapter 2: This chapter covers background, vulnerabilities of SS7 and literature review of the topic in detail.
- Chapter 3: This chapter gives a brief introduction of SS7 Signaling and its MAP message classification w.r.t threats. It further introduces Diameter protocol and highlights Security considerations in its design. Current limitations in security of Diameter are also discussed. Protocol stacks and Common attack ratio of both the protocols is also compared.
- Chapter 4: It provides an introduction of intrusion detection systems and their types with the example of Snort IDS tool used in the research. It further highlights packet sniffing and analysis with the example of Wireshark, second tool used in research. Last part of the chapter gives a detailed working of proposed detection methodology using both the tools with the help of scree-shots of actual implementation.
- Chapter 5: This chapter concludes the report and proposes a few directions for future work.

1.8 Summary

This chapter gives an overview of how the mobile telecommunication evolved and a brief introduction of Signaling and SS7. It further highlights Motivation, Problem Statement, Research Goals, Contributions, Relevance of the Topic to National/Military Needs, Advantages and Outline of the thesis.

Literature Review

2.1 Background

Security of telecommunication networks has always been a prime concern as these networks are complex systems comprising of various twisty sub-systems. Each one of these sub-systems are made up of diverse technologies and hardware. Legacy components and sub-systems shall continue to exist for the next few decades to come, one should not forget that security of the entire system or network relies upon the defense of most fragile part, connection or collaborator.

Placement of voice calls is still carried out with the help of signaling messages of SS7 even in the contemporary mobile networks. Prior to the existence of SS7, a speaking channel used to transfer the service commands for the delivery of data packets and establishing the connection for subscribers. Around 40 years ago, this method was replaced after appropriate up-gradations worldwide with the globally recognized signaling system standard(SS7). At the time of deployment of SS7 network a small number of telecommunication network operators were running the show, making the telephone companies to place trust in one another and to believe that no malicious games can be played on such a small scale of closed networks. During that era of communication, channels and hosts were being physically secured as per security protocols, making it

unfeasible for a remote in nature, illegitimate host, to gain a way-in to the system of signaling.[24].

When the network was closed and castled, it enjoyed an inherent sense of security which required no guards or checks. Small in number and well-trusted networks provided the signaling messages a sense of legitimacy and reliability. Considering the above scenario, the network had no security mechanisms especially with crypto-graphic means to verify the originality of messages. An in-bound signaling message would not have been verified then, for its source. Added to this, there was no replay-protection or prevention of an illegal party from re-sending a signaling message at later intervals which has already been acknowledged/ approved to try and re-create an already performed action. And thus for years, subscribers or operators did not feel unsafe or at risk, because of the walled-network [25].

2.1.1 How SS7 Network became Vulnerable?

As the time goes by, walls built on trust are breached. SS7 gets exposed to a large number of known and unknown threats and vulnerabilities degrading the overall security of the telecommunication networks and compromising privacy of subscribers. Assuagement in governing regulations and alleviation in laws for telecommunication market in the mid of 90s to expand the networks, fulfilling the ever-growing demands started paving the way for an unaccounted for and easy way-in for untrusted parties and even to share or own a part.

Mobile connection and service support forced the network to advance in order to come together and at par with the new standards. Early 21st century witnessed development of a new set of signaling transport protocols namely Signaling Transport or SIGTRAN. It is an extension for the legacy SS7, which utilizes IP-based networks for message-transfer and with this revolutionary yet unwanted advancement the signaling network stopped being hard-to-find for intruders. Efforts to unite other networks with SS7 for

the elimination of inter-operability issues paved way for increase in entry-points to walled-network. Consequently, an attacker can now carry-out a multitude of attacks by sending, intercepting and altering SS7 signaling messages using all the entry points and opportunities created by these advancements.[26].

Much needed requirement of mobility in telephones brought new services on-board. In this regard, a considerable number of signaling messages have been developed to aid the mobile networks in the provision of desired services. The absence of cryptographic security mechanisms guarding SS7 network entry-points caused a number of these lawful signaling messages being exploited. In addition to this, new applications like Short Message Service (SMS) and intelligent-network services brought additional signaling messages and burden thereby increasing the probability of causing more harm or create more holes in the already un-protected SS7 walls.

2.1.2 How Vulnerable is the SS7 Network?

Flaws in the security of SS7 were started to surface in the community of security researchers and network operators just a few years back. Security experts started reporting these flaws and even gave live demonstrations [42]. In 2001 a researcher namely L. Ostman highlighted SS7 vulnerabilities [27], and in 2000, a year before that, US government had already expressed their grave concerns regarding these issues [28]. E. J. Snowden, a US security whistle-blower claimed in 2013 that NSA was exploiting SS7 as one of their many techniques to collect public information. He leaked documents of NSA, classified in nature, claiming that United States is collecting an estimated five billion records per day mainly because of exploiting these signaling vulnerabilities [21]. As per renowned media corporation 'Bloomberg' [29], spying services were being openly offered by many agencies such as 'Verint Systems' and 'Defentek' and all because of the exploitation of SS7 signaling messages. Another whistle comes from Hacking Team (Italian spy-ware maker) in which they claimed to have received similar

offers from the Bulgarian company namely Circles and Israeli start-up namely Clever-Sig. Unfortunately, this was revealed only after the hacking of cyber-group in which more than 400 GBs of data was leaked online from their servers [22]. US based security expert Bruce Schneier is said to have claimed that the UK-based company namely Cobham offers unauthorized location-discovery service and that too with up-to a meter or two in precision inside more than a dozen countries. [31] This clearly shows that the legacy SS7-based exploitation & spying market is rapidly growing, compromising subscribers worldwide.

Apart from private sectors of security, these security vulnerabilities of SS7 have been highlighted in U.S. governmental bodies, for example in April 2016, an oversight committee was called for investigation into SS7 vulnerabilities by renowned US congressman Ted Lieu and raised his deepest concerns in the US-Congress. [20]

In a more recent and horrific in nature attack, a major bank of UK "Metro Bank" fell prey to a cyber attack in Jan 2019, where attackers managed to exploit SS7 vulnerabilities and intercepted transaction verification text messages of many customers which the bank used as a method for Two-factor authentication [17].

2.2 Related Research

2.2.1 Limited Research by Academia

Convergence of new technologies and deregulation resulted in realization that core network is no more a trusted network which triggered work on its vulnerabilities and defenses. Even after this realization, SS7 vulnerabilities and exploits have not been widely published or well-known because of complex cellular networks, intricate protocols and hidden network interfaces [15]. Therefore these attacks draw less attention of general public as compared to other vulnerabilities of cellular networks. Following points are considered some of the contributing factors to limit the amount of research by academia:

- No access to real-time SS7 network due to privacy and legal issues.
- Non availability of any open source simulator or test-bed to simulate these vulnerabilities, provide proof of concept for exploitation and then implement defences to bridge these vulnerabilities.
- Less interest of network providers as it did not affect their earnings because of no public perception of threat.

2.2.2 Less Attention by General Public

Complex nature of unseen networks and intricate unheard protocols are the major reason why these attacks are not globally covered or well-known among the masses. These networks are hidden in nature thereby providing the least opportunity and interest to general public as compared to other network systems and their vulnerabilities. It is need of the hour to create and augment an understanding among subscribers and service providers about harmful vulnerabilities of cellular networks, the current counter-measures in place and encouragement to desired researchers for more work in this area for the better security of 5th and beyond Generations networks.

Most of the time, it is thought that security breaches of the aforementioned nature are extremely complex, expensive to carry-out and are achieved only by some great hackers or a notorious agency with professional excellence or as part of a well-thought and organized crime. These perceptions are spread due to general public's limited access to the true nature of telecommunications networks. These networks are in reality complex systems built on top of twisty sub-systems and each one having a different level of technology, hardware and safeties. This tells that the security level of the weakest link in chain defines the security level of system, and attackers exploit that weakest spot.

2.2.3 Summary of Related Work

A brief summary of the related work is given below:

Table 2.1: Summary of related work

Reference	Year	Summary
G.Lorenz et al [7][32]	2001	Due to advancements in technology, and as SS7 backbone is being merged with internet and wireless communications, attack vectors are increasing in numbers. It presents attack taxonomy and highlights that if an attacker has gained access to SS7 core network, various databases and customer's record stored in SS7 core network can be changed/ deleted. It further highlights the probability of signaling packet sniffing and spoofing due lack of authentication in SS7 network.
H. Sengar et al [4] [34]	2005, 2006	It reviewed the effects of exploiting network management messages (Change-over Order (COO) message and Transfer-Prohibited (TFP) message discussed in [4]). It shows how various signaling links can be declared unavailable and how traffic can be diverted away from these links. This shows how Denial of Service for a particular destination is created, how congestion of the network by routing all the traffic through a single link can be caused, how interception by routing traffic through a particular node under can be performed and a how efficiency can be decreased by routing all the traffic from farthest possible route.

H. Sengar et al [35]	2006	It focuses on issues and security features of SS7 and IP protocols as interconnections. It highlights how vulnerabilities are generated by SIGTRAN protocol and proposes solution to mitigate these vulnerabilities with the help of screening of incoming/outgoing signaling messages, access control and use of anomaly detection techniques [53].
Philippe Langlois [36]	2007	In his talk delivered at BlackHat Convention (BH) [54], 2007, P. Langlois (Telecom Security Task Force (TSTF)) focused on looking for entry points and gaining access to SS7 core network. It further highlights vulnerabilities emerging due to merger of SS7 and IP networks. It also showed that SCTP is vulnerable to simple attacks.
Tobias Engel [33]	2008	Tobias Engel, an expert from Berlin-based security corporation Sternraute showed that location can be disclosed and spam messages can be sent if SS7 network is accessed.
Lingling, Jiang and Ma Hong [37]	2009	Authors discussed effects of exploiting Initial Address Message (IAM) at application layer and Changeover Order (COO) network management message at MTP3 layer.
An Xinyuan et al [38]	2011	It shows how network management messages can be exploited and also focuses on having a solution to identify the counterfeit messages.
P-Olivier & A-De Oliveira [39]	2014	Security experts from P1 labs present a talk in Hackito Ergo Summit [40] (2014) where they explain/ demonstrate user location tracking and how spoofed messages can be used.
Karsten Nohl [41]	2014	Karsten Nohl from Security Research Labs showed how access to SS7 network makes the interception of phone calls and messages possible, in Chaos Communication congress [40] 2014.

Tobias Engel [42]	2014	In Chaos Communication congress 2014, Tobias Engel gives a live demo of location tracking and DoS attacks with access to SS7 network. He also explains several other attacks.
Positive technologies [43]	2014	In December 2014, experts at Positive technologies issued a white paper based on their research which concluded that if an attacker gains access to SS7 network, many of the attacks are possible. Positive technologies also offered their products PT IDS-SS7 and PT SS7 scanner for mitigation of these vulnerabilities.
S.P Rao et al [15]	2015	It gives an overview of SS7 location tracking attacks with detailed methods to accomplish these attacks. It recommends a generic approach and suggests better practices to safeguard the network from a probable attack. It further gives a brief report on entry points of SS7.
S.P Rao [44]	2015	It shows how exploiting MAP messages can lead to a number of attacks. It further explains the method of accomplishing these attacks.
Hassan Mourad [10]	2015	An overview of possible attacks on SS7 is given by a white paper published by SANS institute. It also suggests how critical security controls can be used for better protection of SS7 network.
D-Kurbatov & V-Kropotov [6]	2015	Experts at Positive Security, D. Kurbatov and V. Kropotov present a talk in 2015. They explained entry points of SS7 and explained/demonstrated few attack scenarios.

<p>Kristoffer Jensen[45] [46][47]</p>	<p>2016, 2017</p>	<p>Jensen presented a brief overview of SS7 attacks, with a brief note on SS7 core network entry points. he focused on the use of ML algorithms to detect SS7 attacks. Using one type of MAP messages, he presented a simulated prototype to detect attacks through ML techniques. His major addition to SS7 research was introduction of an open source simulator named as “SS7 Attack Simulator” [48] to produce simulated SS7 normal and abnormal traffic.</p>
<p>S. Holtmanns et al[51]</p>	<p>2016</p>	<p>Holtmanns shows that SS7 vulnerabilities also threaten LTE users in addition to GSM/UMTS subscribers. Because of internetworking functionality, these vulnerabilities can be used for tracking LTE subscribers using Diameter protocol [52]. These attacks are based on a few assumptions such as no IPsec is in use between internetworking nodes, IP address filtering is not in use, no sanity check is being performed by receiving node, Mobile Station International Subscriber Directory Number (MSISDN) of victim and address of the edge node are known to attacker.</p>
<p>M. Savadatti and D. Sharma [49]</p>	<p>2017</p>	<p>It simply presents an overview of signaling system No.7 with a brief discussion of SS7 attacks. It gives no details of methods to carry out these attacks.</p>

S. Puzankov [50]	2017	Stealthy attacks resulting due to SS7 vulnerabilities are discussed by Puzankov. He feared that due to misconfiguration errors, SMS home routing can be bypassed and IMSI of the subscriber can be disclosed helping in launch of further sophisticated attacks. Stealthy location tracking is possible with the help of by silent USSD notification instead of silent SMS as silent USSD notification is not stored in user account whereas silent SMS is stored in user account. For a long time, short messages can be intercepted in a stealthy way. Using fake MSC, an attacker can register himself in a network while VLR remains the legitimate, in this way legitimate MSC is used for voice calls and short messages whereas fake MSC is used for interception of incoming messages.
---------------------	------	--

2.3 Summary

This chapter gives the background of the SS7 and how it became vulnerable to the present day vulnerabilities. It discusses reasons for limited research in this area and reviews in detail all the available literature on SS7 security flaws.

SS7 and Diameter - A Comparison

SS7 is the most widely used signaling protocol on the interconnection network in both 2G and 3G cellular systems. Diameter is gradually replacing SS7 protocol [55] in 4G systems. On the other hand, regardless of billions spent on the up-gradation of a protocol from 70's era (SS7) to a new generation protocol (Diameter), flaws exist making Diameter equally vulnerable to eavesdropping, tracking, fraud, theft and attacks that plagued its predecessor for years. This chapter briefly compares the two signaling protocols.

3.1 SS7 Signaling

American Telephone & Telegraph (AT&T) created a signaling protocol in the 1975, the protocol was an execution of the Common Channel Signaling (CCS) standard enabling the signals to be routed on a different passageway from that of the voice feed [56, 57]. AT&T's signaling protocol was given the status of a standard in the mid of 1980s by Consultive Committee for International Telephony and Telegraphy (now recognized as ITU-T) which at present has been deployed worldwide on the telecommunication network. SS7 was put into design to make the telecommunication networks more efficient and making certain the appropriate exploitation of network resources. SS7 is an out-

of-band protocol for signaling which means that it allows telecommunication points to send/ receive management information over a channel which is different than voice carrying channel.

Primarily, this signaling system was proposed to work as a call-associated signaling network, to set up, maintain and break up telephone calls over the Public Switched Telephone Networks (PSTN) network. Advancements in technology and subscriber demands paved way for further developments in this standard. North America and Europe deployed these advancements of SS7 application protocols such as Integrated Services Digital Network User Part (ISUP) and Telephone User Part (TUP), respectively [58]. Presently the signaling network offers potential to transmit Non-Facility associated signaling (NFAS) and Non-Call Associated Signaling (NCAS)[57, 58]. NFAS makes it possible to carry out signaling when a call is already set-up. Some of the Non-Call-Associated Signaling services are:

- Short Message Service
- Administration of the mobility services and
- Network services intelligent in nature.

The SS7 network is based on three fundamental nodes as shown in Figure 3.1.

SS7 links connect these nodes with each other which are also recognized as Signaling Points (SP). Service Switching Point (SSP) is a component for signaling which places the Mobile Station (MS) over signaling network. Special software capable of originating, switching and terminating calls is loaded into these SSP switches. Service Control Point (SCP) is a signaling point which contains routing information available to be accessed by signaling messages originating from the SSPs. Special software is designed and developed to transmit the routing data over the network and is then loaded into SCPs. This software allows routing information to be fetched from telecommunication databases and sent to other signaling points. To facilitate the call processing SSPs re-

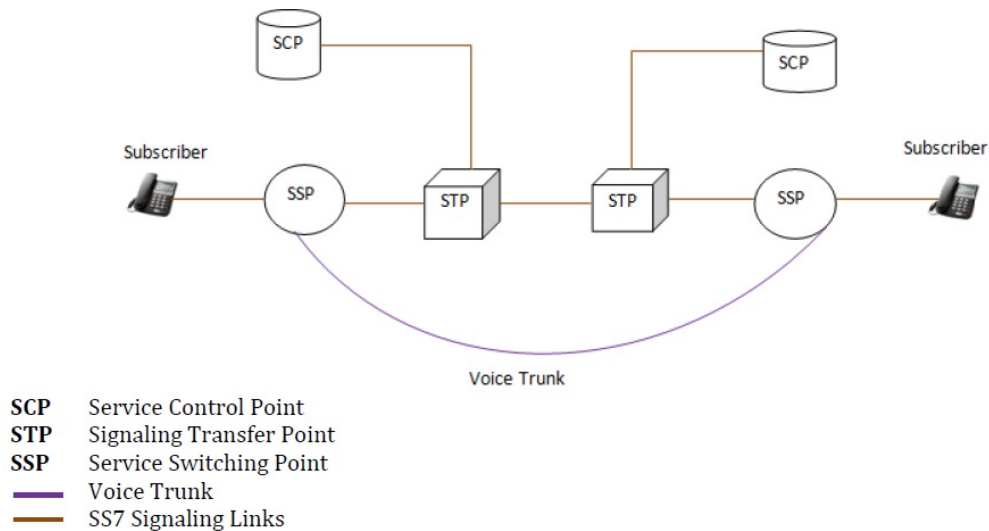


Figure 3.1: SS7 Network Components

quest for information from SCPs in the form of database queries. Third signaling point also known as routers of SS7 network at times is called Signaling Transfer Point (STP). It acts as a liaison connecting SSPs & SCPs. STPs route incoming messages towards the specified destination instead of originating or terminating signaling messages. STPs can be deployed as standalone or integrated STPs as required [59]. The role of both SSP and STP is combined in an integrated STP; when acting as SSP it generates database queries and when acting as a role of STP it sends messages of query to SCP.

3.1.1 SS7 MAP Message Classification

GSMA IR.82 categorizes SS7 MAP messages in three categories based on:

- Messages which are solely for home network elements and need no external exposure.
- Messages not required for own Home network but can be sent externally for visited networks where subscriber is registered.
- Legitimate external exposure as these messages are sent from visited network to Home network.

Based on this, a classification of SS7 MAP messages used in publicly disclosed attacks is given below [45]

Category	Signaling Message	Attack Type
I	<i>sendIdentification</i>	Interception
I	<i>anyTimeInterrogation</i>	Tracking
I	<i>anyTimeModification</i>	Tracking
I	<i>provideSubscriberLocation</i>	Tracking
II	<i>insertSubscriberData</i> and <i>gsmSCF</i>	Interception(Outgoing)
II	<i>insertSubscriberData</i>	DoS
II	<i>deleteSubscriberData</i>	DoS
II	<i>provideSubscriberInformation</i>	Tracking
III	<i>sendAuthenticationInformation</i>	Interception
III	<i>registerSS - eraseSS</i>	Interception(Incoming), Fraud
III	<i>updateLocation</i>	Interception(SMS), DoS
III	<i>processUnstructuredSS</i>	Fraud
III	<i>cancelLocation</i>	DoS
III	<i>sendRoutingInformation(-SM,-LCS)</i>	Multiple Attacks

Table 3.1: Categorization of MAP Messages used in attacks

3.2 Diameter Signaling

RFC 3588 defines the Diameter protocol [55] which is the next generation Authentication-Authorization-Accounting (AAA) and application layer Peer-to-Peer (P2P) protocol, evolving from RADIUS [60]. Diameter supports SCTP, an extensively used transport protocol in telecom networks [61]. It is a request-answer protocol based on messages.

A Diameter message contains data units which are called Attribute Value Pairs (AVPs). [62] presents a comprehensive tutorial about Diameter. Secure and efficient provision of Authentication-Authorization-Accounting services are required by Mobile networks so 3GPP chose Diameter for signaling and AAA services in 4G and all other mobile networks of next generations.

3.2.1 Considering Security in Diameter Design

Diameter was developed considering the security features lacked by all the communication protocols built on top of IP networks. However, it is merely relevant and does not matter what security features Diameter has to offer, it depends mostly on factors such as correct and standardized implementation of the protocol by all the operators. Network Domain Security NDS/IP Security demands that nodes beyond interconnection are secured individually to communicate using TLS or IPsec by the operators and it is further assumed by 3GPP standards that trust must be established between the nodes residing inside the domain of trusted operator network on either side of the interconnection [63]. Operators tend to make available a huge base of roaming partners to their subscribers and hence they utilize roaming hubs instead of connecting their nodes directly with their associates over the interconnection, making it a challenge for their business. Considering this practice by the operators, it raises a lot of concerns with respect to reliability as the roaming hubs supporting Diameter nodes may not be having NDS/IP Security enabled.

Built-in Security

Diameter has been developed to provide cryptographic protection in a number of modes unlike SS7 which offered un-secure communication between the core network nodes [55]. It provides connection-based (hop to-hop) and session-based (end-to-end) security with the help of Transport Layer Security (TLS) and IP Security (IPsec) respectively

[66]. TLS is recommended by Diameter protocol between its nodes. To augment the security of authentication procedures Diameter also supports other authentication protocols, such as Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), Extensible Authentication Protocol (EAP) and Network Access Identifier (NAI).

Discovering Peers Dynamically

Discovering peers dynamically is one of the advantages offered by Diameter protocol, where a next hop to which a signaling message needs to be forwarded can be discovered by a Diameter client. This is achieved by nodes broadcasting the security and application level that they support, in this way neighboring nodes may dynamically find out the suitable peers using either DNS Service Protocol [65] or SRVLOC (Service Location Protocol) [64]. When a new peer is discovered, the appropriate information about the routing configurations, peer location, application and service supported by them will be saved in peer tables and peer routing tables correspondingly. This feature gives another layer of security as the information useful for the attacker is locally stored making it difficult for him to know the routing paths or IP addresses of important nodes. In Dynamic peer discovery, as the sender needs not to know of the internal IP addressing, configuring the networks becomes much easier.

Built-in Global Title Translation (GTT)

SS7 interconnection is abused mostly due to the exposed core network with its critical nodes to the attackers or even the partners from outside the home network. A routing table of the communication message can disclose the Global Titles (GTs) of the entire network, keeping in view the aforementioned disclosure; Diameter offers Global Title Translation functionality protecting the core network nodes by reducing this need for openly disclosing the GTs. Topology of critical infrastructures like HSS and EIR gets

hidden with the help of GTT, which provides internal routing tables within the nodes instead of communication message. Diameter suite implements this concept of GTT, especially in HSS. Impersonation and port scanning attacks can be averted at the core network with the help of mutual node authentication in GTT. Translation of GTs is also important considering the assigning of global titles in the form of ranges to nodes, a common wrong practice by operators as it helps the attackers brute force GTs of a whole network if he has knowledge of one valid GT.

3.2.2 Limitations in Diameter Security

Diameter not only provides robust support for AAA and numerous aforementioned security considerations, it also gives, in comparison to SS7, the advantage of increased security to the core network nodes as well as enhancement in the end-user privacy. These advantages have led to a perception that the diameter by default provides security. Nevertheless, in the real world the actual implementation and security level in LTE networks depends on numerous other factors related to business and interoperability. Alongwith the generic security issues mentioned in [72] (which are related to air interface vulnerabilities), a few of the limitations that allow impersonation of network nodes by an attacker can be best described as:

Encryption brings overhead

In Diameter the authentication is done using Public Key Infrastructure (PKI) and X.509 certificates. The administration overhead for mobile networks is created due to the management issues in PKI for example key distribution, certificate management and revocation. In addition, more encrypted traffic is induced in the upper layers that require more bandwidth due to the piggybacking of acknowledgement messages in the transport layer (via TCP or SCTP). Interconnection network is a global network; serious problems are created by the financial overhead of certificate distribution, maintenance

of certificate revocation lists, and management of the central PKI system. Due to this reason the operators with fewer budgets are often unable to safeguard their nodes with the help of PKI.

Difference between standardization and implementation

Use of IPsec for intra-operator communications and TLS for inter-operator communications is highly recommended by the 3GPP standard for Diameter base protocol [55]. Their use is not mandatory although they are standardized in Diameter based communication. Moreover due to a lack of procedure the nodes in a Diameter based network might not have any means for verifying the use of IPsec and TLS [67] during communication with their peers. Practically, it can be observed that many operators do not secure their home LTE network to reduce the overhead of implementing the non-mandatory functionality and this reflects their ignorance to recognize the threats from the interconnection. Mostly focus is made on the attacks coming over the interconnection interface, it is important to note that a compromised core network node can also launch the same attack directly. The core network nodes (that run telnet or ftp protocol) are sometimes visible on the Internet; thereby attackers can further launch their attacks by compromising them.

Legacy systems support

The LTE is an in-homogeneous network because of the slow and gradual up gradation process from 2G and 3G networks. Consequently, current interconnection network has nodes which provide support for either SS7 or Diameter or both. Due to this an attacker can disguise as a roaming partner with SS7 network and it may lead to downgrading of the LTE network to use less protected legacy communication messages. Support for translation between Diameter and SS7 protocols is available with the help of Interworking Functions (IWF) [70, 71] to help cater the interoperability issues. SS7-based attacks

can easily be ported to Diameter based LTE networks with IWF. Due to interoperability, lack of security measures is being exploited in the interconnection by a considerable number of attacks, list for which can be found in [51].

Fail-over algorithms and issues

Numerous fail-over [68] and error-handling algorithms are provided by the Diameter base protocol to enable descriptive feedback if the system/network fails. The client initiates them when for a given amount of time it has not received any responses [69]. By sending bogus traffic of the fail-over algorithms, an attacker can flood the peers by impersonating as a Diameter client. Although the receiving peers are able to recognize the traffic as bogus or faulty (if the peer filters them), the fail-over algorithms try to process the traffic in order to provide useful feedback, and hence denial of service (DoS) attack is successful.

Applications decide Reachability

The communication messages (data packets) sent by a Diameter node depend on the application instead of network configuration (Diameter being an application layer protocol). Impersonation can be done by an attacker at the application layer thereby penetrating further into the network as the application controls the reachability [67]. This enables spoofing or impersonation attacks, especially if the attacker is successful in the interception of the interconnection traffic.

3.3 Comparing Protocol Stacks

Diameter replaces network and transport layer protocols of SS7 such as MTP2 and MTP3 by SCTP/IP. The application, presentation and session layer protocols like MAP, TCAP and SCCP are substituted with Diameter protocol. Figure 3.2 illustrates a short comparison between SS7 and Diameter signaling stacks.

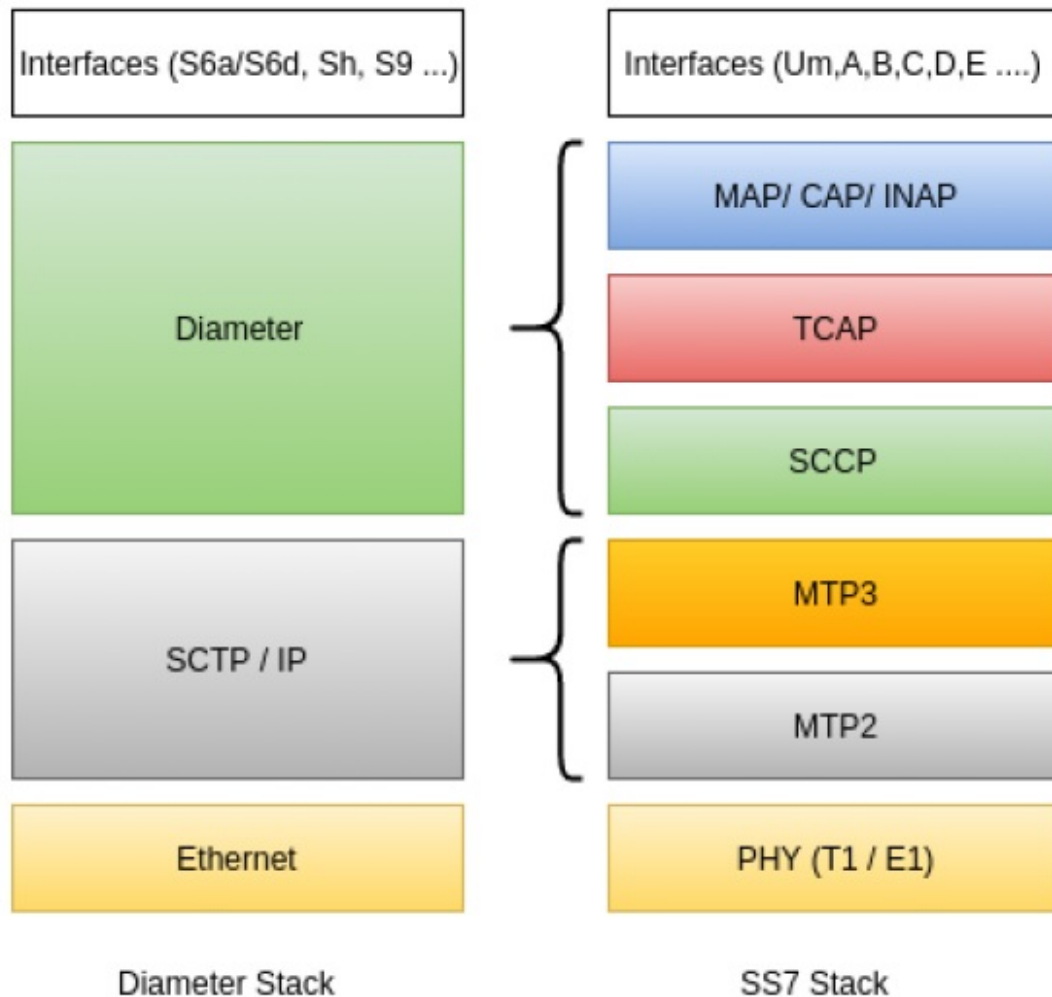


Figure 3.2: Comparison of SS7 & Diameter Stack

3.4 Comparing Attack Ratio in Diameter and SS7 [89]

Threat/ Attack	SS7 Network	Diameter Network
Intercepting the subscriber's traffic	89%	-
Information of the subscriber's is disclosed	100%	100%
Scams and fraud	78%	33%
Denying the services to subscribers	100%	100%
Information of the network is disclosed	63%	75%

Table 3.2: Percentage of Vulnerable Networks (2017)

3.5 Summary

This chapter gives a brief introduction of SS7, SS7 MAP messages categorized with respect to attack types and Diameter Signaling. It discusses the security consideration while designing Diameter to improve upon SS7 flaws and then what holes were left to be plugged in real implementation. It further compares SS7 and Diameter Protocol stacks and Attack ratios with respect to different common attacks.

Implementation of Malicious Traffic Filter with Snort and Wireshark

4.1 Intrusion Detection Systems

4.1.1 Introduction

Computer systems have always been and may continue falling victim to manipulation, unwanted attempts of accessing and disabling along with many other types of attacks. A system or software which detects such activities is known as Intrusion Detection System (IDS). List of the people making these attempts is long, mostly consists of disgruntled employees, hackers, or malicious programs. There are various types of malicious behaviors that can be detected using Intrusion Detection Systems. An IDS usually detects data driven attacks on applications, network based attacks on vulnerable services, attacks against hosts such as unauthorized and undesired log-ins, escalation of privileges and unwanted way-in to sensitive data and files.

4.1.2 Intrusion Detection Systems (IDS) Types

Intrusion Detection has two fundamental techniques namely anomaly detection and signature detection. Normal working or standard profile of systems is defined in the first method and then anything which deviates from that profile is detected [74]. In other words a desired action is defined and unwanted or undesired behaviours are distinguished from that using this technique. Defining boundaries between stored data sets and behaviours are two different things in nature. In a stored data, a single bit altered bit can be detected easily whereas differentiating anomalous behaviours from the acceptable ones is not an easy task [74]. Characterizing known ways to penetrate a system is called mis-use detection which is the second technique of Intrusion detection. These known ways are termed as patterns. Unambiguous patterns are monitored by misuse detection system. Patterns may vary from a static bit string to a suspect set of actions. For the past three decades, intrusion detection systems are exploring both these fundamental approaches to detect intrusions. Although both techniques have their own value, yet there are systems which use both these approaches in a hybrid system of detection. There have been considerable improvements in User interface, system control and efficiency of the intrusion detection systems in past few years. Implementations of all the intrusion detection systems available are based on mostly extensions of operating systems. OS data collection, notions of events and audit records are used by IDSs.

4.1.3 Detection Based on Anomalies

Anomaly-based detection is also distinguished as statistical or profile-based intrusion detection. In this approach, a “regularity” is defined and any irregular or abnormal traffic deviating from that regularity profile is declared as intrusive [75]. It is assumed in this technique that intrusion constitutes of events which are irregular in nature. Behavior profiles of users and applications are created based on their normal activity. Through heuristics or training these user and application profiles are built [82]-[87]. Behavior

of these users and applications is then monitored by Anomaly-Based IDS. Whatever differs from the normal profile can be comfortably considered as intrusive. Classifying a normal activity as intrusive or abnormal is considered as false-positive, whereas classification of abnormal activity as normal is known as false-negative. False-negative is considered more harmful than false-positive as it shows failure to detect harmful activities. What makes the anomaly based intrusion detection systems hard to implement is their requirement of not only complying with protocols and understanding the inner-working of an application, added with expert level users with their preferences, and date and time [76]. Anomaly based IDS requires computationally intensive behavioral models with respect to construction and tuning.

4.1.4 Signature-Based Detection

The second technique has many names. It is called signature-based, pattern-based or misuse detection. In this approach, abnormal activity is defined in the form of patterns. Data stream is monitored and IDS looks for those defined patterns. Intrusion is detected if any of those patterns are found in the data stream [77]. To represent or distinguish an attack, this footprint or pattern also called as a signature, is used [78]. Known malicious activities or attacks are analyzed for attributes and signatures, which are then recorded in a database to which a signature-based IDS matches against packet stream [79]-[81]. In a similar fashion, malwares are detected by anti-virus softwares. Signatures malicious in nature are searched by antivirus inside executables of applications whereas similar operation is performed by the signature-based IDS at network layer.

4.1.5 Snort-IDS

One of the most famed, free and useful open-source Network IDS is Snort. Snort utilizes a rule-based language combined with signature, protocol and anomaly inspection techniques to detect activities malicious in nature such as denying the service attacks,

Operating Systems fingerprinting attempts, Stealth port scans and Memory or Buffer overflow attacks. On networks based on IP, it performs traffic analysis and packet logging in real-time. Configuration file of the snort contains hundreds of rules defined for each type of anomalous behaviour to detect, based on which the program generates alerts. The best thing about the program is the way its rule language is kept flexible and handy to write rules for new attacks, due to which creation of new rules is reasonably simple. Rules are the major entities on which Snort relies to differentiate between usual internet activities and malicious behaviours. As compared to Wireshark, the program lacks a good GUI and is terminal based. A rule template for ICMP attack detection is given in figure 4.2.

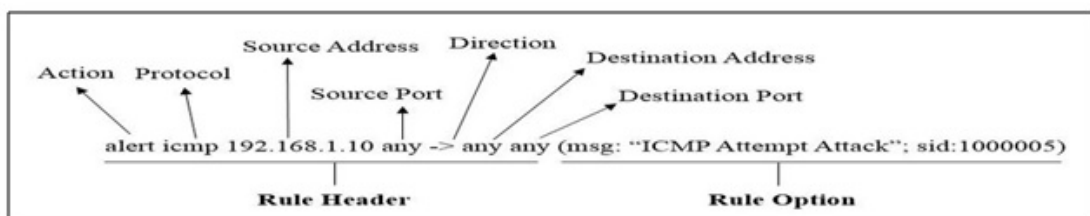


Figure 4.1: Sample of a basic Snort Rule for ICMP attack detection

4.2 Packet Sniffing and Analysis

An Ethernet sniffer, protocol or network analyser is a program, passively capturing all frames of data link layer, passing through the network adaptor of the device with which the program is attached for such purposes. It can capture data addressed to other nodes and save it for later purposes such as offline analysis. A system or network administrator can legitimately use such a program to analyse, monitor and troubleshoot network traffic [73]. To help keep up the efficient transmission of network data, administrators can use captured packets by the sniffer program for identification of erroneous packets, pinpointing bottlenecks and malicious behaviour prevention. Opposed to typical network hosts receiving traffic relayed exclusively to them, sniffer programs have the capability of capturing all in-bound and out-bound traffic. What makes them theoretically impos-

sible to detect and pose them as a threat is their ability to be detected while passively sniffing all the data packets, which may include clear text passwords and keys. However, it depends solely for what purpose such programs are used as their contribution towards maintaining the security is also beyond admiration.

4.2.1 Wireshark

Wireshark is a distinguished packet-analyzer for all types of networks, a network packet-analyzer can be thought of as a gauging device to determine what's happening on inside the network cable. It is a data-capturing software that has the understanding of encapsulation (structuring) of different networking protocols. It can capture live packet data from a network interface or may read from a file containing previously captured network packets. It can also parse and display the fields as well as their implication as specified by different networking protocols. Live data can be read from different types of networks which can be saved for later purposes. Program can export some or all packets in many of the file formats available. It helps searching the saved packets on many criteria. Captured network packets can be examined with the help of a Graphical User Interface (GUI), or by the use of command line (terminal) version of the utility also known as TShark. A display filter can help refining the captured data. Wireshark can colorize packets displayed, based on filters. It further helps in creating various statistics. Connections wireless in nature can also be filtered as long as they navigate the Ethernet being monitored. Various other timers, settings and filters can be put in place to facilitate the filtering of the output traffic.

4.3 Simulation and Testing Environment

Experiment was performed on a normal HP laptop with following specifications/ programs:

- Operating system: Open source OS Ubuntu 16.04.
- Processor: Intel(R) Core(TM) i7 7500U CPU @ 2.70 GHz 2.90 GHz
- RAM: 8.00 GB
- Hard Disk: 1.00 TB
- Simulation was performed in a VM (Oracle VirtualBox) on version 16.04 of Ubuntu loaded with Snort and Wireshark tools.
- To have samples of SS7 attack traffic, a simulation with SS7 Attack Simulator was performed.

4.4 SS7 Attack Simulator

SS7 attack simulator is built upon open source JSS7 stack by Restcomm. Simulator makes it possible to simulate three of the many publicly disclosed attacks on the SS7 network. Open source attack simulator for SS7 traffic was utilized in this research to generate signaling attack traffic as dataset. [48]. This attack traffic is generated with the help of Stream Control Transmission Protocol (SCTP) protocol and is then sent on *Lo* interface. It is built with following two modes:

4.4.1 Simple Mode

Simple mode supports following three types of attacks:

- Tracking location using Any Time Interrogation message(location:ati).
- Tracking Location using Provide Subscriber Information message(location:psi).
- SMS interception by stealing the subscribers(intercept:sms).

4.4.2 Complex Mode

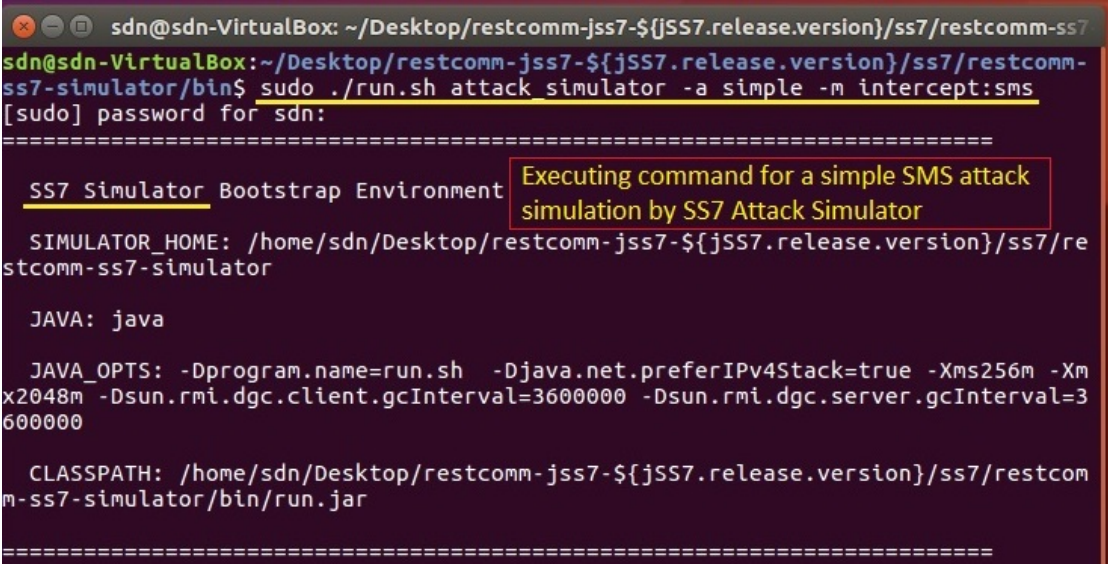
Simulator is built to generate normal and malicious traffic for a set of subscribers in complex mode which are passed as input string to the attack simulator.

Simulator requires an operational Java-environment and SCTP support installed on Linux. For Ubuntu VM, *libsctp1* and *lksctp-tools* dependencies were installed.

4.5 Proposed Detection Scheme

4.5.1 Attack No 1: Interception of SMS Attack

Ubuntu VM was hosted in the aforementioned machine for the experiment. Open Source SS7 Attack Simulator, Wireshark and Snort with all the necessary dependencies were installed in the VM and set up as required for the implementation and simulation. SS7 attack simulator generates attack traffic for three types of attacks. Figure 4.2 shows



```
sdn@sdn-VirtualBox: ~/Desktop/restcomm-jss7- $\{jSS7.release.version\}$ /ss7/restcomm-ss7
sdn@sdn-VirtualBox:~/Desktop/restcomm-jss7- $\{jSS7.release.version\}$ /ss7/restcomm-ss7-simulator/bin$ sudo ./run.sh attack_simulator -a simple -m intercept:sms
[sudo] password for sdn:
=====
SS7 Simulator Bootstrap Environment
SIMULATOR_HOME: /home/sdn/Desktop/restcomm-jss7- $\{jSS7.release.version\}$ /ss7/restcomm-ss7-simulator
JAVA: java
JAVA_OPTS: -Dprogram.name=run.sh -Djava.net.preferIPv4Stack=true -Xms256m -Xmx2048m -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000
CLASSPATH: /home/sdn/Desktop/restcomm-jss7- $\{jSS7.release.version\}$ /ss7/restcomm-ss7-simulator/bin/run.jar
=====
```

Figure 4.2: Intercept SMS Attack Traffic Simulation by SS7 Simulator

simulation of SMS intercept attack in simple mode. Simulator generates data set of attack and normal traffic. This traffic is then captured on loopback interface (*Lo*) using packet capturing tool Wireshark. As discussed earlier, Wireshark is a great tool for both

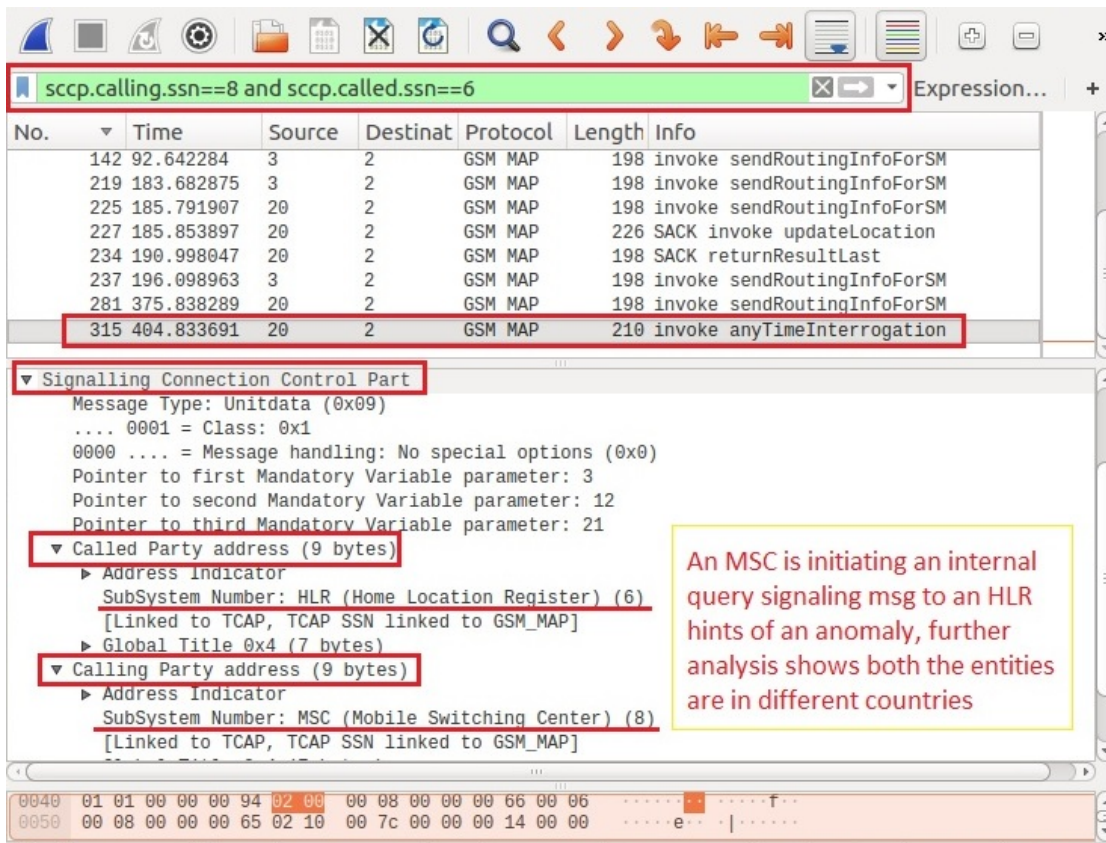


Figure 4.3: Identification and Analysis of Attack Packets captured in Wireshark

offline and online analysis of captured packets, especially with its GUI equipped with three interesting and helpful windows as shown in Figure 4.3. First or upper window shows live packet capturing. Middle or second window shows the protocols underneath. Lower or third window offers the packet information in "hexadecimal", a primary version of the "bits" truly flowing through the channel at that time. This window of the tool is of major importance as it helps in collecting signatures in the form of hexadecimal traffic patterns. Bits are the deepest level of signatures for analysis as any other form of analysis in the higher protocols will face more packaged data than bits. Information circulating at the lowest level in the form of bits can not avoid detection. During this experiment, Wireshark helped in a major way, identifying and analyzing attack packets from the captured traffic. Differentiating attack packets manually by analyzing each packet individually is not an easy and recommended approach.

If the basic idea behind an attack is well-understood then the tool helps alot in differen-

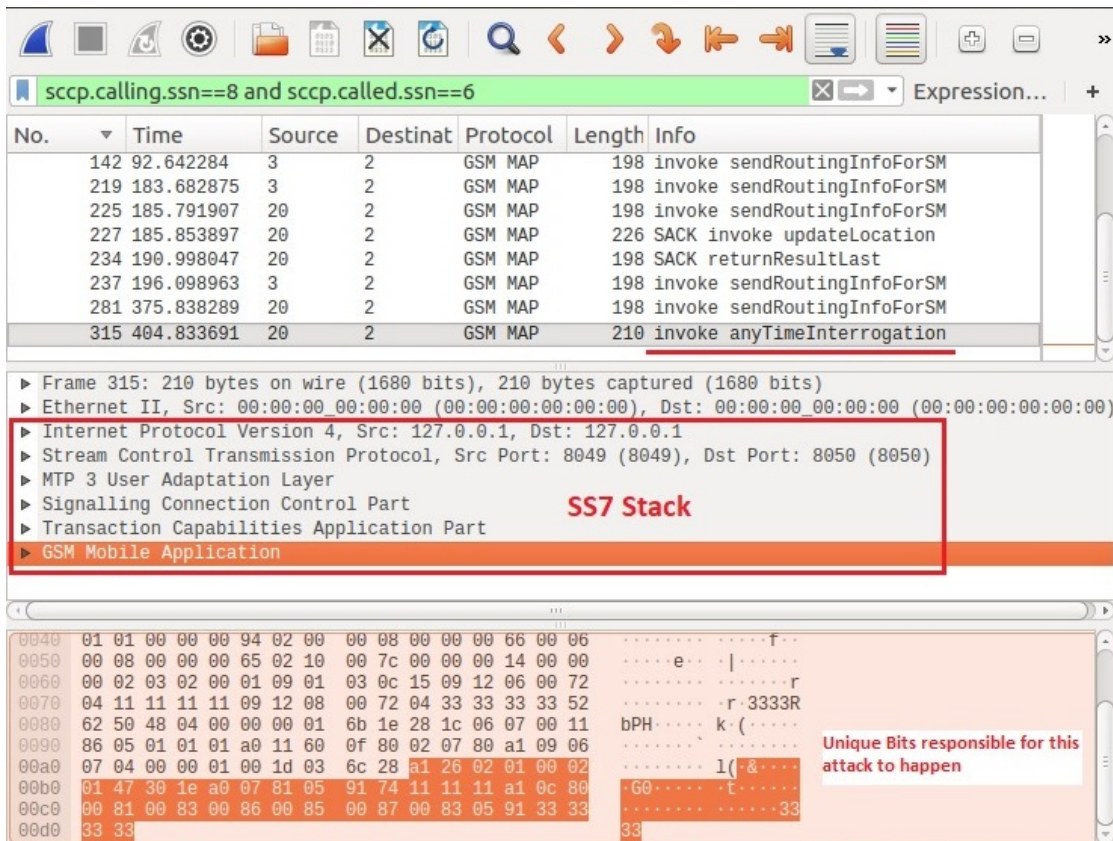


Figure 4.4: Signatures Derivation from Attack Packets after analysis in Wireshark

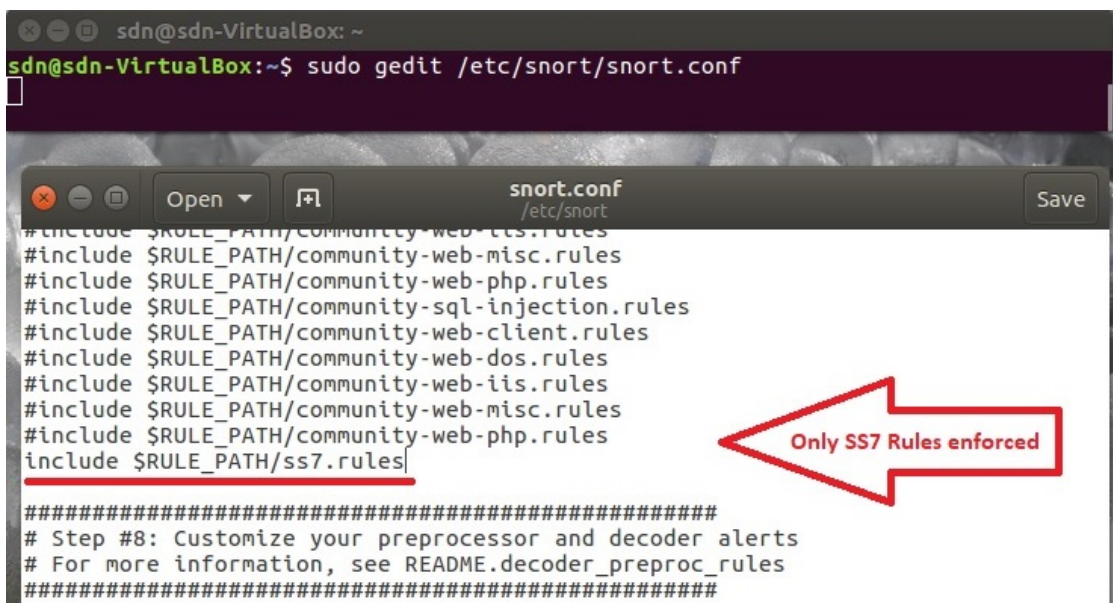


Figure 4.5: Addition of Custom Rules to Snort Configuration File

tiating attack packets from normal traffic. Considering the Figure 4.7, SMS Interception sequence of packets is shown. Now considering figure 4.8, where Wireshark shows sim-

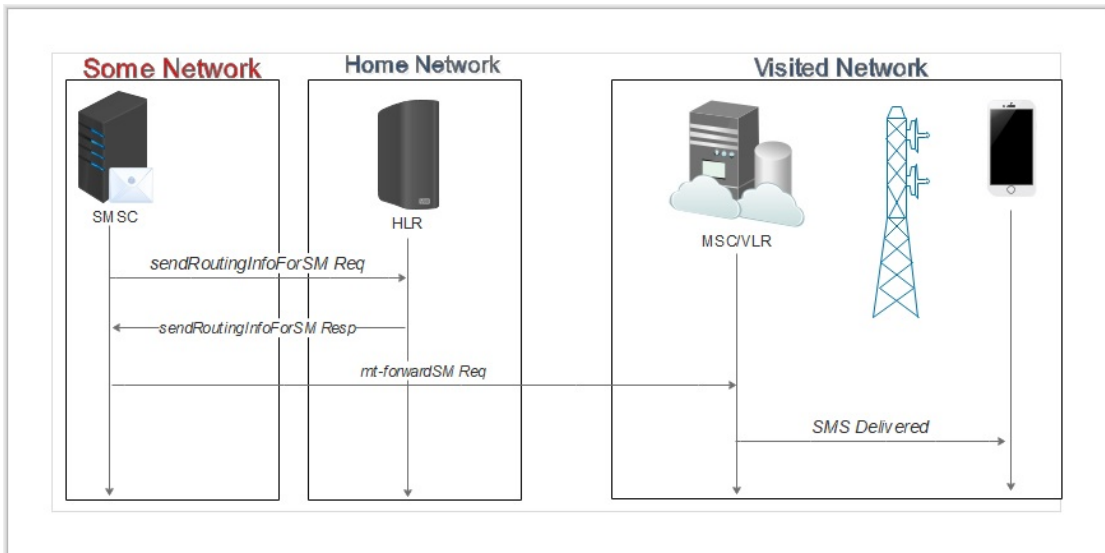


Figure 4.6: SS7 Normal SMS Delivery Procedure

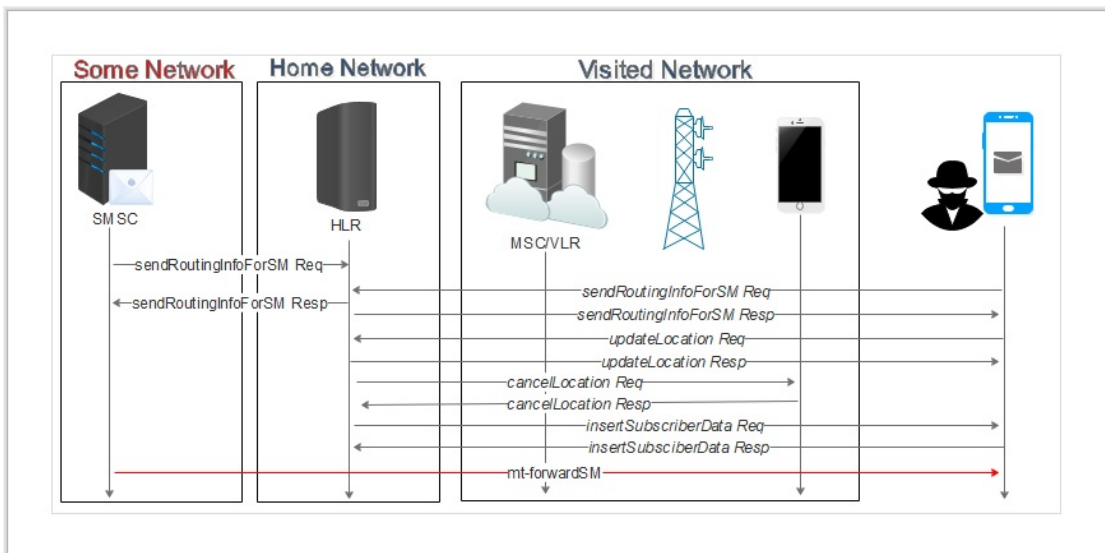


Figure 4.7: SS7 SMS Interception Attack

ilar sequence of packets. From this information, it can be assumed that it is anomalous.

SCCP protocol is supported by Wireshark and the tool has an option of applying a visualization filters for SCCP elements. It allocates different SSN numbers to each entity, making it easier to use them as filter. In Figure 4.3, Wireshark is attempting to show only those packets where an HLR (SubSystem Number 6) has been queried by an MSC (SubSystem Number 8) due to the display filter in place. In this way, the tool

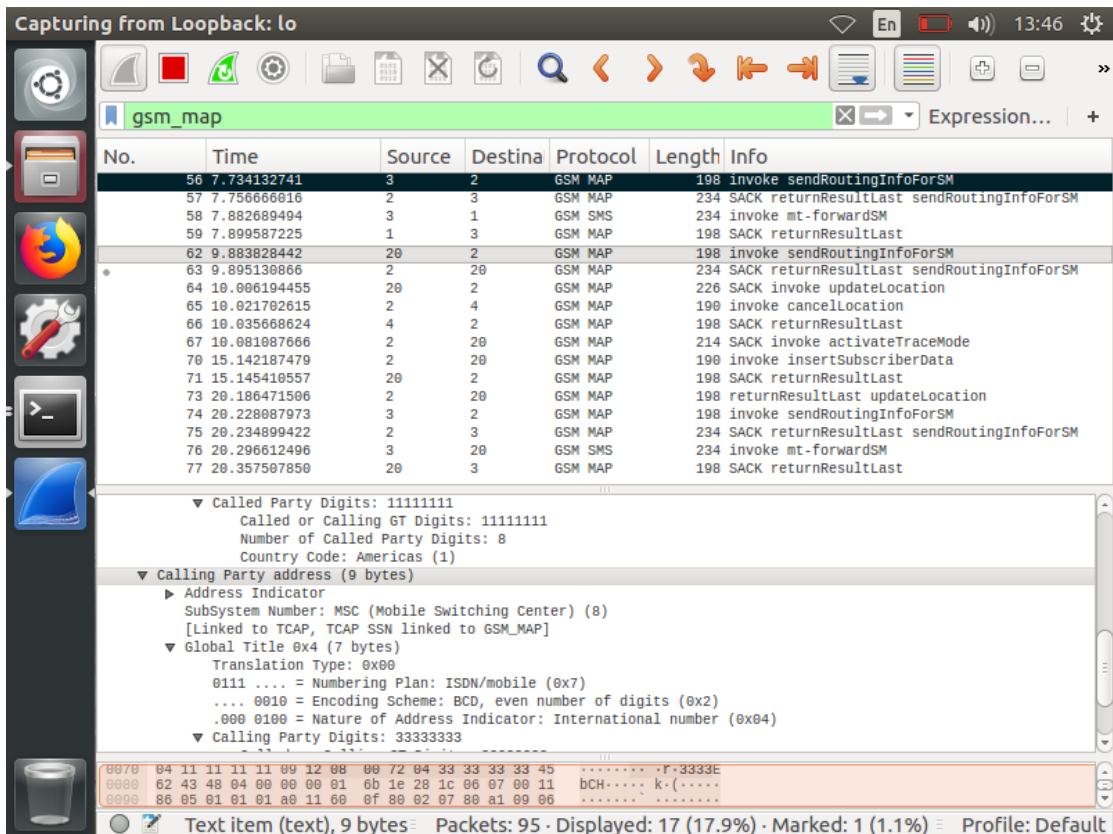


Figure 4.8: Wireshark Captured Sequence of Attack Packets

offers a great deal of help as it filters unwanted traffic and only shows packets of our interest to let us go further deep into protocols pane.

Keeping in mind Figures 4.3 and 4.12, going down a little further inside SCCP pane, shows that both Called Party/Calling Party Global titles are from different countries, which confirms that this signaling query was not from inside the HomeNet of HLR, instead it was initiated by what seems to be an MSC from another country which can be fake or an attacker, consult Figure 4.12. At this point, wireshark provided maximum help it could to let us deduce that if somehow this attack packet is given as an input to a detection tool, all the attack packets can be detected live or during the attack if it reoccurs.

In this regard, Figure 4.4 presents third window of GUI of the tool offering the packet information in "hexadecimal", which is the preliminary version of the "bits" for that packet actually passing through the channel at that time. These bits could be useful as

```

Match States      : 3855
Memory (MB)     : 17.00
Patterns        : 0.51
Match Lists     : 1.02
DFA
  1 byte states : 1.02
  2 byte states : 14.05
  4 byte states : 0.00
-----
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".

--== Initialization Complete ==--

-*> Snort! <*-
o''~)~ Version 2.9.7.0 GRE (Build 149)
''''~)~ By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.4
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>

Snort successfully validated the configuration!
Snort exiting

```

Validating the Snort Rules and Configuration before listening for Attack Traffic from Simulator

Figure 4.9: Validating Snort Configuration after the addition of new Rules

detection signatures if provided as an input to some content matching tool, which will match the all the packets against these bits to help us detect all such attack packets.

In a similar way, Figures 4.6 and 4.7 shows a normal and an attack procedure for SMS delivery and interception respectively, and Figure 4.8 confirms the sequence of Figure 4.7.

At this stage, Snort brings the content matching feature for detection as IDS. Snort provides hundreds of pre-loaded rules classified under different families such as *http*, *telnet*, *ssh* etc. All these rules if enforced, can help detect almost hundreds of attacks. However, keeping the tool up to date is necessary for normal usage, as new rules are published and regularized on routine basis.

With its powerful flexibility, Snort allows addition of custom rules in its configuration file. In this research, as shown in figure 4.5, custom rules named as SS7 Rules were

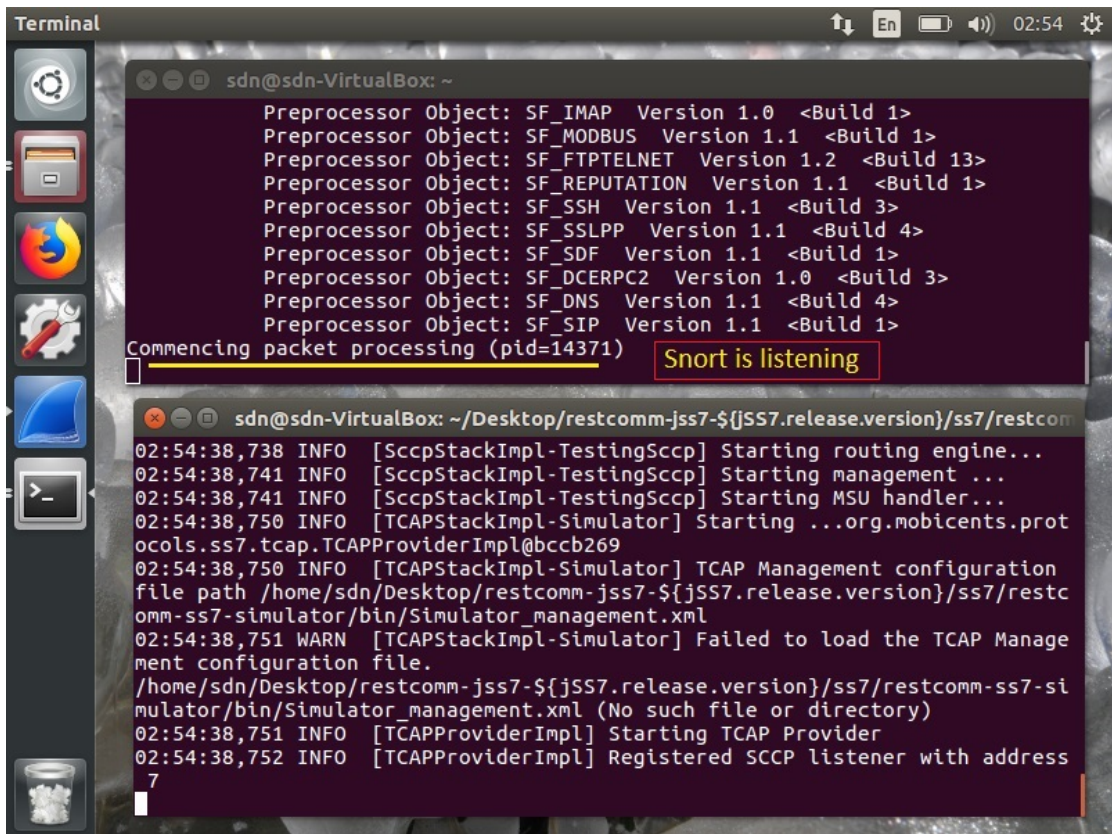


Figure 4.10: Parallel listening of Snort and Attack Simulation on Lo Interface

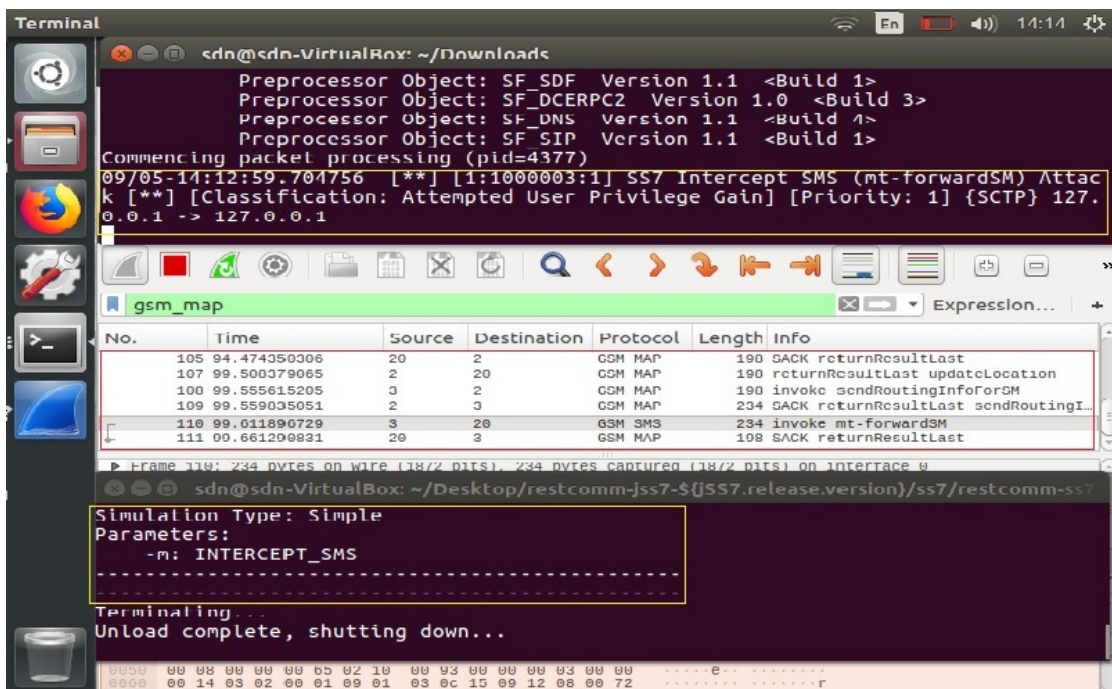


Figure 4.11: Parallel Attack Simulation and Detection

added to the configuration file of Snort. This rules file contains all three types of rules covering all simulated attacks, carefully adding aforementioned hexadecimal bits from the third window of Wireshark as content matching information in these rules. After addition of these rules, all other rules were disabled using hash symbol in the start. The tool was then run to validate the configuration, a basic and a must check before proceeding for detection as shown in figure 4.9.

To test the SS7 Rules, Simulator was run to generate attack traffic in parallel with Snort. The tool detected the attack without any false-positive or negative. Live demonstration of parallel attack simulation and detection can be seen in Figures 4.10 and 4.11.

In a similar way, anyTimeInterrogation and provideSubscriberInformation attacks are detected using the above detection scheme. Screen shots are attached.

4.5.2 Attack No 2: anyTimeInterrogation Attack

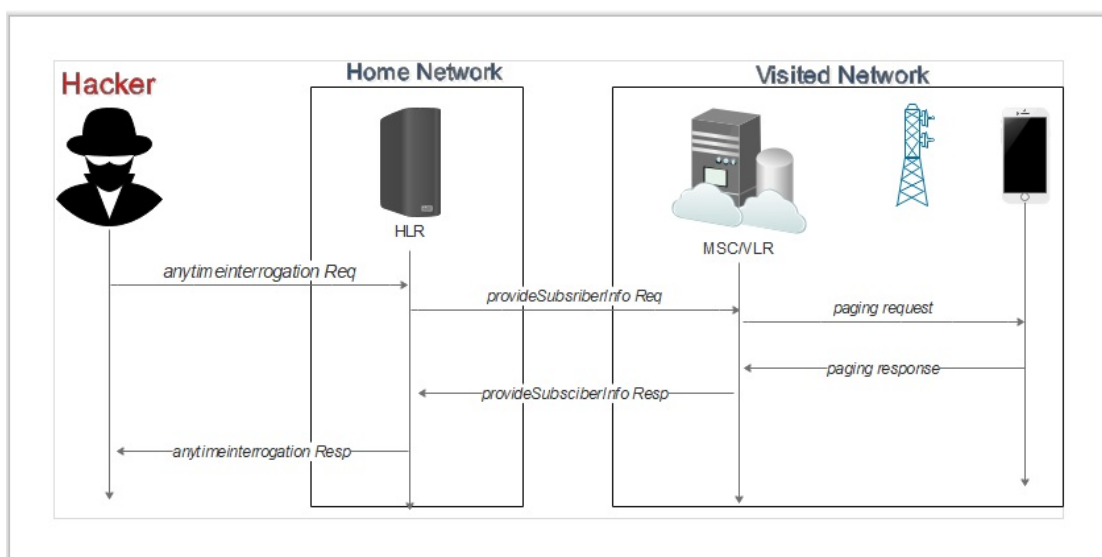


Figure 4.12: How ATI signaling message is exploited

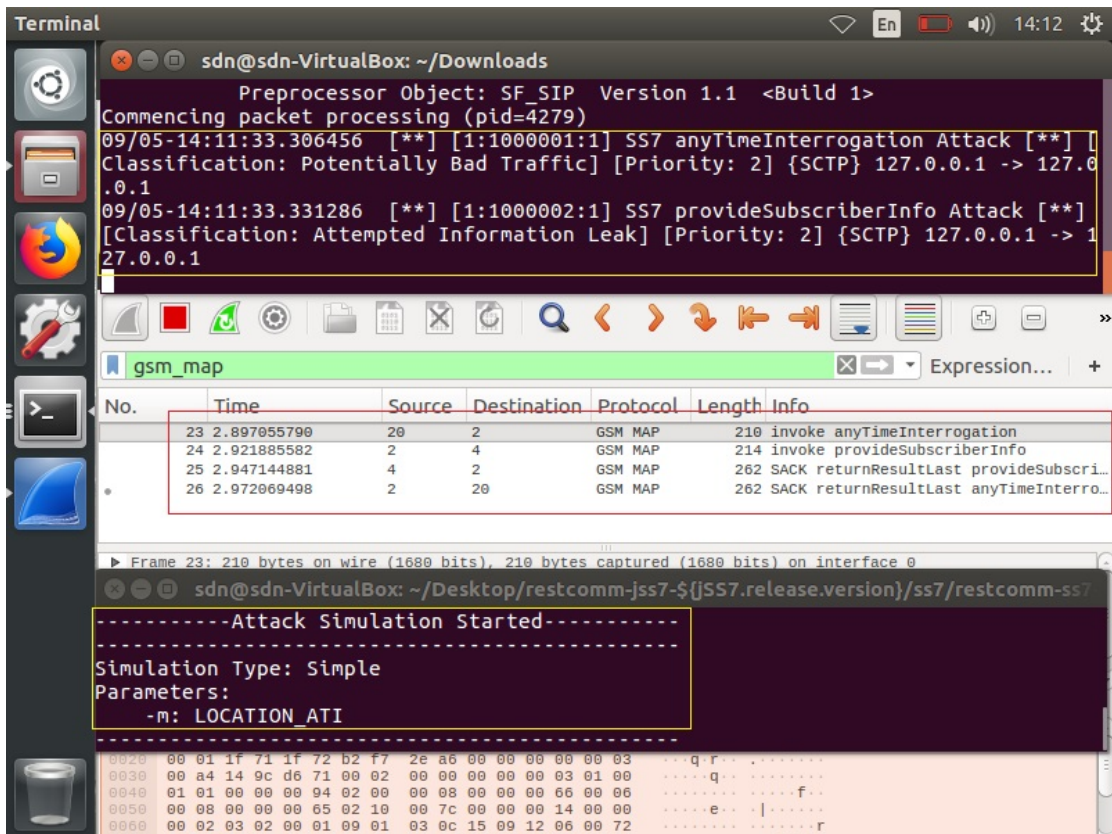


Figure 4.13: SS7 Attack using ATI signaling message

4.5.3 Attack No 3: provideSubscriberInformation Attack

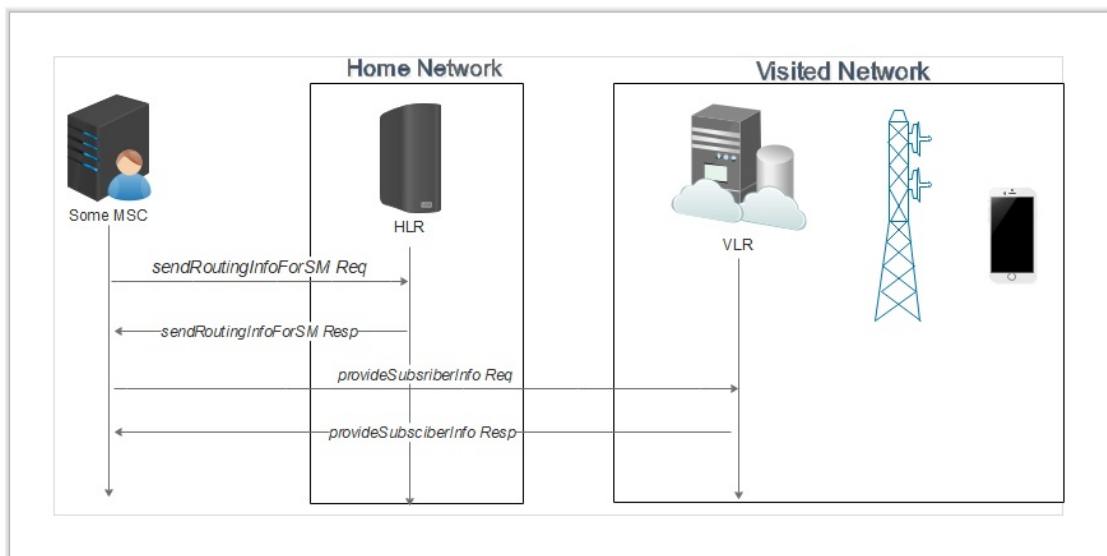


Figure 4.14: How PSI signaling message is exploited

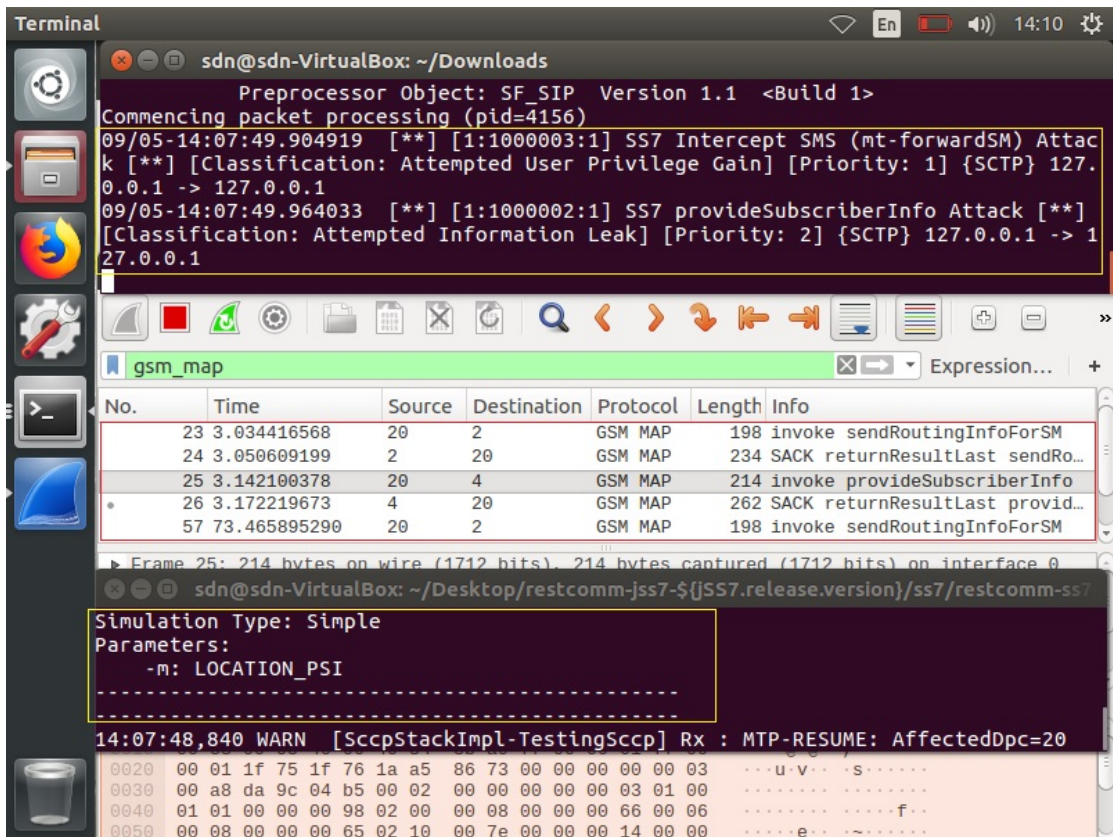


Figure 4.15: SS7 Attack using PSI signaling message

4.6 Results

Results of the proposed detection scheme are given below:

Type of Simulated Attack Traffic	Detection Rate %	FP %	FN %
<i>anyTimeInterrogation</i> Attack	100%	Nil	Nil
Interception of SMS Attack	100%	Nil	Nil
<i>provideSubscriberInformation</i> Attack	100%	Nil	Nil

Table 4.1: Comparing results for all attacks detected

4.7 Summary

This chapter presents a detailed introduction of Intrusion detection systems and their types with the help of Snort, a tool used in this work. It also discusses packet sniffing and analysis with the help of Wireshark, second tool used in this research for signature collection from SS7 attack packets. It also gives a brief introduction of Open Source SS7 attack simulator used in this work to simulate SS7 attacks. In the end it presents the proposed detection scheme in detail with the help of screen shots of actual work.

Conclusion

Signaling System No.7 network has become wall-less and found itself exposed to a large number of vulnerabilities, degrading security of telecommunication networks. The main reason behind this was the assuagement in governing regulations and laws for telecommunication market. For appropriate interoperability endeavors to merge the networks with each other added numbers to SS7 castle wall breaches. Addition of newer signaling messages for the mobility of telephone and advanced services for telecommunication paved the way for further attacks and abuses which included tracking of the subscribers, interception of calls, SMS scams and spamming and service denying to users (DoS). As though the advantages of Diameter, a new protocol gradually replacing the SS7 signaling protocol in the next generation telecommunication networks, are many, however, the default security provided by Diameter is not sufficient to make LTE an attack-resistant network.

This thesis gives a detailed review of available literature on SS7 security with reasons of why the literature is less as compared to other fields of research. It provides an insight of security, protocols and attack ratio on SS7/ Sigtran in comparison with its successor Diameter protocol. A comprehensive review of security considerations and possible exploits of Diameter signaling for an LTE network has been presented. The thesis contributes the concepts of Intrusion detection and Packet sniffing in a detailed

way with the aid of examples of Snort and Wireshark.

It is worth mentioning that traffic analysis has been found to be a useful tool for network monitoring and anomaly detection since long. In an effort to use this approach for detecting SS7 attacks, Snort and Wireshark tools were deployed on a simulated SS7 attack traffic data set to show feasibility of Snort deployment to this particular problem. It provides analysis of SS7 attack traffic in Wireshark (packet capture tool) for collection of malicious patterns and signatures to create rules in Snort IDS (Intrusion Detection System) to detect common attacks. Test results of the proposed detection methodology showed that Snort detects the all 3 types of attacks which simulator can generate by the help of signatures provided as rules in its configuration file. This methodology allows us to analyze and identify the flow of bits that circulated through the network during attack simulation and to detect the potential occurrences of such traffic patterns. This scheme uses tools with open-source licenses to avoid the huge costs of custom developments and it is essentially useful for small and medium networks with manageable volumes of traffic to filter.

While the roaming interconnections ensures cost-efficient way to provide cellular services on a global scale, it is need of the hour to deploy extra security measures in the interconnection network to protect the users from privacy breaches. This thesis is a step in the direction towards a sound network security architecture. The findings of this thesis are useful to ensure interconnection security in both old and new deployments. Fifth generation mobile networks are gaining a lot of momentum now a days and it can be easily argued that, without appropriate countermeasures and mitigation techniques in place, the threats discussed in this thesis might be carried onto the next generation networks.

5.1 Future Work

Following works can be carried out as future research:

5.1.1 Extending Functionality of Attack Simulator

As a future work, functionality of SS7 attack simulator can be extended to include all publicly disclosed attacks.

5.1.2 New Snort Rules with Real SS7 Traffic

Snort can be used with real SS7 attack traffic after signature collection with the help of Wireshark and Snort rules can be modified in a similar fashion.

5.1.3 Integration of SCTP in Snort

A library capable of calling rules with SCTP inside Snort instead of IP for SS7 rules.

References

- [1] B. Sanou, "ICT facts and figures 2017" International Telecommunications Union, 2017.
- [2] Statista, "Number of LTE subscriptions worldwide from 2015 to 2020." <https://www.statista.com/statistics/206615/forecast-of-the-number-of-global-hspa-LTE-subscriptions-up-to-2014/>.
- [3] Positive Technologies, 2016. "Primary Security Threats for SS7 Cellular Networks." [Online]. Available: <https://www.ptsecurity.com/upload/corporate/ww-en/analytics/SS7-Vulnerabilities-2016-eng.pdf>.
- [4] H. Sengar, D. Wijesekera and S. Jajodia, "MTPSec: Customizable Secure MTP3 Tunnels in the SS7 Network". 19th International Parallel and Distributed Processing Symposium, Workshop-17, IPDPS, 2005.
- [5] 3GPP TS 23.002 version 14.1.0. May 2017. GSM, UMTS, LTE Network Architecture Release 14.
- [6] D. Kurbatov and V. Kropotov. (2015). "Hacking mobile network via SS7: interception, shadowing and more". [Online] Available: <https://hitcon.org/2015/CMT/download/day1-d-r0.pdf>
- [7] G. Lorenz, T. Moore, G. Manes, J. Hale, and S. Sheno, "Securing SS7 Telecommunications Networks," IEEE Workshop on Information Assurance and Security, pp.273-278, June 2001.

- [8] M Isomaki, "Security in the Traditional Telecommunications Networks and in the Internet" http://www.tml.tkk.fi/Opinnot/Tik-110.501/1999/papers/tradsec/security_comparison.html. November 29, 1999.
- [9] B.Welch. "Exploiting the weaknesses of SS7." Network Security, Volume 2017 Issue 1, pp.17-19, January 2017.
- [10] H. Mourad. The fall of SS7-How can the critical security controls help? [Online]. Available: <https://www.sans.org/reading-room/whitepapers/critical/fall-ss7-critical-security-controls-help-36225>
- [11] Brewster, R. L. "Packet switched networks." In ISDN Technology, pp. 32-41. Springer, Dordrecht, 1993.
- [12] V. Mayer-Schonberger and M. Strasser, "Closer look at telecom deregulation: The European advantage," Harv. JL & Tech., vol. 12, p. 561, 1998.
- [13] "Telecommunications Act of 1996," US government Publication Office, Public Law 104-104 section 301, 104th Congress, 1996.
- [14] Spies A, Wrede JF. The New German Telecommunications Act. Mich. Telecomm. & Tech. L. Rev.. 1997.
- [15] S. P. Rao, I. Oliver, S. Holtmanns, and T. Aura, "We know where you are!" In 8th International Conference on Cyber Conflict, CyCon 2016, pp. 277-293.
- [16] Positive Technologies. December 2014. Signaling System 7 (SS7) Security Report. [Online]. Available: <http://www.ptsecurity.com>.
- [17] Metro Bank hit by cyber attack [Online]. Available: <https://telegraph.co.uk>. 01 Feb 2019
- [18] H. Kaaranen, S. Naghian, L. Laitinen, A. Ahtiainen, and V. Niemi, UMTS Networks: Architecture, Mobility and Services. New York: Wiley, 2001.

- [19] ETSI, TS. "136 101 V10. 3.0 (2011-06) LTE.Evolved universal terrestrial radio access (E-UTRA)."
- [20] S. Gibbs, "US congressman calls for investigation into vulnerability that lets hackers spy on every phone", the Guardian, 2016. [Online]. Available: <https://www.theguardian.com/technology/2016/apr/19/ss7-hack-us-congressman-calls-texts-location-snooping>.
- [21] A. Gellman and A. Gellman, "New documents show how the NSA infers relationships based on mobile location data", Washington Post, 2013. [Online]. Available: <https://goo.gl/cCmIzn>.
- [22] C McDaid,"Can They Hear You Now? Hacking Team & SS7 | AdaptiveMobile", Adaptivemobile.com, 2015. [Online]. Available: <http://www.adaptivemobile.com/blog/can-they-hear-you-now-hacking-team-ss7>.
- [23] WhatsApp rushes to fix security flaw [Online]. Available www.nytimes.com. 13 May 2019
- [24] "Positive Technologies - Signaling System 7 [SS7]-Security Report 2015", [Online]. Available: <https://www.ptsecurity.com/>
- [25] "Positive Technologies - PRIMARY SECURITY THREATS FOR SS7 CELLULAR NETWORKS 2016", [Online]. Available: <https://www.ptsecurity.com/>
- [26] Signaling Transport (sigtran). — The Internet Society, 1999-2007, [Online]. Available: <http://datatracker.ietf.org/wg/sigtran/documents/>
- [27] Ostman, L. CellPoint Systems. 2001. "A Study of Location-Based Services", [Online]. Available: <http://epubl.ltu.se/1402-1617/2001/254/LTU-EX-01254-SE.pdf>

- [28] Porter, T., and M. Gough. 2007. "How to Cheat at VoIP Security", [Online] Available: <https://goo.gl/dxQfgs>
- [29] Kolker, R. Bloomberg Businessweek. 2016. "What Happens When the Surveillance State Becomes an Affordable Gadget?", [Online]. Available: <http://goo.gl/weqptW>
- [30] Coulthart, R. 2015. Special Investigation: Bugged, Tracked, Hacked. www.9jumpin.com.au/show/60minutes/stories/2015/august/phone-hacking/
- [31] Schneier, B. Schneier on Security. 2015. SS7 Phone-Switch Flaw Enabled Surveillance, [Online]. Available: <https://www.schneier.com/blog/archives/2015/>
- [32] G. Lorenz, J. Keller, G. Manes, J. Hale, S. Sheno. "Public telephone network vulnerabilities." In Database and Application Security XV, pp. 151-164. Springer, Boston, MA, 2002.
- [33] Engel, T. "Locating Mobile Phones Using Signaling System 7". <https://events.ccc.de/congress/2008/Fahrplan/attachments/1262-25c3-locating-mobile-phones.pdf>
- [34] H. Sengar, R. Dantu, and D. Wijesekera, "Securing VoIP and PSTN from integrated signaling network vulnerabilities," in 1st IEEE workshop on VoIP Management and Security (VoIP MaSe), Vancouver, Canada, April 2006.
- [35] H. Sengar, R. Dantu, D. Wijesekera, and S. Jajodia. "SS7 over IP: Signaling interworking vulnerabilities". In IEEE Network, Vol. 20, No. 6, pages 32–41, November 2006.74
- [36] P. Langlois, "SCTPscan-Finding entry points to SS7 networks & telecommunication backbones," in BlackHat Convention (BH), 2007.

- [37] Lingling, Jiang, and Ma Hong. "New Trends of Attack and Prevention Technologies in Telecommunication." In Information Technology and Applications, 2009. IFITA'09. International Forum on, vol. 1, pp. 80-82. IEEE, 2009.
- [38] An Xinyuan, J Chen, Yi Liu, X Wei, and Tianye Xu. "A defense method based on improved MTP3 message discrimination in SS7 network." In Natural Computation (ICNC), 2011 Seventh International Conference on, vol. 2, pp. 711-715. IEEE, 2011.
- [39] Alexandre De Oliveira et al. 'Worldwide attacks on SS7 network' Hackito Ergo Summit (2014), http://2014.hackitoergosum.org/slides/day3_Worldwide_attacks_on_SS7_network_P1security_Hackito_2014.pdf.
- [40] "Hackito Ergo Sum 2014 | Hacker Community for Free Security Research", 2018. [Online]. Available: <http://2014.hackitoergosum.org/>
- [41] Karsten Nohl (SR Labs), 'Mobile self-defense' 31st Chaos Communication Congress 31C3 (2014), https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf.
- [42] Tobias Engel (Sternraute), 'SS7: Locate. Track. Manipulate', 31st Chaos Communication Congress 31C3 (2014), <http://berlin.ccc.de/tobias/31c3-ss7-locate-track-manipulate.pdf>.
- [43] Positive Technologies. December 2014. Signaling System 7 (SS7) Security Report. [Online]. Available: <http://www.ptsecurity.com>.
- [44] S.P Rao. Analysis and Mitigation of Recent Attacks on Mobile Communication Backend. Master's thesis, University of Tartu, 2015.

- [45] Kristoffer Jensen. "Improving SS7 Security Using Machine Learning Techniques" Master's thesis, Norwegian University of Science and Technology, 2016.
- [46] Jensen, K., Do, T.V., Nguyen, H.T., Arnes, A.: Better protection of SS7 using machine learning techniques. In: 6th International Conference on IT Convergence and Security (ICITCS) (2016).
- [47] Jensen, K., Nguyen, H.T., Van Do, T. and Arnes, A., 2017. A big data analytics approach to combat telecommunication vulnerabilities. *Cluster Computing*, 20(3), pp.2363-2374.
- [48] "SS7 Attack Simulator based on RestComm's jss7." [Online]. Available: <https://github.com/polarking/jss7-attack-simulator>.
- [49] M. Savadatti and D. Sharma, "SS7 Network and Its Vulnerabilities: An Elementary Review", *Imperial Journal of Interdisciplinary Research (IJIR)*, vol. 3, no. 3, pp. 912-916, 2017.
- [50] S. Puzankov, "Stealthy SS7 Attacks", *Journal of ICT Standardization*, vol. 5, no. 1, pp. 39-52, 2017.
- [51] S. Holtmanns, S. P. Rao, and I. Oliver, "User location tracking attacks for LTE networks using the interworking functionality," in 2016 IFIP Networking Conference (IFIP Networking) and Workshops, May 2016, pp. 315-322
- [52] M. Hamdi et al., "Voice Service Interworking for PSTN and IP Networks," *IEEE Commun. Mag.*, May 1999, pp. 104-11
- [53] Chandola V, Banerjee A, Kumar V. Anomaly detection: A survey. *ACM computing surveys (CSUR)*. 2009 Jul 1;41(3):15.
- [54] "Black Hat", [Online]. Available: <http://blackhat.com/>.
- [55] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, Diameter base protocol," RFC 3588, The Internet Engineering Task Force, September 2003.

- [56] White Paper: 5G Security," tech. rep., Ericsson AB, 2015.
- [57] C. Cox, An introduction to LTE: LTE, LTE-advanced, SAE and 4G mobile communications. John Wiley & Sons, 2012.
- [58] M. Paolini, White Paper: Wireless security in LTE networks," tech. rep., Senza Fili Consulting, 2012.
- [59] Lee, D., & Jeff, H. (2005). Signaling System No. 7 (SS7 C7): Protocol, Architecture, and Services.
- [60] C. Rigney, A. Rubens, W. Simpson, and S. Willens, Remote Authentication Dial In User Service (RADIUS)," RFC 2865, The Internet Engineering Task Force, June 2000.
- [61] R. Stewart, Stream Control Transmission Protocol," RFC 4960, The Internet Engineering Task Force, September 2007.
- [62] J. Liu, S. Jiang, and H. Lin, Introduction to Diameter." <https://www.ibm.com/developerworks/library/wi-diameter/>.
- [63] 3GPP, 3G security; Network Domain Security (NDS); IP network layer security," TS 33.210; Release 12, 3rd Generation Partnership Project (3GPP).
- [64] E. Guttman, C. Perkins, and J. Kempf, Service Templates and Service: Schemes," RFC 2609, Internet Engineering Task Force, June 1999.
- [65] S. Cheshire and M. Krochmal, DNS-Based Service Discovery," RFC 6763, Internet Engineering Task Force, Feb. 2013.
- [66] T. Dierks and E. Rescorla, The Transport Layer Security (TLS) Protocol," RFC 5246, The Internet Engineering Task Force, August 2008.
- [67] P. Langlois, Diameter vs SS7 from a security perspective," 2013. <http://labs.p1sec.com/2013/07/28/346/>.

- [68] S. K. Yoo, H. G. Kim, and S. W. Sohn, Enhancement of failover using application layer watchdog and SCTP heartbeat in diameter," in Mobile Communications, pp. 239-246, Springer, 2003.
- [69] A. Hosia, Comparison between RADIUS and Diameter." <http://www.tml.tkk.fi/Studies/T-110.551/2003/papers/11.pdf>, May 2003.
- [70] 3GPP, InterWorking Function (IWF) between MAP based and Diameter based interfaces," TS 29.305; Release 12, 3rd Generation Partnership Project (3GPP).
- [71] 3GPP, InterWorking Function (IWF) between MAP based and Diameter based interfaces," TR 29.805; Release 12, 3rd Generation Partnership Project (3GPP).
- [72] N. Seddigh, B. Nandy, R. Makkar, and J.-F. Beaumont, Security advances and challenges in 4G wireless networks," in Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on, pp. 62-71, IEEE, 2010.
- [73] Bo Yu 'Based on the network sniffer implement network monitoring Computer Application and System Modeling (ICCASM), 2010 International Conference on Volume: 7, 2010, Page(s): V7-1 - V7-3
- [74] Axelsson, S., "Research in Intrusion-Detection Systems: A Survey". Technical Report, Department of Computer Engineering, Chalmers University of Technology, Sweden, 1998.
- [75] Patrick Wheeler, Errin Fulp,"Taxonomy of Parallel Techniques for Intrusion Detection", ACMSE 2007 March 23-24, 2007
- [76] Errin W. Fulp and Ryan J. Farley, "A Function- Parallel Architecture for High-Speed Firewalls", Proceedings of ICC IEEE 2006
- [77] Anita K. Jones and Robert S. Sielken ,"Computer System Intrusion Detection: A Survey"

- [78] Northcutt, S., Cooper, M., Fearnow, M., and Frederick, K. *Intrusion Signatures and Analysis*, 1st ed. New Riders, SANS GIAC. Indianapolis, IN, January 2001
- [79] Staniford-Chen, S., Cheung, S., Crawford, R., Dilger, M., Frank, J., Hoagland, J., Levitt, K., Wee, C., Yip, R., and Zerkle, D., “GrIDS – A Graphbased Intrusion Detection System for Large Networks”, 19th National Intrusion Detection Working Group – Information Systems Security Conference, October 1996
- [80] Dowel C, R. “The Computer Watch Data Reduction Tool”, 13th National Computer Security Conference, Washington, October 1990
- [81] Goldberg, I., Wagner, D., Thomas, R., and Brewer, E. A.” A Secure Environment for untrusted Helper Applications”, 6th USENIX Security Symposium, July 1996.
- [82] Paxson, V. “Bro: A System for Detecting Network Intruders in Real-time” Elsevier Computer Networks, 1998
- [83] Lane, T., Brodley, C. E., “Temporal Sequence Learning for Anomaly Detection” 5th ACM Conference on Computer and Communications Security, 1998
- [84] Hofmeyr, S. A., Forrest, S., and Somayaji, A., “Intrusion Detection using Sequences of System Calls” *Journal of Computer Security*, 1998
- [85] Samaha, S. E. Haystack: “An Intrusion Detection System”, 4th Aerospace Computer Security Applications Conference, IEEE Computer Society Press, 1988
- [86] Lane, T., and Brodley, C. E. “Temporal Sequence Learning and Data Reduction for Anomaly Detection”, *ACM Transactions on Information Systems Security*, 1999
- [87] Forrest, S., Hofmer, S. A., Somayaji, A., and Longstaff, T. A. “A Sense of Self for UNIX Processes”,. *IEEE Symposium on Security and Privacy*, IEEE Press, Oakland, May 1996

- [88] Christopher Kruegel Fredrik Valeur Giovanni Vigna Richard Kemmerer, “Stateful Intrusion Detection for High Speed Networks”, Proceedings of IEEE symposium on Security and Privacy, 2002
- [89] Positive Technologies. 2018. Diameter Vulnerabilities Exposure Report. [Online]. Available: <http://www.ptsecurity.com>.