UNIVERSITY OF THE WITWATERSRAND

SCIENTIA ET LABORE

JOHANNESBURG

VULNERABILITIES OF SIGNALING SYSTEM NUMBER 7 (SS7) TO CYBER ATTACKS AND HOW TO MITIGATE AGAINST THESE VULNERABILITIES.

BOB KAMWENDO

A Research Report submitted to the Faculty of Engineering and the Built Environment,
University of the Witwatersrand, in partial fulfillment of the requirements
for the award of the degree of Master of Science in Engineering

Johannesburg, August 25, 2015

Declaration

I declare that this research project is my own unaided work. It is being submitted as a partial fulfillment for the Degree of Master of Science in Engineering to the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination to any other University.

Candidate Name: Bob Kamwendo

Candidate Signature:................................

Date: 25 th August, 2015

Abstract

As the mobile network subscriber base exponentially increases due to some attractive offerings such as anytime anywhere accessibility, seamless roaming, inexpensive handsets with sophisticated applications, and Internet connectivity, the mobile telecommunications network has now become the primary source of communication for not only business and pleasure, but also for the many life and mission critical services. This mass popularisation of telecommunications services has resulted in a heavily loaded Signaling System number 7 (SS7) signaling network which is used in Second and Third Generations (2G and 3G) mobile networks and is needed for call control and services such as caller identity, roaming, and for sending short message servirces. SS7 signaling has enjoyed remarkable popularity for providing acceptable voice quality with negligible connection delays, possibly due to its circuit-switched heritage. However, the traditional SS7 networks are expensive to lease and to expand, hence to cater for the growing signaling demand and to provide the seamless interconnectivity between the SS7 and IP networks a new suite of protocols known as Signaling Transport (SIGTRAN) has been designed to carry SS7 signaling messages over IP.

Due to the intersignaling between the circuit-switched and the packet-switched networks, the mobile networks have now left the “walled garden”, which is a privileged, closed and isolated ecosystem under the full control of mobile carriers, using proprietary protocols and has minimal security risks due to restricted user access. Potentially, intersignaling can be exploited from the IP side to disrupt the services provided on the circuit-switched side.

This study demonstrates the vulnerabilities of SS7 messages to cyber-attacks while being transported over IP networks and proposes some solutions based on securing both the IP transport and SCTP layers of the SIGTRAN protocol stack.

Acknowledgements

Heartfelt gratitude to my supervisor, Professor Rex Van Olst for his time, guidance and unwavering support. Thank you Prof. for your constant reminders on the deliverables due dates and always being available to help and give direction.

Many thanks also go to my work colleague, Patrick Khaile, for the technical assistance rendered throughout the course of this research. Ntates, your contribution was invaluable and priceless.

Finally, I would like to thank my daughter Sindi and Captain Ken for thier patience and understanding. The times you wanted me to teach you some alphabet symbols and draw you pictures, I was also busy with my work. You never gave up on me but kept on coming.

Dedication

To my departed father and sister. How I wish you were here to witness and celebrate with me for achieving this milestone. I am not despaired, though, because I know that you are happy for me wherever you are.

Contents

List of Tables

List of Figures

Glossary

Abbreviation	Definition
2G	Second Generation
3G	Third Generation
4G	Fourth Generation
ACK	Acknowledgement
ARP	Address Resolution Protocol
BSC	Base Station Controller
BSD	Berkeley Software Distribution
BSSAP	Base Station Subsystem Application Part
BTS	Base Transceiver Station
CAMEL	Customised Applications for Mobile Enhanced Logic
CAS	Channel Associated Signaling
CCITT	Consultative Committee for International Telephony and Telegraphy
CLEC	Competitive Local Exchange Carrier
CRC	Cyclic Redundancy Check
DDoS	Distributed Denial of Service
DoS	Denial of Service
DS	Digital Signal
ETSI	European Telecommunications Standards Institute
FISU	Fill In Signal Unit
GMSC	Gateway Mobile Switching Centre
GPRS	General Packet Radio Service
GSA	Global mobile Suppliers Association
GSM	Global System for Mobile communications
GTT	Global Title Translation
HLR	Home Location Register

Abbreviation	**Definition**
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
INIT	Initiation
IP	Internet Protocol
IPSEC	IP Security
ISDN	Integrated System Digital Network
ISUP	ISDN User Part
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union - Telecommunications
Kbps	Kilobits per Second
LAP-D	Link Access Protocol for the ISDN “D” channel
LAP-Dm	Link Access Protocol for the ISDN “D” channel modified
LAN	Local Area Network
LKSCTP	Linux Kernel SCTP
LSSU	Link Status Signal Unit
LTE	Long Term Evolution
M2PA	MTP Level 2 Peer-to-Peer Adaptation
M2UA	MTP Level 2 User Adaptation
M3UA	MTP Level 3 User Adaptation
MAC	Media Access Control
MAP	Mobile Application Part
Mbps	Megabits per Second
MGC	Media Gateway Controller
MITM	Man In The Middle
MNO	Mobile Network Operator
MoIP	Media over IP
MSC	Mobile Switching Centre
MSU	Message Signal Unit
MTP	Message Transfer Part
MTR	MAP Test Responder
MTU	Map Test Utility

Abbreviation	**Definition**
NGN	Next Generation Networks
OMAP	Operations, Maintenance and Administrative Part
OSI	Open Systems Interconnection
PSTN	Public Switched Telephone Network
SACK	Selective Acknowldgement
SCCP	Signaling Connection Control Part
SCP	Service Control Point
SCTP	Stream Control Transmission Protocol
SEP	Signaling End Point
SG	Signaling Gateway
SIGTRAN	Signaling Transport
SMS	Short Message Service
SP	Signaling Point
SPC	Signaling Point Code
SS7	Signaling System Number 7
SS7oIP	SS7 over IP
SSP	Service Switching Centre
STP	Signaling Transfer Point
SU	Signal Unit
SYN	Synchronisation
TCAP	Transaction Capabilities Application Part
TCB	Transport Control Block
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TLS	Transport Layer Security
TUP	Telephone User Part
UA	User Adaptation
UE	User Equipment
UDP	User Datagram Protocol
VLR	Visitors Location Register
VoIP	Voice over IP
WIN	Wireless Intelligent Network

Chapter 1

Introduction

The traditional Signaling System number 7 (SS7) networks have existed for a long time and have gone through a lot of improvements over the years to meet the high performance demands (low loss and low delay) of a phone call. Despite the high acceptance levels, SS7 networks are not as scalable as IP networks as a result they are expensive to expand. The telecommunications industry has witnessed a tremendous growth in the demand for SS7 signaling networks due to the exponential growth of the number of mobile phone users which has resulted from the mass popularity of communication services. Also the increase in demand for services such as Media over IP (MoIP) has led the telecommunication operators to start planning for future networks that better support the resulting datagram traffic. In this regard IP has been considered the most promising network protocol, since it can offer improved resource utilisation while reducing the operational, maintenance, and network infrastructure costs.

The traditional SS7 networks are being migrated to the much anticipated Next Generation Networks (NGN) with a goal of achieving an all – IP network. However, this transition from traditional telecom networks to all - IP networks will not happen overnight and the co-existence is expected to last for a long period of time, perhaps even for decades. The challenge today is to integrate these two types of existing networks (IP and SS7).

It is becoming more and more important to combine classical SS7-based networks with IP-based networks using the latter to transport SS7 signaling messages. Deploying such a combined architecture enables operators to make use of the advantages of IP-based equipment in an SS7 based environment, avoiding some of the problems increasingly appearing in the rapidly growing SS7 networks, such as link set capacity and load sharing [3]. For this reason, the Signaling Transportation (SIGTRAN) working group of the Internet Engineering Task force (IETF) [22] has developed a new signaling protocol suite that will make it possible to carry SS7 signaling messages over IP.

SS7 is built for reliability and performance by providing a heavily redundant signaling network which reduces signaling network downtimes by carrying signaling traffic in redundant signaling links in case of a link failure. In order for packet based voice services to find acceptance in the marketplace it is paramount that the reliability, security and privacy of communication, as perceived by the end user of such services, is as good or better than the one experienced in present day circuit switched networks.

In order for the IP networks to achieve the same level of reliability as the SS7 networks, the Internet Engineering Task Force (IETF) has designed a signaling interface commonly referred to as Signaling Transport (SIGTRAN) which is a protocol suite that specifies a method of transporting SS7 signaling information over IP-based packet networks. The multi-homing and multi-streaming features of the SCTP protocol of the SIGTRAN protocol stack provide the necessary redundancy and reliability features similar to those of the traditional SS7 networks.

The introduction of Internet connectivity and many more IP based services to 3G networks through network interconnections imports not only the high speed capabilities of the Internet but also very high risks of cyber-attacks which may be launched from the IP side of the network. Cyber–attacks may be launched from the packet switched networks while targeting a particular SIGTRAN signaling node of the circuit switched network. These kinds of attacks are referred to as the Cross infrastructure cyber-attacks [1].

The transition of mobile SS7 networks to IP brings some additional security threats, such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, ping floods, SYN floods, replay attacks, DNS hijacking, IP port scanning [40] and many others, which may result in the interception of both network and subscriber data, limit subscriber access (causing congestion), and/or compromise the overall network security of the network, as some of the core network elements' functionality may be lost.

Typically SS7 networks are very secure in that they are proprietary and the equipment is kept in highly lock secured areas with limited physical access by employees. Transporting the once secure TDM–based SS7 signaling messages over public IP networks as payload packets opens the messages to cyber threats which can easily be launched from the IP side of the interconnected networks.

The SIGTRAN protocol suite through the introduction of the Stream Control Connection Part (SCTP) above the traditional IP layer only addressed the intersignaling issues between the legacy SS7 and the IP systems such as reliability and performance, however little effort was directed towards the SIGTRAN security issues.

While there are a number of other important aspects of convergence, such as addressing [2] that require further research, this study therefore focuses on the security of the SS7 messages in a converging environment. The study aims at demonstrating the vulnerabilities of IP networks to cyber-attacks which would subsequently render the SS7 messages exposed to attacks in an interconnected network infrastructure. So the above reasons have motivated the Key Research Question that this study aims to investiage and reads: *"There is much emphasis these days on the security of communications, and there are some solutions available in the market place for voice and data. However it is anticipated that 2G and 3G communications technologies will be with us for a lot longer than we think, and thus SS7 will also be a driving force to communication. What are the vulnerabilities of Signaling System Number 7 to cyber-attacks and how can we mitigate against these vulnerabilities?"*

1.1 Summary of the Research Report

The research paper is structured as follows:

Chapter One: Introduction

This Chapter gives an overview of the critical issues which have been discussed in this introduction regarding the subject matter. The chapter introduces the driving forces behind the convergence and interworking between the circuit based signaling and the packet based signaling networks and the problems intersignaling has brought about to the once “walled garden” of SS7 signaling network. The chapter clearly highlights the key research question and the objectives which necessitated the study of SS7 vulnerabilities to cyber-attacks.

Chapter Two: Literature Survey

This Chapter starts by introducing the SS7 signaling system together with all its reliability and performance characteristics. In this regard the SS7 network architecture is identified as being designed to provide redundancy. The different protocol stacks of SS7 signaling system are looked at and compared against the Open Systems Interconnection (OSI) levels. SS7 signaling protocol binaries which are unique only to mobile networks in providing mobility of subscribers like BSSAP and MAP are introduced. The limitations of SS7 system that have resulted into mobile operators migrating to IP services are also discussed in this chapter. The chapter further introduces SIGTRAN, the interfacing signaling technology between SS7 and IP systems. All the SIGTRAN protocols including the SCTP which offers performance and reliability features similar to SS7 signaling are looked at in details. This chapter further revisits some publications on similar work regarding the subject matter previously done by other researchers highlighting the research efforts that have already been put into the investigation of SIGTRAN technology security and reliability.

Chapter Three: Key Research Question

This chapter focuses on the SIGTRAN transport technology as a whole and validates the need for the investigation in this study by providing an overview of the problem statement and the objectives behind this study.

Chapter Four: Methodology

This chapter discusses in detail the approach adopted in the simulation experimentation that tested the problem and outlines the goals the tests aimed to achieve in determining whether through network interconnections, IP networks are a security risk to SS7 networks. Details about the simulation SIGTRAN implementation, test equipment setup and test software used for the experimentation are discussed in this chapter.

Chapter Five: Experimentation

This chapter explains the different experimentation tests which were conducted in trying to establish whether IP networks render SS7 signaling messages vulnerable to cyber-attacks or not. The testing tools and procedures are outlined clearly in this chapter. The test results are tabulated and the key findings, observations and conclusions of all the tests explained.

Chapter Six: Mitigating Factors against SIGTRAN Cyber-Attacks

The most common attack scenarios and their counter cyber measures are outlined in this chapter.

Chapter Seven: Conclusions and Recommendations

This chapter provides a summary of the report by revisiting every aspect of the research and ensuring that all objectives and the key research question have been responded to satisfactorily. Recommendations and potential future research areas in SIGTRAN networks security conclude this report.

Chapter 2

Literature Survey

2.1 Common Channel Signaling System Number 7 (SS7)

In a lay man's language, signaling in telecommunications network systems can be looked at as a set of messages which are used for setting up, supervising and tearing down of a call. However the ITU-T defines signaling as "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 operation [4].

In telecommunications, different network components indicate (signal) to each other certain information to coordinate themselves for providing services to network users. A signaling network is as important to telecommunications network as the nervous system is to the human body. It breathes life into the infrastructure. Richard Manterfield, author of Telecommunications Signaling poetically stated that: "Without signaling, networks would be inert and passive aggregates of components. Signaling is the bond that provides dynamism and animation, transforming inert components into a living, cohesive and powerful medium" [5].

2.1.1 Evolution of Signaling in Telecommunications Networks

Notable telecommunication systems signaling inventions date back to 1876 in the United States of America when Alexander Graham Bell invented the telephone. Signaling in this telephony system involved manual telephone connection between the caller and the called party via most preferably a female telephone operator.

Amon Strowger in 1892 developed the dial telephone system with an automatic Central Office (Exchange/Switch) which helped to get rid of the manual telephone operators. To date, many different inventions and innovations in the telecommunications signaling networks have been implemented but all of them are meant to only satisfy the initial objective of helping in setting up, supervising and tearing down of a call.

Harmonisation of Signaling Systems

Depending on many different factors, a variety of signaling systems have been developed in telecommunications networks with different signaling standards in different parts of the world. This then created problems between the calls originating from one network with one type of signaling implementation terminating into another network with a different type of signaling system. Some sort of adaptation had to be made.

The then telecommunications governing body, Consultative Committee for International Telephony and Telegraphy (CCITT) later changed to the International Telecommunications Union (ITU) was tasked to find the common standard through which all the different signaling systems would work together. The Channel Associated Signaling (CAS) System was then recommended as the common standard. As the name suggests, CAS is a signaling system in which control signaling messages for synchronisation and frame alignment are carried in the same channels as traffic (voice and data). When using CAS system, signaling messages are only sent whenever traffic is being transmitted. This creates bottlenecks in telecommunication networks and also wastes bandwidth. As a result this type of signaling is better suited for networks with low traffic capacities.

In around the early 1980's a more robust and highly redundant and fault tolerant signaling system was developed. This out-of-band signaling system was defined by the ITU as a Common Channel Signaling System Number 7 commonly known as Signaling System Number 7 and herein referred to as SS7. In out-of-band signaling, the call control information travels on separate and dedicated 56 or 64 kbps channels rather than within the same bearer (traffic) channels [46].

Figures 2.1 and 2.2 on page 8 illustrate the differences between CAS and SS7 signaling systems.

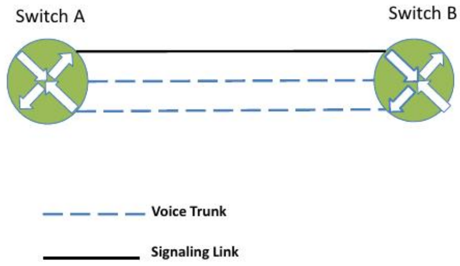


Figure 2.1: Channel Associated Signaling [46]

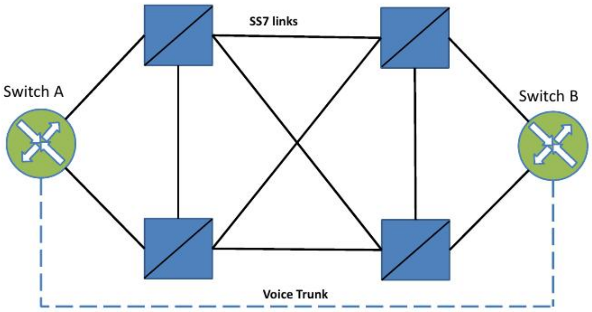


Figure 2.2: Common Channel Signaling [46]

2.1.2 SS7 Network Architecture

The SS7 architecture comprises of three main nodes known as the Signaling Points (SPs) depending on their functionalities. These include the Service Switching Point (SSP), Signaling Transfer Point (STP) and the Service Control Point (SCP).

Each SP on the network is identified by a unique 14-bit integer known as Signaling Point Code (SPC). SPs are interconnected by signaling links whose bandwidths are normally 56 or 64 kbps [41]. To cater for higher bandwidths and redundancy on the signaling network, a set of up to 16 links can be used between any two SPs. The combination of all the links between any two SPs is called a linkset.

In practice SSPs are the telephone exchanges (central offices) and are the entry and exit points of an SS7 signaling network. STPs relay SS7 messages between signaling end points (such as the SCP and SSP) and other STPs. For redundancy purposes, STPs are deployed in mated pairs. SCPs provide application access. SCPs act as an interface to applications such as network databases. Figure 2.3 shows the general structure of a digital telephone network with SS7 signaling.

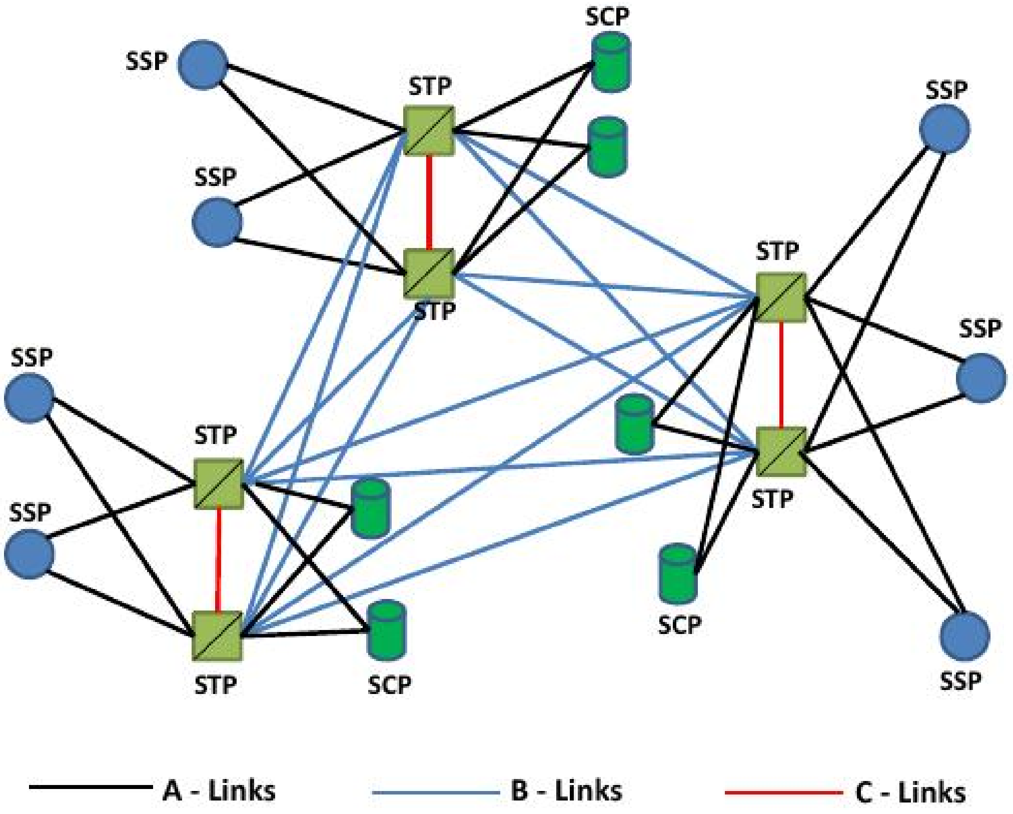


Figure 2.3: SS7 Network Architecture [41]

With reference to Figure 2.3 above, the signaling links connecting the different SP are known by different names. A-Links (Access links) are the signaling links that connect the signaling end points (SSP and SCP) to the STP. The A-links carry messages only destined for the signaling end points. One mated pair of STPs from one network is connected to other mated STP pairs in other networks using the B-Links (Bridge links). Lastly, the C-Links (Cross Links) interconnect the paired STPs. C links are used only when an STP has no other route available to a destination signaling point due to link failure(s). Note that SCPs may also be deployed in pairs to improve reliability; unlike STPs, however, mated SCPs are not interconnected by signaling links [41].

The signaling information (messages) that are transmitted through an SS7 network are carried in a data packet called Signal Unit (SU). There are three main types of signaling units. These include the Fill In Signal Units (FISU), Link Status Signal Units (LSSU) and Message Signal Units (MSU).

Fill In Signal Units are sent when the signaling link is idle. This is recommended so that link-error information is available even in the absence of high-level information being sent. In this way, problems will be recognised quickly and corrective actions can be implemented with minimal loss of service.

Link Status Signal Units are used by the signaling link level to bring the link into alignment. Like FISUs, LSSUs are sent continuously end to end between SP.

Message Signal Units carries the actual upper-level information that contains control flags that indicate the protocol that is being transmitted e.g. ISDN User Part (ISUP), originating and destination point codes along with the variable length information (message content) field.

2.1.3 SS7 Protocol Stack

A stack is a set of data storage locations that are accessed in a fixed sequence. The hardware and software functions of the SS7 protocol stack are divided into layers which are compared against the Open Systems Interconnection (OSI) model for communication between different systems made by different vendors. Figure 2.4 shows different components that make up the SS7 protocol stack.

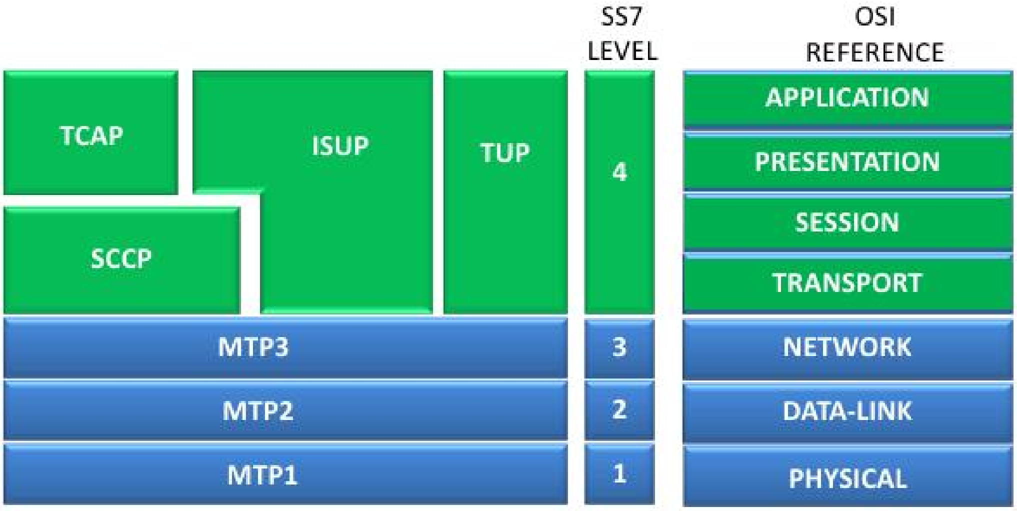


Figure 2.4: PSTN Based SS7 Protocol Stack [47]

While the OSI reference model consists of seven layers, the SS7 model is looked at as having four levels. The functionalities of the upper layers (4-7) of the OSI model are compressed to only one level (level 4) in SS7 protocol stack.

The Message Transfer Part (MTP)

MTP provides the rest of the levels with node-to-node transmission, including physical network nodes connections, basic error detection and correction schemes and message sequencing. It provides routing, message discrimination and distribution functions within a node. The MTP is comprised of three different logical parts known as levels and the different functions of the MTP are distributed within these levels [47].

Message Transfer Part Level 1 (MTP1)

MTP 1 defines the physical, electrical and functional characteristics of the digital signaling link. Some of the physical interfaces defined include E-1(2048 kb/s; 32 64 kb/s channels), DS-1 (1544 kbps; 24 64 kbps channels), V.35 (64 kbps), DS-0 (64 kbps) and DS-0A (56 kbps).

Message Transfer Part Level 2 (MTP2)

MTP2 is equivalent to the Data Link layer of the OSI model. It ensures accurate end-to-end transmission of a message across a signaling link. Level 2 implements flow control, message sequence validation and error checking using cyclic redundancy check (CRC). When an error occurs on a signaling link, the message/set of messages is/are retransmitted. MTP Level 2 uses length indicators to determine what type of signal unit it is being received and how it must be processed.

Message Transfer Part Level 3 (MTP3)

The MTP 3 is analogous to the Network layer of the OSI model and depends on the services of Level 2 to provide routing, message discrimination and message distribution functions. MTP Level 3 reroutes traffic away from failed links and signaling points and controls traffic when congestion occurs.

The level 4 layers of the SS7 protocol stack which includes the protocols, user parts and application parts together with their functionalities are discussed in the following subsections:

Signaling Connection Control Part (SCCP)

Signaling Connection Control Part (SCCP) is a higher level protocol than MTP that provides end-to-end routing of signaling messages. SCCP is required for routing Transaction Capabilities Application Part (TCAP) messages to their proper databases. SCCP provides connectionless and connection-oriented network services and Global Title Translation (GTT) capabilities above MTP Level 3. SCCP is used as the transport layer for TCAP-based services [47].

Telephone User Part (TUP)

Telephone User Part (TUP) is an old protocol for analog telephone systems. It was/is used to perform basic telephone call setup and tear-down. TUP handles analog circuits only. It has been replaced by ISDN User Part (ISUP), but is still used in some parts of the world like China and Brazil [47].

ISDN User Part (ISUP)

The ISDN User Part (ISUP) defines the protocol used to set-up, manage and release trunk circuits that carry voice and data between terminating line exchanges. As previously explained, ISUP was derived from TUP. ISUP supports ISDN and intelligent networking functions. However, calls that originate and terminate at the same switch do not use ISUP signaling [47].

2.1.4 SS7 Signaling Performance Requirements

SS7 signaling network being the heartbeat of the whole telecommunications networks was primarily designed for performance and reliability. The design of the SS7 provides for error detection, correction and sequential transfer of signal units.

The SS7 signaling performance and reliability requirements directly or indirectly translate into the MTP requirements (which then also fulfill the requirements of the MTP users) [6] and [7]. The ITU-T through recommendations, Q.706 [8] and Q.709 [9] recommends a number of reliability and performance requirements the SS7 signaling network must meet:

1. Not more than one in 10^{10} of all message signal units must contain an error that is undetected by the MTP.
2. Not more than one in 10^{7} messages will be lost due to failure in the MTP.

3. The availability of any signaling relation (i.e. communication path between two communicating SEPs) has to be at least 0.99998 corresponding to a downtime of at most 10 minutes/year.

4. Not more than one in 10^{10} messages will be delivered out-of-sequence to the User Parts due to failure in the MTP. This value also includes duplication of messages.

5. In addition there are requirements on message transfer times in STPs, which under normal conditions are supposed to be less than 100 msec, and implicit requirements on limits for the outgoing queuing delays which must not become a dominating factor of the transfer times.

Requirement 1 is a function of the quality of the underlying physical transport, the CRC function of the MTP2, and the likelihood of system internal errors of implementations.

In order to fulfill requirement 2 with unreliable hardware the MTP deploys redundant signaling links and the so called change-over procedure which allows the loss-free switching of traffic from a failed link to other links, provided the signaling link terminations on both nodes involved are still functioning and can communicate with each other via alternative links/paths.

In order to enable the design of signaling networks fulfilling requirement 3 the MTP provides several procedures supporting redundancy in the network. On 64 kbit/s links link failures are discovered within 128 msec by the error rate monitor of MTP2. If an alternative link or path exists, MTP3 initiates the changeover procedure.

To enable the fulfillment of requirement 4, MTP3 performs explicit or timer based sequence control procedures wherever possible when rerouting traffic via alternate links or routes or when reverting traffic back to the original routes.

While STP transfer times are an implementation and not a protocol issue the MTP provides several mechanisms to limit outgoing queues (requirement 5) and thus overall signaling transfer times. The error rate monitor of MTP2 not only rapidly discovers failed links but will also take a link out of service when the signal unit error rate approaches 4×10^3. If outgoing congestion occurs on links, MTP management takes action and informs traffic sources to reduce traffic. If congestion is of a lasting nature (e. g. caused by too many link failures) a conditional rerouting procedure (transfer restricted procedure) can optionally be deployed [3].

2.1.5 Signaling in 2G and 3G Mobile Networks

In 3G mobile networks SS7 signaling is used between the core network elements. These include the Base Station Controller (BSC), Home Location Register (HLR), Mobile Switching Centre (MSC) and also between the MSC and the other mobile networks and the Public Switched Telephone Network (PSTN) through the Gateway Mobile Switching Centre (GMSC).

Other signaling protocols used in 3G networks apart from the SS7 include the Link Access Protocol for the ISDN “D” channel (LAP-D) which is used between the BSC and the Base Transceiver Station (BTS) [44]. LAP-D message structure is similar to SS7 only that it does not support networking capabilities as a result it is only used for point to point connections. Another protocol also used in 3G networks is Link Access Protocol for ISDN “D” channel modified (LAP-Dm) and is used for signaling between the mobile station and the BTS.

The SS7 protocol stark layers explained in subsection 2.1.3 on page 10 mostly relate to the PSTN. In 2G and 3G cellular networks the signaling is complex. Unlike the PSTN, 2G and 3G mobile networks demand for extra signaling requirements due to differences in network architecture that requires a large amount of non-call-related signaling.

The subscriber in PSTN is static as opposed to the mobile subscriber in the 2G and 3G networks. The subscriber mobility in the later networks requires a continuous tracking of the mobile station which results in location update procedure. The tracking of a mobile station by the network to update its current location is an example of a non-call-related signaling because the signaling takes place in the absence of a call. This requires additional sets of standard signaling messages to manage this requirement in 2G and 3G mobile networks.

In 2G and 3G systems, the additional signaling message protocol layers are:

Transaction Capabilities Application Part (TCAP)

Transaction Capabilities Application Part (TCAP) supports the exchange of non-circuit related data between applications across the SS7 network using the SCCP connectionless service. It facilitates connection to an external database. Queries and responses sent between SSPs and SCPs are carried in TCAP messages. Some of the application entities that use TCAP include Operations, Maintenance and Administrative Part (OMAP) which uses services for communication and control functions through the network via a remote terminal. Also in GSM mobile networks, Mobile Application Part (MAP) uses TCAP to share cellular subscriber information among different networks to support user authentication, equipment identification and roaming [44].

Mobile Application Part (MAP)

MAP is the SS7 application-layer protocol used in GSM network systems to access the Home Location Register, Visitor Location Register, Mobile Switching Centre, Equipment Identity Register, Authentication Centre, Short Message Service Centre and Serving GPRS Support Node to provide services, such as roaming capability, text messaging (SMS), and subscriber authentication. MAP is transported and encapsulated with the SS7 protocols MTP, SCCP, and TCAP.

Base Station Subsystem Application Part (BSSAP)

The BSSAP is used for signaling communication between the MSC and the BSC and also between the MSC and the mobile station. It carries call control requests for initial connection establishment, and changes in connection attributes between BSC and MSC. It also handles handovers between relay MSC and BSC.

Figure 2.5 shows a complete SS7 protocol stack for the GSM Network System.

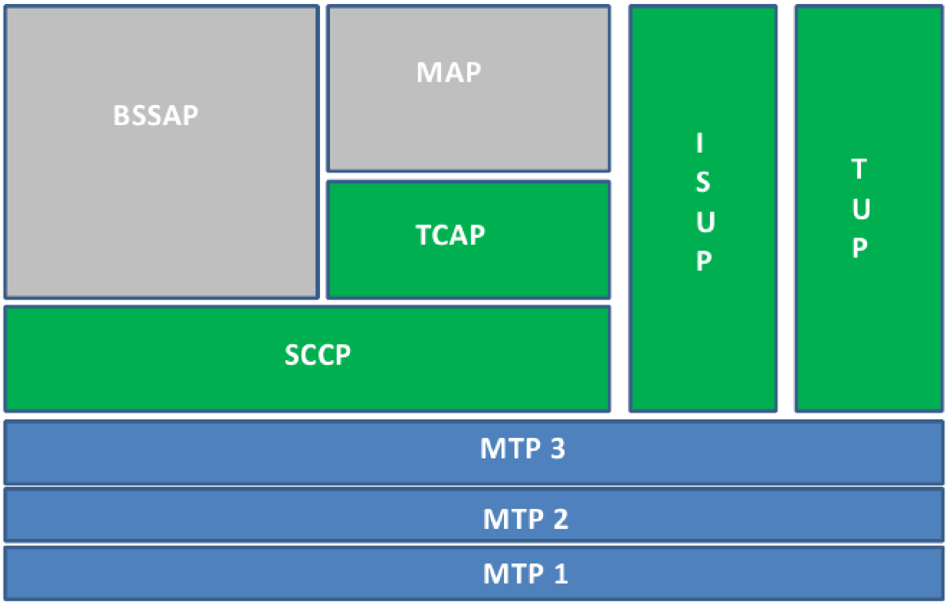


Figure 2.5: SS7 Protocol Stack for the GSM Network System [44]

2.1.6 Protocol Layers in 3G Network elements

The SS7 requirements for individual 3G network elements are different. Not all network elements have all the protocols in the SS7 stack.

The Mobile Switching Centre (MSC)

The MSC is a 3G network element that is responsible for call control therefore TUP and ISUP protocols are required for that function. Also the MSC in conjunction with the VLR are responsible for location updates and communicating with the BSC and HLR. To be able to perform these tasks BSSAP and MAP are required. BSSAP sits on top of SCCP while TCAP provides service to MAP.

MTP is the foundation on which SS7 is built and therefore it must be found in every network element, including the MSC, which is capable of processing SS7 signaling. Therefore it can be seen that the MSC has all the SS7 protocol stacks.

The Base Station Controller (BSC)

When using SS7 signaling messages, BSC only communicates with the MSC to manage all call activities such as connection establishment and handovers and therefore requires BSSAP protocol to perform such functions. BSSAP sits on top of SCCP which in turn rests on the MTP layers.

The Home Location Register (HLR)

As opposed to the MSC which requires TUP/ISUP for call control on the mobile station and the BSc, HLR only deals with database queries regarding the status of the network users for authentication purposes. For this purpose it uses MAP protocol. MAP sits on TCAP which gets serviced by SCCP which rest on MTP layers.

Figure 2.6 shows SS7 protocol stacks in various network elements and the signaling communication linkage between those different network elements.

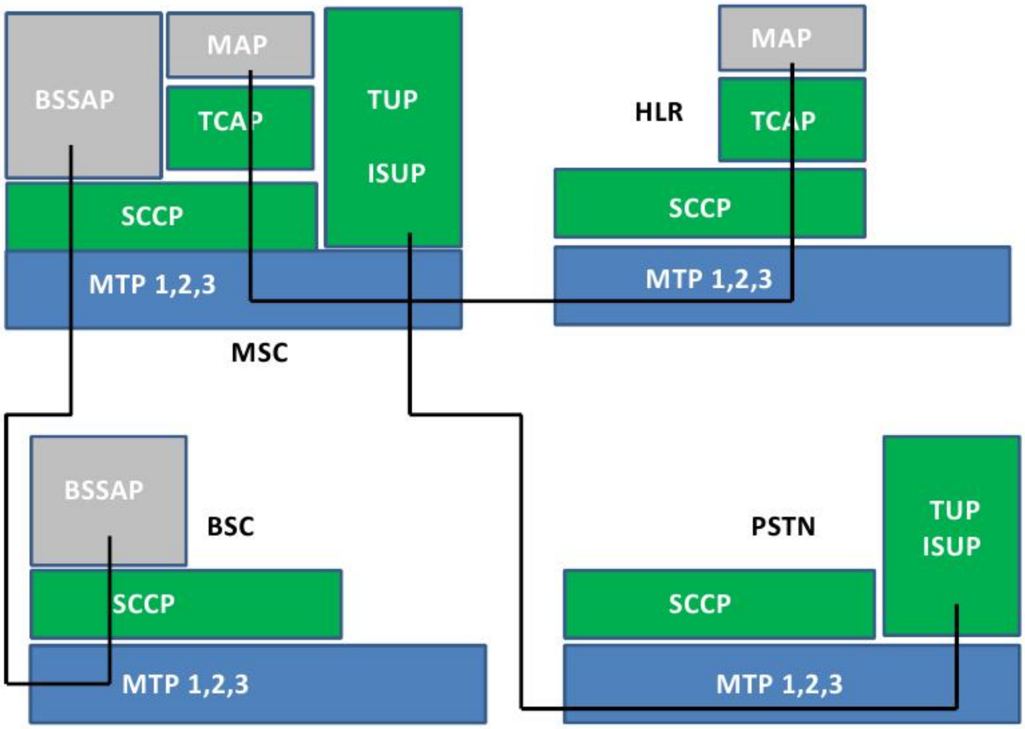


Figure 2.6: SS7 Protocols in Different Network Elements [44]

2.1.7 Limitations of SS7 Signaling System

Advances in technology more especially on the mobile platforms have meant that SS7 networks supporting wireless traffic are bursting at the seams. Due to backward compatibility and coordination considerations, moving forward with SS7 will be difficult as deploying dedicated SS7 signaling networks to support high speed multi- media streaming will prove to be commercially unviable and technically nearly, impossible.

The main drawbacks of SS7 signaling system to optimally support the recent boom in multi-media services include:

Scalability and Bandwidth

The standard link speed with SS7 is 64 kbps. This was designed to fit nicely within T1 trunks (which contain 24 circuits, each with a 56-64 kbps capacity) or E1 trunks (32 circuits running at 64 kbps). Dedicated links reduce flexibility and increase cost significantly when creating sufficient bandwidth for new service applications. In a TDM network, entire transmission segments must be reserved for each call, even if the TDM connection is idle.

In order to increase the capacity 16 SS7 links at a single SP can be implemented but still this is way far below the necessary capacity of signaling to handle multi-media streaming. It can be argued off course that capacity can be further expanded by implementing 1.5 Mbps links (i.e. an entire T1). Well, in theory this can be seen as true but in practice it is not so easy.

Despite the increased capacity due to the deployment of a maximum of 16 links at any SP, the SS7 protocol further recommends that links and linksets should be configured to no more than 40% of their maximum capacity, so that the alternate path can carry the full load of messages during failover [10].

Message Size, Addressing and International Routing

Application messages on an SS7 network are limited to between 200 and 250 bytes depending on the size of the message headers. Some recent versions of SS7 can support larger messages through message segmentation on any link but this is not easy to implement. Even if it is known that the destination signaling point supports this capability, segments may be lost if they encounter an STP that does not support it. And, with the number of routing options in SS7, determining the list of potential intermediate STPs is very difficult.

The fundamental address in SS7 is the point code system, which a unique number is assigned to a signaling point. Point codes are assigned separately by each network, and vary significantly in size, from 14 bits to 24 bits. Consequently, point code routing can only be used within a single national network and this limitation makes signaling more complex to all other countries.

The second address type in SS7 is known as the 'global title'. The global title may be translated into either an intermediate or destination point. In the case of international signaling the global title will first be translated into the point code of an international gateway which will perform protocol translation, and then translate the global title into a point code in the destination national network, or use global title routing to forward the message to an STP to perform this function.

Although International routing using SS7 is accomplished with global titles, it does not mean that the global titles are fully compatible between countries. The encoding of global titles is a national issue and this makes international gateways specialized and complex devices.

The major problem with global titles is the management burden they impose on STPs. Every STP has to have a set of routing tables for each type of global title, these must be customized for the position of an STP in the network and they have to be frequently updated. Errors in the global title tables could cause the loss of messages or even network failure.

2.2 Internet Protocol, Technology for the Future

2.2.1 Introduction

Despite the high reliability of the SS7 signaling networks due to dedicated signaling routes and high network elements redundancy which reduces the network failure rate and network service downtimes to as low as zero, however, there are still some shortfalls to the SS7 networks. These SS7 limitations can only be overcome through the use of Internet Protocol (IP) network service capabilities in the transportation of the SS7 messages.

The primary reason for the use of IP in transporting SS7 messages is to off-load the heavily loaded SS7 networks and make them scalable for the increasing amount of telephone and mobile users. The IP solution will also be used to connect isolated islands of SS7 networks, which otherwise would have required the deployment of a dedicated and expensive SS7 infrastructure.

In recent times the IP has changed the whole landscape and dynamics of the telecommunications infrastructure. Most of the traditionally Time Division Multiplexing (TDM) based telecommunications networks operators are making use of the IP offerings such as scalability, bandwidth, network availability and fast network growth and opportunities to realise better returns on their investment. Service providers cut costs when using SS7 over Internet Protocol (SS7oIP) by offloading data traffic from SS7 networks onto IP networks. SS7 over IP enables wireless service providers to rapidly deploy emerging IP-based services for the mobile Internet that freely interact with the legacy mobile infrastructure.

At present SS7 networks form the bulk of all telecommunications' core networks. According to the latest figures (Q2/2013) from the Global mobile Suppliers Association (GSA), "Of the 6.57 billion global mobile subscriptions only 126.1 million subscribers were LTE" [12]. This just reaffirms the fact that there will always be an interworking between the TDM-based and IP-based networks through the use of a composite signaling protocol type known as Signaling Transport (SIGTRAN).

Using the SIGTRAN protocols is the first step to merge SS7 networks with IP networks. Today's telecom companies are moving towards an all-IP network also known as the Next Generation Network (NGN), where IP will replace traditional telecom networks, but such a transition will not happen overnight, perhaps never, and the main task now is to enable these systems to co-exist and to enhance the services they provide.

In SIGTRAN technology, also known as SS7 over Internet Protocol (SS7oIP), the different nodes of the traditional TDM-based SS7 Network are signaled by SS7 protocol messages, which are piggybacked on the Internet Protocol for transportation purposes between distant Signaling Switching Points (SSP) or between an SSP and a Softswitch for the Voice over IP (VoIP) bound traffic.

2.2.2 SS7 over Internet Protocol

Long distance routing of telephone calls over an IP network is more cost effective than comparable routing over more conventional methods such as TMD-based circuit switching.

IP access standards are emerging that offer great flexibility. However, nowhere amongst the new generation of IP protocols had emerged one that offers all of the signaling capabilities of SS7. There was a need therefore to leverage the capabilities of SS7 in the IP world and to find a role for SS7 in soft switch architectures. A working group known as the Signaling Transport Group of the Internet Engineering Task Force (IETF)[22] was established to work on the requirements of transporting SS7 signaling messages over IP based networks without compromising on the SS7's capabilities and reliability. The IETF group came up with the Signaling Transport (SIGTRAN) standards.

The SIGTRAN standards, as they are known, describe a way of presenting SS7 signaling information over an IP transport in such a way that all of the benefits of SS7 are maintained. The standards allow next generation IP-based networks to interface with existing SS7 networks and to exchange information with no loss of service capability. SIGTRAN decomposes the SS7 stack and allows different layers to communicate using an IP transport layer. Instead of using MTP as a transport protocol, SIGTRAN separates this from the user parts and simply transports the information that would be passed to each layer of an IP infrastructure.

For message delivery over IP on the Internet two transportation protocols have been defined. These are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), but for real-time signaling they exhibit certain limitations which make them unsuitable for the task.

The User Datagram Protocol (UDP) was developed purposely to provide a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. This protocol presumes that the Internet Protocol (IP) is offered as the underlying protocol. It makes provision for application programs in transporting messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed. The UDP is a connectionless transport protocol and does not intrinsically employ acknowledgement (ACK) messages to guarantee reliable and ordered transportation. The UDP is mostly helpful in situations where high transmission rates are required, but does not necessarily fulfill the other performance conditions of SS7 signaling messages [13].

TCP is a byte oriented transport protocol which offers a stream of bytes and guaranteeing their ordered delivery. This is necessary particularly during transmission of huge volumes of data as applicable in emails application and file transfers, but the strictly in-order-delivery is responsible for its unsuitability for signaling messages. TCP is highly sensitive to delay variance arisen from the packet loss and therefore leads to retransmissions. While waiting for lost packet for acknowledgement, the remaining packets will be delayed, known as head-of-line blocking. This usually lead to unnecessary delays for the remaining packets; and as such TCP is unsuitable for real-time applications, such as Voice over IP (VoIP). In establishing a TCP connection, Host 1 sends a SYN message to Host 2 which is replied with a SYN-ACK. Then Host 2 will hold on for the corresponding ACK from Host 1, the last step in the three-way handshake in the TCP connection setting. However, this procedure may be susceptible to some type Denial of service (DoS) attack known as SYN attack, originated from the numerous SYN messages that are sent to Host 2 of which they utilized some memory resources and may subsequently end up to collapse Host 2 and legitimate users will be denied of obtaining the available service. This scenario is not tolerated in SS7 network of which telephone services are expected to be always readily available [14].

The key desired characteristics of network signaling transportation are: Ordered and reliable message transfer, redundancy in case of link a failure, low loss and delay and security against denial of service (DoS) attack. UDP and TCP cannot support all these requirements, hence a new transport protocol was designed by SIGTRAN, the Stream Control Transmission Protocol (SCTP) that improves upon previous TCP and UDP to ensure reliable transfer of information in a way that meets the requirements of SS7 systems.

2.2.3 SIGTRAN Protocol Stack

As discussed in subsection 2.2.2 on page 21, SS7 signaling messages have very stringent loss and delay requirements. TCP falls short of those requirements and is not a suitable choice, because the delays are too long while UDP does not provide sufficient reliability. The SIGTRAN protocol suite was therefore developed to bridge the reliability and performance gaps between the two conventional IP transportation methods.

The SIGTRAN protocol suite includes the transport protocol SCTP, along with several user adaptation (UA) layer protocols that are necessary for the transportation of SS7 messages over IP, See Figure 2.7.

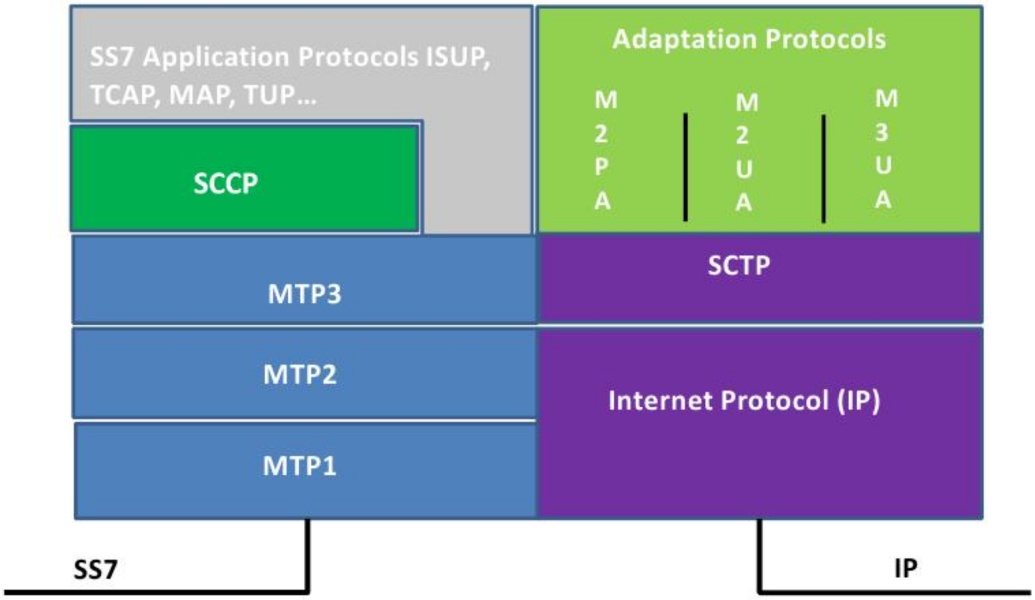


Figure 2.7: SIGTRAN Interface Protocol Stack [48]

The SIGTRAN architecture consists of two main layers:

- Common signaling transport - supports the error-free, in-sequence delivery of application messages. It includes the underlying IP network layer and the SCTP.
- User Adaptation layers - supports specific primitives required by a particular signaling application (e.g. M2PA, M2UA, M3UA, and SUA)

Stream Control Transmission Protocol (SCTP)

The Stream Control Transmission Protocol (SCTP) was primarily developed to transport telephony SS7 messages over IP networks with the objectives to duplicate reliability and performance features of SS7. SCTP is an application level datagram transfer protocol that operates on top of an unreliable datagram solution like UDP or TCP.

The SCTP protocol is equivalent to TCP since it offers both flow and congestion control mechanisms, however it has two major features that enhance its reliability and performance thus making it more suitable for SS7 signaling transportation. These features are multi-homing and multi-streaming [15].

Multi-Homing

Like SS7 signaling, multi-homing features provides redundancy in IP transmission of signaling messages using SIGTRAN. Multi homing feature of the SCTP allows each network node to have several IP-addresses, where each IP-address pair between two nodes is called a path.

Each path between the two physically connected network nodes is associated with heartbeat messages which indicate an active or inactive mode. Each node chooses a primary path and if a failure occurs on this path, retransmissions are sent via an alternative path (if available). After a specific number of retransmissions, a path is considered inactive and a new path is chosen, and if it is active, then it becomes the new primary path.

In Figure 2.8, node A has three paths (associations) to node B and node B has four paths (associations) to node A.

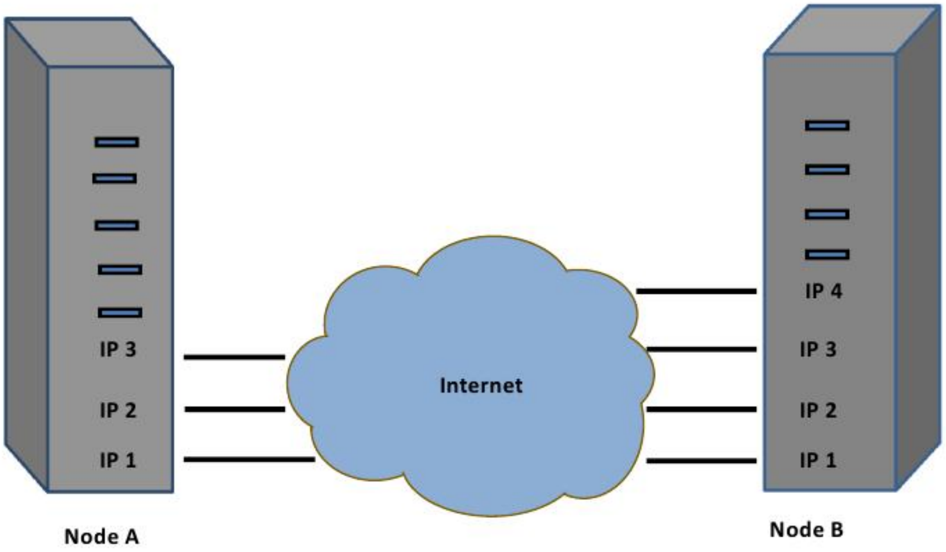


Figure 2.8: SCTP Multi-Homing Feature [15]

This multi-homing feature enables a network to reroute data to other IP addresses, thus the network is more tolerant of physical link failures. In a classical SS7 network there are always at least two physically different paths over which to transmit data. Since SIGTRAN should provide an IP solution with all the qualities of the SS7 network, the multi-homing feature can be used to provide the same level of redundancy as in SS7 signaling networks.

Multi-Streaming

The multi-streaming feature of the SCTP helps to reduce delays in call establishment and also reduces network congestion when using SIGTRAN transport protocol suite in transporting SS7 signaling messages. SCTP multi-streaming is the sending of data packets in multiple, simultaneous and independent streams so that if there is a data loss in one stream, delivery will not be affected for the other streams. These multi-streams are possible without opening separately multiple connections between the two nodes. Multi-streaming is used to avoid head-of-line blocking, which is a common phenomenon in normal TCP, as shown in Figure 2.9 .

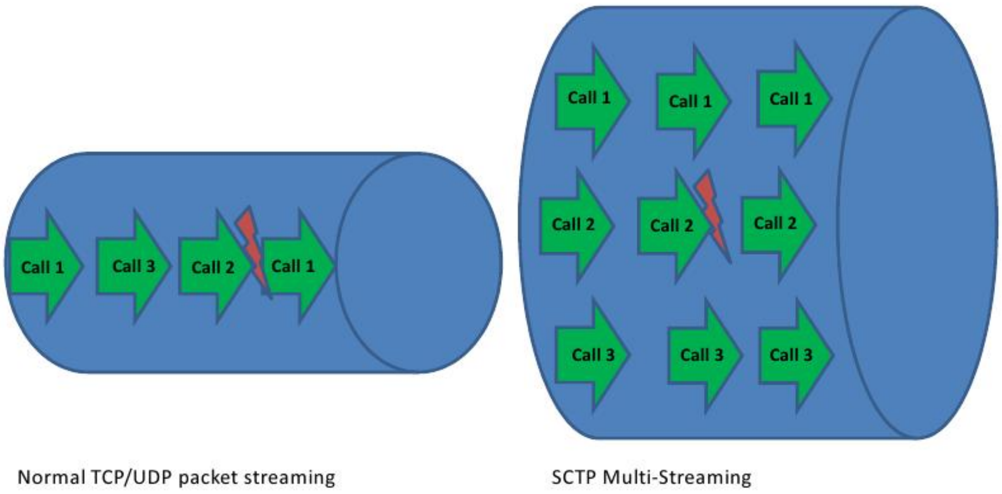


Figure 2.9: SCTP Multi-Streaming Feature [15]

In normal TCP streaming of data, when a signaling packet for a call is lost the whole connection is blocked while waiting for a retransmission, resulting in head-of-line blocking. The delay for recovering the lost data can be several milliseconds or even seconds. This signaling delay is not acceptable while making a phone call using SS7 signaling. In SCTP streaming with reference to figure 2.9 above, an association between two nodes can have several streams, each one assigned to a particular resource or application. Loss of message relating to call 2 affects only that stream of data. Calls 1 and 3 are serviced as normal.

Creating several streams with TCP is also possible, but requires opening multiple TCP-connections where each one acts as a stream. Every connection introduces a Transport Control Block (TCB) at the server side, which contains all the important information about a connection. These TCBs consume memory, and their numbers could be significant for a busy signaling point with various clients, hence multiple TCP connections are not a desirable alternative [16]. Also using only one SCTP association with streams instead of several TCP connections helps to reduce unnecessary call setup times.

SIGTRAN is therefore a preferred protocol to transport SS7 messages over IP due to the multi-homing, multi-streaming and many other enhancement features of the SCTP transport layer.

Table 2.1 highlights the main differences between several features of the three known IP transportation protocols namely TCP, UDP and SCTP.

Feature	**UDP**	**TCP**	**SCTP**
Congestion control	x	✓	✓
Connection-oriented	x	✓	✓
Unordered data delivery	✓	x	✓
Full duplex	✓	✓	✓
Multi-streaming	x	x	✓
Preserve message boundaries	✓	x	✓
Ordered data delivery	x	✓	✓
Multi-homing	x	x	✓
Allow half-closed connections	N/A	✓	x
Reachability check	x	✓	✓
Protect against SYN flooding attacks	N/A	x	✓
Flow control	x	✓	✓
Selective acknowledgements	x	Optional	✓
Reliable data transfer	x	✓	✓

Table 2.1: Feature Comparison Between UDP, TCP and SCTP [45]

User Adaptation Layer Protocols

The User Adaptation layer protocols support specific primitives required by a particular signaling application. The main user adaptation layer protocols which are commonly used in SIGTRAN are the MTP2 Peer-to-Peer Adaptation Layer (M2PA) protocol, MTP2 User Adaptation Layer (M2UA) protocol and MTP3 User Adaptation Layer (M3UA) protocol [17]. The user adaptation layers are named according to the service they replace other than the user of that service. For example M2UA adapts SCTP to provide services of MTP2 rather that providing service to MTP2.

These SIGTRAN adaptation layers serve a number of purposes which include [17]:

- To carry upper layer signaling protocols over a reliable IP-based transport.
- To provide the same level of class of service offered at the interface of the SS7 network.
- To be transparent. The User of the service should be unaware that the adaptation layer has replaced the original protocol.
- To remove as much need for the lower SS7 layers as possible.

MTP2 Peer-to-Peer Adaptation Layer (M2PA) protocol

M2PA provides a peer to peer mode of operation in backhauling SS7 signaling messages over an IP network. It replaces an MTP2 link beneath MTP3. The user of M2PA is MTP3 on both ends of the connection.

M2PA provides a means for peer MTP3 layers in SGs to communicate directly. This protocol is used for SG to SG connection and is best suitable for bridging two SS7 network islands.

M2PA is mainly responsible for link activation/deactivation in response to requests from MTP3, maintaining link status information, maintaining sequence numbers and retransmit buffers for retrieval by MTP3 and maintaining local and remote processor outage status.

MTP2 User Adaptation Layer (M2UA) protocol

M2UA is a protocol for the backhauling of SS7 MTP3 messages over an IP network and is used between a Signaling Gateway (SG) and a Media Gateway Controller (MGC) in VoIP networks. M2UA provides an interface between MTP3 and SCTP that enables MTP3 applications to transparently operate over an underlying transport service of SCTP and IP instead of MTP2. This interface provides transparent connectivity between traditional circuit-switched SS7 signaling points and Next Generation, IP-enabled signaling elements, such as a Softswitch or Media Gateway Controller.

M2UA protocol is used where network devices are connected in a client–server mode, i.e. MGC as a client and SG a server. M2UA backhauls provide a method of communication for an MTP3 layer on an SS7 device to reach Media Gateway Controllers, as well as database applications and other applications with peer MTP3 layers that run on IP-enabled devices.

MTP3 User Adaptation Layer (M3UA) protocol

MTP3 User Adaptation (M3UA) protocol was developed by the IETF for the transport of any SS7 MTP3 User signaling (e.g. ISUP, SCCP and MAP) over IP, using the Stream Control Transport Protocol (SCTP). M3UA can also work in diverse architectures, such as a Signaling Gateway to IP Signaling Endpoint architecture as well as a peer-to-peer IP Signaling Endpoint architecture [18].

M3UA provides the service of MTP3 between SG and application server. M3UA supports MTP3 users ISUP and SCCP. M3UA replaces SS7 signaling link, signaling link set, combined link set and signaling routes. M3UA is designed to allow legacy SS7 TDM nodes to communicate with SIGTRAN IP-capable nodes.

2.2.4 SIGTRAN Integrated Network Architecture

As mobile communications evolve, mobile end-users are offered wideband multi-media capabilities. The associated multi-media streams require that the networks should be more flexible at providing bandwidth on demand than present-day networks which are based on TDM. The networks transport technology must thus evolve toward cell and packet based technologies.

Though regarded as a legacy signaling system, SS7 signaling based network components which include the MSCs, SSPs STPs, HLRs and the Signaling Gateways (SGs) continue to claim a lion's share of the telecommunications market. A number of factors have energised this SS7 signaling growth beyond simple "call control" to provision enhanced services for TDM and IP domains. These factors include new subscriber growth rates in emerging markets, steady growth in SMS messaging, VoIP-enhanced services, and interoperability between the legacy SS7 based TDM networks and next-generation networks.

The driving force behind the interoperability between the TDM based SS7 networks and the emerging IP-based IP Multimedia subsystem (IMS) networks using the SIGTRAN protocol translation technology is the Signaling Gateways (SGs).

SGs transport application signaling between the SS7 network and the IP network, serving to bridge legacy TDM based networks with the packet-switched, next-generation networks. SGs implement SS7 protocol stack and related SS7-over-IP SIGTRAN subcomponents and handles mobility protocols for interworking with wireless networks. When used in conjunction with soft switches, media gateways, application servers, and media servers, SGs provide the call control functionality and service processing capabilities of traditional PSTN switches [36].

Figure 2.10 shows the signaling network interoperability between the Cellular Network, PSTN and the IP network using the SG.

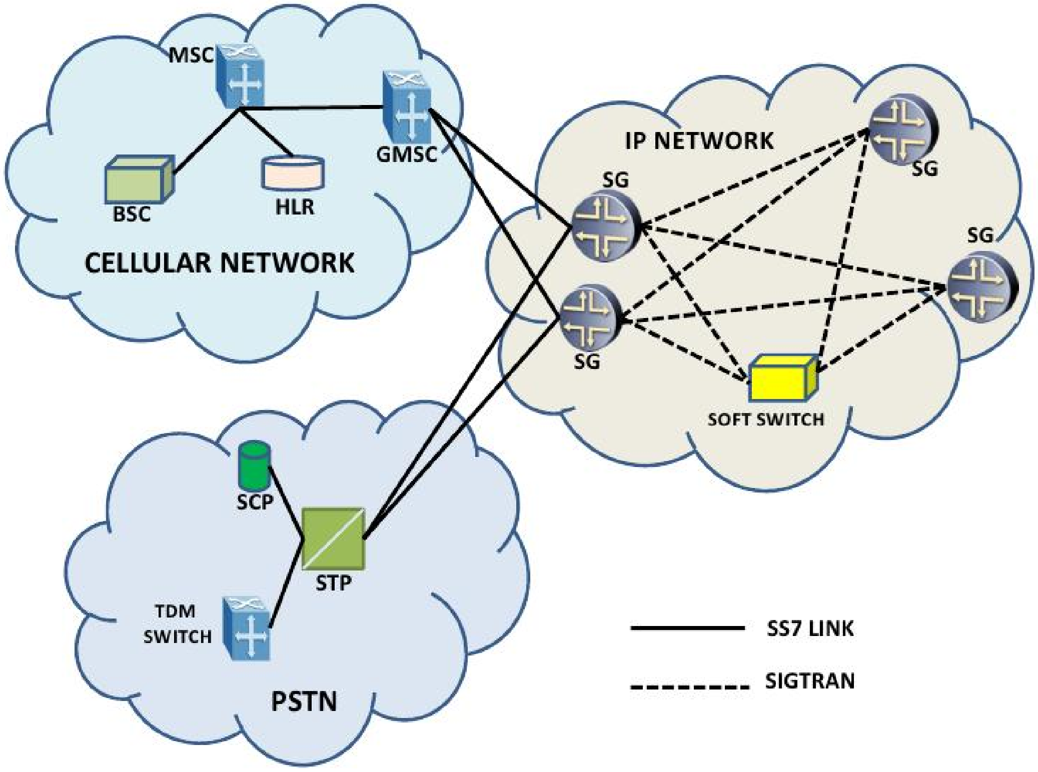


Figure 2.10: Internetwork Signaling Connection Using Signaling Gateway [36]

From the network interoperability shown in Figure 2.10 above, only logical signaling interconnection is represented as the physical network elements locations and positioning can be totally different.

2.2.5 SIGTRAN Simulation Implementations

SIGTRAN is getting adopted quite fast because it is the only integrating catalyst between the two merging technological systems, SS7 and IP.

There are many commercial implementations of SIGTRAN stack. Many of the big players participate in the European Telecommunications Standards Institute (ETSI) Plugtest Service. The ETSI Plugtest Service is a professional unit of the European Telecommunications Standards Institute (ETSI) that specializes in arranging interoperability test events for companies, organizations, and standardization bodies (ETSI, Internet Engineering Task Force (IETF), International Telecommunication Union (ITU), etc.) [53]. These tests are in the area of telecommunications, Internet, broadcasting, and multimedia. Some of the main players include, just to name a few; Adax, Cisco

Systems, Ericsson, Hewlett-Packard, Siemens, Intellinet, Performance technologies and Ulticom.

Additionally, there are plenty of free Proprietary and Open Source SIGTRAN implementations available via the Internet [25], and the purpose of these is to be able to test an "SS7 over IP" solution. Most of these only implement the SCTP protocol, while the user adaptation layers are only available in a few of them. The following subsubsections explain in brief some of the popular freely available SIGTRAN implementations:

Siemens/University of Essen Implementation

This implementation [26] was designed by Siemens, the University of Essen, and the University of Applied Sciences, Germany. It is only an implementation of SCTP. It runs on Linux 2.4, and 2.6, FreeBSD 4.8, Solaris 8, Mac OS 10, and Windows (with some limitations). Moreover, it supports both IPv4 and IPv6 and includes a SCTP test tool. With the test tool you can verify that your installation is correct and try the test cases.

Berkeley Software Distribution (BSD) with KAME Project Implementation

The KAME project [27] is a joint effort between six Japanese companies to create a single solid software set, especially targeting IPv6/IPsec. It works on FreeBSD 4.0, OpenBSD 2.7, NetBSD 1.5, BSD/OS 4.2, and newer versions of these. The project was aimed at providing free reference implementations of IPv6 and IPsec (for both IPv4 and IPv6) stack for BSD variants and provides advanced internetworking such as advanced packet queuing, mobility, etc.

Linux Kernel SCTP (LKSCTP) Implementation

The LKSCTP project [28] was started by one of the inventors of SCTP – Randall Stewart – in cooperation with Motorola. This implementation supports SCTP, and also provides test tools with numerous test cases. It can be run on both IPv4 and IPv6. To install the package, a Linux-2.5.36 or later kernel version is necessary, and it has to be configured with the network options "SCTP Configuration" support enabled.

Sun SCTP Implementation

Sun Microsystems' SCTP is another pure SCTP implementation which runs on Solaris 9, update 6 [29].

Open SS7 Implementation

The OpenSS7 [30] project started in 1996 but was initially only an SS7 stack. The SIGTRAN features were introduced in 2001 and include the SCTP protocol and the M2PA user adaptation protocol. The other UA (user adaptation) protocols exist (M2UA, M3UA and SUA), but are still at a testing stage and have not yet been released. There is also a TCP implementation available for comparisons between the two transport protocols (SCTP vs. TCP).

OpenSS7 project is still in production release for many of its components; some code is still being worked on and is not really suitable for public release. Only the source code is available for those that are interested in following the development.

There is an interest in widening the OpenSS7 SIGTRAN stack to also include mobile communication parts, such as a home location register (HLR) with GPRS capabilities. This project is still in the design stage and is currently on hold.

OpenSS7 was developed for the Linux kernel. It currently requires the 2.4.10+ kernel and a C compiler (gcc) capable of compiling the Linux kernel.

Dialogic SS7/SIGTRAN Implementation

Dialogic SS7/SIGTRAN Implementation is a proprietary SS7 development kit of Dialogic Corporation which is a worldwide telecom equipment supplier, serving both enterprise and service provider markets. Dialogic's broad product range incorporates media gateways, media servers, signaling gateways and media boards, and embraces both traditional TDM technology and VoIP/SIP [31].

This simulation implementation has been used for testing the experiments in this study and has been discussed in detail in Chapter 4.

2.3 Review of Previous Work

In the recent past a lot of effort has been put into researching the interoperability between the TDM-based SS7 signaling system and the Internet Protocol. The areas of study range from the social and economic benefits (to both the subscribers and the network operators) of migrating services from SS7 to all IP, through the performance analysis of the IP network in transporting SS7 without compromising the quality of service to the problems that have resulted from the interoperability.

This literature review encompasses online research into journal articles, conference papers, thesis studies and library studies into relevant text books covering topics similar to the subject matter.

According to Klaus D. Gradischnig and Michael Tuxen in their publication "Signaling transport over IP-based networks using IETF standards" [22] reliability features of SS7 are compared to those of the SIGTRAN. The paper identifies parameters which have to be adjusted and restrictions to available addressing options which have to be made in order for the SIGTRAN protocol stack to achieve the reliability and performance of SS7. The authors identify SCTP as a modified IP transportation layer for achieving the performance and fault detection capabilities needed for signaling applications. Also assigning IP based elements like MGCs their own point codes allows seamless network management in an SS7 network crossing the MTP/IP boundary. In combination this results in a converged signaling network architecture which can deliver the reliability and performance end users of the SS7 signaling driven network have become accustomed to.

The redundancy and reliability characteristics of IP based signaling networks were investigated in a thesis by Mia Immonen "Signaling over IP — a step closer to an all-IP network" [16]. In this study the performance of the two features of the underlying SCTP layer of the IP protocol stack namely multi-homing and multi-streaming were measured against the known performance features of SS7 signaling. The multi-homing experiments carried out in this paper, suggest that SCTP does meet the performance requirements for signaling even though the message transfer times in the case of a link failure were achieved with a large margin of error observing that the time it takes to detect a failure strongly depends on the number of maximal path retransmissions. Being liberated from the extremely complex TCP retransmission behaviour, the SCTP protocol can be used for a reliable transportation of Media over IP (MoIP). When providing a multimedia transfer with related but yet independent data streams, e.g. voice and video, the SCTP multi-streaming feature is suitable, so that head-of-line blocking and multiple TCP connections are avoided.

With the widespread of mobile internet in the recent years, Dong W. Kang, Joo H. Oh, Chae T. Im, Wan S. Yi and Yoo J. Won in their paper "A Practical Attack on Mobile Data Network Using IP Spoofing" of July 2013 [23] highlight the security threats which have been posed due to the abnormal traffic of mobile networks which results from IP spoofing. As IP Spoofing is not taken seriously in the mobile environment, the resulting security threats were not taken into consideration in a big way, but IP Spoofing in the mobile environment can lead to overbilling and power consumption for certain UE, occupy the wireless resources of the mobile network, and induce abnormal traffic into components in the mobile network.

With the growing acceptance of the SIGTRAN protocol suite for transporting SS7 signals across IP networks, there is a need to secure both SS7 and IP networks. Still, most of the focus is on securing the public IP network, leaving SS7 network vulnerable and the signaling gateway virtually untouched. One reason for this disequilibrium may be the folklore that the SS7 network is secured enough and, consequently there are no threats. Hemant Sengar and Ram Dantu in their publication [24] argue the opposite, by showing some example exploits of fabricated messages or malicious (hijacked) signaling nodes. Even misconfigured SGs, STPs, SSPs, and MGCs can generate spurious messages and consequently affect other signaling nodes by shutting them down or by functioning erratically.

Cross Network Services are a new breed of services that have spawned from the merger of the Internet and the previously isolated wireless telecommunication network. These services act as a launching pad for a new type of security threat - the Cross Infrastructure Cyber Attack. The paper "A Taxonomy of Cyber Attacks on 3G Networks" [1] proposed attack taxonomy for 3G networks. The uniqueness of this taxonomy is the inclusion of Cross Infrastructure Cyber Attacks in addition to the standard Single Infrastructure attacks. This paper also proposed an abstract model of the 3G network entities. This abstract model has been a vehicle in the development of the attack taxonomy, detection of vulnerable points in the network and validating 3G network vulnerability assessment tools. The paper also examined the threats and vulnerabilities in a 3G network with special examination of the security threats and vulnerabilities introduced by the merger of the 3G and the Internet.

As VOIP and PSTN coexist despite their technical differences, the internetworking of these networks presents a significant challenge because VoIP and PSTN use widely varying infrastructures and protocols. Interoperability issues arise because of differences in protocols, vendor implementations, the carrier used, and the services provided. Internetworking makes the infrastructure more vulnerable to attacks therefore interoperability issues need to be addressed at every interconnection point of the network components. Ram Dantu, Sonia Fahmy, Henning Schulzrinne and Joao Cangussu identify compromised Signalling nodes and Spoofing as the two examples of attacks on a SIGTRAN network [55]. Internetworking increases the possibility of signaling nodes' being compromised in the signaling system (SS7) or IP networks. The compromised node can then exploit the signaling messages to disrupt telephone services. Spoofing can be used to compromise data integrity and thus prevent the use of the technology in critical domains. When VoIP and PSTN interwork together, the traffic passing through the gateways must be screened. SS7 network's gateway screening, the only widely deployed security solution available today, does not check the actual content and structure of the VoIP signaling messages. The inability to interpret or properly parse messages with inappropriate content may cause a serious problem at the signaling node and thereby affect telephone services.

Today's telecom networks are a combination of the traditional circuit switched (TDM) and packet switched (Internet Protocol (IP) based switches) networks. IP based interconnect allows different sectors/services such as telecom, data, radio and television, to be merged together to provide huge bandwidth, consolidate terminating traffic and reduce long-distance charges. Now all new networks being deployed by the operators are using IP based systems because of the inherent advantages of using common backbone infrastructure for different type of services. However this transition has a lot of challenges. U.C. Meena, R. Saji Kumar and J.M. Suri in their publication "Interconnect Issues in IP Networks" [56], points out that the IP network including the interconnect interfaces use open protocols which are universally accessible, so the networks are susceptible to denial of service attacks, exposure to remote attacks and data theft. Hence the challenge is in protecting the gateways and control systems from intruders.

As the telecommunications industry migrates to the packet-based network paradigm, it now faces fresh challenges in securing its networks, as end-users have access to networks like never before. As such, new approaches to security are critical. Today, logical and physical security elements of the network must be designed in (from the beginning) and not retrofitted. Operators seek to ensure there is no malicious action between the customer and the system, or between the operations force and the system, or even between the system elements in the case of an indirect attack. With 80-85% of the communications critical infrastructure residing in the private sector, responsibility for ensuring network integrity falls on private industry. According to the Alliance for Telecommunications Industry Solutions (ATIS) [57], a collective effort between different industry role players is key in securing the telecommunications networks. The standards bodies are challenged to address carrier class security issues and architecture, the vendors need to produce equipment and software that meet security needs, and the customers and carriers need to work together to mitigate security threats.

Due to the exponential growth of mobile data traffic, mobile network operators are adapting and deploying key data offloading technologies such as femtocells not only to boost their network capacity but also to increase indoor cellular coverage. However, the consequences of such integration of two architectures over the Internet together with an array of security threats that originate through a rogue femtocell have not been fully analysed. Ravishankar Bhaskarrao Borgaonkar in his thesis “Security Analysis of Femtocell-Enabled Cellular Network Architecture” [58] investigates security architecture of femtocell-enabled cellular network that facilitates integration of these two architectures by evaluating impact of compromised femtocells on the fundamental security aspects of cellular systems - integrity, confidentiality, authenticity, and availability.

The Stream Control Transmission Protocol (SCTP) does not retain state information at the server side to avoid the traditional denial of service attacks. Unfortunately, SCTP is not secure against verification-tag guessing-attack which leads to association-hijacking and forces that victim clients to starve out of services. A secure SCTP mechanism called SCTP-Sec that includes Cookie mechanism as base to make the server a stateless, while it uses cryptographic hash operation to resist against the verification tag and hijacking attacks was proposed by Rahul Choudhari and Somanath Tripathy [59] in their publication called SCTP-Sec: A secure Transmission Control Protocol.

From the reviews of previous work done regarding SIGTRAN transport protocol, a vast amount of research effort has been put into investigating the reliability and performance characteristics of SCTP layer of the SIGTRAN transportation technology. Since intersignaling phenomenon is new to most mobile network operators who were very much used to managing the closed SS7 networks. This study therefore aims at validating the need for more research focus and further investigations into the security aspects of the SIGTRAN technology as the interworking between SS7 and IP networks become more relevant now than ever before.

2.4 Conclusion

The merging of SS7 based signaling system with the IP based signaling has brought about tremendous benefits to both the Mobile network operators and the subscribers. The demand for data-centric services such as Short Message Service (SMS) and Unified Messaging has created an opportunity for 3G carriers to capitalize on new revenue generating opportunities. Carriers significantly reduce SS7 transport costs by replacing expensive long-haul dedicated signaling links with very competitively priced IP connectivity between network elements. Service providers cut costs with SS7 over IP by offloading data traffic from SS7 networks onto IP networks.

The performance characteristics of SS7 signaling networks are incomparable to any other signaling transport system. The high redundancy rate in SS7 system makes the network performance fast and reduces considerably the network downtimes to as low as zero. This is why the IP transport systems such as the TCP and UDP in SIGTRAN had to be reinforced with an extra protocol layer, the SCTP, above the IP layer to provide similar performance and reliability characteristics as the SS7 networks.

Despite the revolutionary talk of all IP next generation networks, such are the capabilities of SS7 that it will become an integral part of the telecommunications infrastructure. More importantly, however, there is a tremendous investment in the conventional network that has not stopped. SS7 requirements continue to grow and access to SS7 signaling remains as essential as ever. For most operators SS7 is the preferred means of network connectivity and is not a matter of choice. New standards that built on its proven capabilities are emerging, such as Wireless Intelligent Network

(WIN) and Customised Application for Mobile Enhanced Logic (CAMEL) [54], and it is destined to play a huge role in 3G Mobile networks. In the network core it is likely to remain unchallenged for some considerable time and with the advent of new IP-based SS7 networks; it is likely to play a key role in the next generation networks. However the security challenges that might arise due to the interworking between the traditional SS7 and the IP networks have led to the Key Research Question this study aims to address.

Chapter 3

Key Research Question

3.1 Introduction

In this chapter the key research topic is explained.

In a typical 3G mobile network set-up, a subscriber (mobile station) gets services from the network via the access network and the access protocols such as LAP-Dm are used for signaling, while SS7 signaling is only used in the core network. SS7 networks are often physically inaccessible to end-users, so they are considered to be protected from attacks, since the network equipment is behind locked doors.

However, Voice over IP (VoIP) telephony is emerging as an alternative to public telephones, due to its convenience, cost effectiveness, and the ease of designing new services. Consequently, there has been a need to interoperate signaling and media between these two competing services. Also IP networks due to their ease of deployment, flexibility in offering new services and cost effectiveness are being considered as the best possible option in transporting signaling messages between two distant TDM-based SS7 networks which would otherwise be costly to deploy an own dedicated SS7 signaling network.

The signaling interoperation, made possible by using the signaling transport (SIGTRAN) protocol suite proposed by the Internet Engineering Task Force (IETF), allows any subscriber in either network to transparently call another subscriber in either network.

3.1.1 Review of the Problem

As the demand for multimedia-based traffic started to exponentially increase with users demanding for more freedom of mobility without any service disruptions while not compromising on the quality of service, it became clear that the SS7 driven 2G/3G legacy mobile telecommunication systems which were optimally designed for voice performance, were soon going to get saturated.

The high demand for these services then led to the design of the Next Generation Network (NGN) systems that would be data optimised to provide more capacity and high data rates while at the same time efficiently utilising the licensed radio spectrum. A system was required that would be capable of satisfying the ever increasing appetite for data traffic and enhance performance in the long run. Long Term Evolution (LTE) technology was identified as the way forward and the future of high speed Cellular services.

Despite the high hype of LTE offerings, realising a full migration from 3G to LTE in any foreseeable future is merely a dream. A number of issues ranging from regulation, through high network deployment costs to fewer LTE ready mobile equipment need to be addressed first before a full transition to LTE from 3G networks can be realised. Most operators will roll out LTE first in small portions of their networks, which is why Informa Telecoms and Media forecasts North America will achieve 56% penetration by 2017, with the world's second largest LTE region, Asia Pacific expected to reach just 11% penetration by 2017 [52].

Switching from 3G network systems to LTE does not require network infrastructure upgrades but rather calls for a complete infrastructure replacement which makes it economically not easy for network operators to deploy the LTE networks, operators are therefore rolling out LTE networks in phases. Lack of regulation in allocating the required spectrum for LTE by National regulators coupled with high spectrum auctioning prices has forced the mobile network operators to resort to using spectrum re-farming. Lastly the network operators are faced with a dilemma of what to do with the billions of subscriber mobile equipment in circulation using 2G/3G which are not LTE ready.

Signaling in pre-4G/LTE networks (2G/3G) is based on SS7. Commercial 2G and 3G networks worldwide make extensive use of SS7 signaling both within their own network and between networks. It is estimated that 2G will represent half of all the mobile network connections through 2017[1]. 2G and especially 3G networks will continue to co-exist with the LTE until all the networks have fully migrated to 4G/LTE a feat which is likely not going to happen in any foreseeable future.

The arguments above just re-affirm the fact that although LTE is a future technology for mobile/cellular networks, the legacy 2G and 3G networks will still play a key role for a long time to come and there will always be an interworking between these two technologies and all the other IP related services.

Most mobile operators are making use of IP networks to transport signaling messages between two distant TDM-based SS7 networks using the Signaling Transport (SIGTRAN) protocol suite [19]. This is done in order to take advantage of the IP offerings such as scalability, bandwidth, network availability and fast network growth and opportunities. SIGTRAN technology is also used to offload IP bound traffic such as VoIP by interconnecting SS7 core networks and the IP's Softswitch.

The introduction of Internet connectivity and many more IP based services to 3G networks through network interconnections imports not only the high speed capabilities of the Internet but also very high risks of cyber-attacks which may be launched from the IP side of the network.

Understanding that 2G and 3G networks will be with us for a very long time, and owing to the fact that more and more networks are being migrated to the next generation's all IP networks, this research was aimed at identifying if IP networks, through network infrastructure interconnections, are vulnerable to security threats as compared to the once isolated and secure SS7 signaling networks. Once the vulnerabilities, if any, have been identified some mitigating factors would be proposed. The key research question for this proposed thesis reads as follows:
"There is much emphasis these days on the security of communications, and there are some solutions available in the market place for voice and data. However it is anticipated that 2G and 3G communications technologies will be with us for a lot longer than we think, and thus SS7 will also be a driving force to communication. What are the vulnerabilities of Signaling System Number 7 to cyber-attacks and how can we mitigate against these vulnerabilities?"

3.1.2 Objective of the Investigation

Through the findings of this research, we aimed to establish if an IP network can pose as a source of potential cyber threats to a 3G TDM-based SS7 network through the interconnection between these two technologies. Also the motives behind the cyber-attacks would be briefly highlighted and some solutions in trying to avert the cyber-attacks would be proposed.

An SS7 network was originally designed as a closed network and thus more secure to external attacks. As the telecommunications networks started to open up, coming into one global network due to interconnection of different networks each using its own preferred choice of technology and also the need by the service operators to utilise the cheaper IP connectivity offerings, the cyber threats to the once closed SS7 network also increased. The cyber-attacks targeting a particular SS7 network node can easily be launched from the IP network interconnected to it using SIGTRAN transport protocol suite.

An SS7 network through SIGTRAN transportation can be targeted by cyber attackers for so many reasons such as but not limited to: theft of service i.e. interception of calling cards numbers and compromising of general communication privacy for subscribers. Hackers may also introduce harmful packets into the national and global SS7 networks so as to get control of call processing and accounting reports and obtain credit card numbers, non-listed numbers etc. Hackers may also read, alter, inject or delete messages SS7 signaling messages. Hacking can also result into denial of service to all network users, disrupting free and emergency calls. Capturing of gateways through hacking can cause re-routing of call traffic [20].

Telecommunication deregulation of 1996 [21] and liberalized economies have introduced many new players, known as Competitive Local Exchange Carriers (CLECs), thus increasing the number of interfaced access points to SS7, and thereby exposing new points for attacks. Also the interconnection of SS7 backbone networks to IP based networks can introduce some new threats to the SS7 signaling networks. As it will be show herein, one such interface to both networks, SIGTRAN, can be exploited as well unless care is taken.

Because of the interconnection between the SS7 network and the IP network, the investigation in this research was aimed at:
a) Identifying the vulnerabilities of an SS7 network which could come about due to its interconnectivity with an IP based network service using a SIGTRAN Media Gateway as a protocol converter.
b) Suggesting the mitigating factors to the identified vulnerabilities of the SS7 networks which could come about from the SS7/IP interconnectivity.

3.2 Conclusion

This chapter serves as a basic introduction to the subject of the vulnerabilities of SS7 signaling messages to cyber-attacks when transported over IP in the technologically merging environment and validates the need for this investigation by providing an overview of the problem statement, the objectives of the research.

SS7 and related technologies will be around for many years, if not decades; it will remain a vital part of mobile networks. For these reasons, SS7 must be supported and enhanced so that service providers keep pace with demands for more connectivity, capacity, complex applications, and security.

To successfully consolidate networks for economies of scale and to improve performance for end users, end-to-end signaling across 2G, 3G and 4G networks is needed [52]. For this reason it was worthwhile investigating, through experimentation, the cyber security threats that might arise due to the intersignaling between these technologically different networks.

Chapter 4

Methodology

4.1 Introduction

The research was performed using the experimentation approach which has been explained in details in the later sections of this research report. However, this chapter gives an overview of the approach used. With reference to the subject of study of the vulnerabilities of SS7 to cyber-attacks, special attention was placed on Signaling Transport (SIGTRAN) Technology, also known as SS7 over Internet Protocol (SS7oIP).

In SS7oIP arrangement, different nodes of the Mobile Wireless Network are signaled by SS7 protocol messages, which are piggybacked on the Internet Protocol for transportation purposes between distant Signaling Switching Points (SSPs) or between an SSP and a Softswitch for the Voice over IP (VoIP) bound traffic. The layout can be seen in Figure 4.1.

Note that the main focus area for the experimentation was the Packet Network.

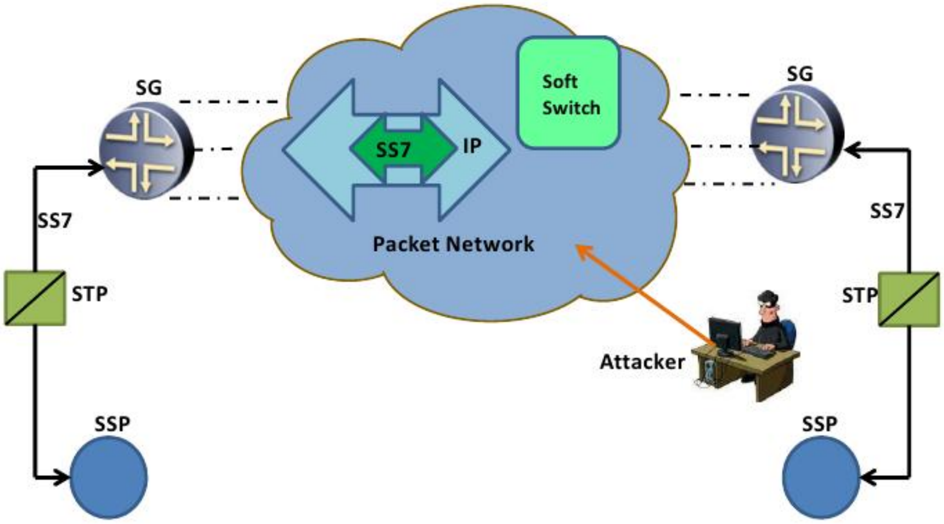


Figure 4.1: SS7 over IP (SIGTRAN) Experimentation Setup

With reference to Figure 4.1, the SS7 Signaling messages from distant SSPs are converted into SIGTRAN IP traffic at a SG. In this particular case, all SS7 messages are handled as payload data, and placed in the data octets after the first twenty bytes of the IP packet. IP reassembles packet datagrams back into the segments on the receiving side and each datagram is assigned the IP address of the source and destination node. Each router within the IP network (the layer 3 device) that receives a datagram makes routing decisions based on the packet's destination IP address. The resulting packetised SS7 traffic is then transported over an IP network to its destination be it another distant SSP or a Soft switch.

Now an attacker, using any network enabled computer connected in a **promiscuous mode** *"(an IP network interface mode in which the network interface card reports every packet that it sees)"* to the same IP network transporting the packetised SS7 messages, will be able to sniff the network and capture all the packetised SS7 traffic of interest. This computer will be equipped with Wire shark which is IP packet sniffing software and will be able to capture any packets passing through the network including the information about the source and destination IP addresses. Once this critical information has been uncovered, an attacker using network and packet manipulation software will destabilise or kill the network connections completely between the target IP nodes.

During the design of the research project, it was anticipated that access permission to a live SIGTRAN network to conduct the necessary security vulnerability tests would be secured. According to the initial design the testing would just demand plugging the probe straight into the network and monitoring the network activities between the different network nodes. However during the course of the study it was discovered that securing the permission was getting more difficult than was initially thought due to several concerns such as fears of interfering with the network operations if something goes wrong during experimentation and testing.

Considering the time constraints it was thought as wise to proceed with a simulation of the SIGTRAN network using one of the freely available SIGTRAN Implementation tools from the internet, an alternative way which would achieve similar results like testing in a live environment.

4.1.1 Dialogic SS7/SIGTRAN Network Simulation Implementation

The experimentation and testing done in this study to establish the vulnerabilities of SS7 signaling messages to cyber-attacks have been based on Dialogic SS7/SIGTRAN Simulation Implementation.

Dialogic SS7/SIGTRAN Implementation is a proprietary SS7 development kit of Dialogic Corporation which is a worldwide telecom equipment supplier, serving both enterprise and service provider markets. Dialogic's broad product range incorporates media gateways, media servers, signaling gateways and media boards, and embraces both traditional TDM technology and VoIP/SIP [31].

Dialogic SS7 development kit's software versions run on both Linux and Windows and is mostly used by SS7/SIGTRAN developers, experts and professionals to test different applications and also in online technical forums to brainstorm ideas, share best practices and tips or just chat about the latest emerging technologies making noise in the field of telecommunications signaling.

For development and testing purposes, the Dialogic SS7 development package has free software licences for simulation tests unless if implemented into a live environment after successful tests.

4.1.2 Devices and Software Used

To obtain a better understanding and analysis of the cyber threats to SS7 signaling messages while being transported over an IP network, critical evaluations were based on several systematic IP network security tests using Dialogic SS7 development package which is a propriatary but freely available internet software.

Key Assumption

With reference to subsection 2.2.3 on page 23, the assumption made in this study was that the SIGTRAN network under study was connecting two distant TDM-based SS7 networks. As a result the association (communication between SIGTRAN nodes) relationship between the two distant SG nodes was that of peers, therefore M2PA would be used instead of M2UA which works in a client – server relationship mode.

In order to perform these tests, the required equipment was as follows:
Two distant nodes (Win XP/ 7 Operating System based PCs)
One hacking device (Linux Operating System based PC)
A network Hub
Ethernet straight network cables
Dialogic SS7 Development Package
Dialogic User Part Development Package
Dialogic M2PA, MTP3, SCCP and TCAP, MAP host binaries, for SIGTRAN configuration
Wireshark network sniffing software
Ettercap packet manipulating software

4.1.3 Simulation Network Setup and Configuration

Figure 4.2 below shows network connectivity between the different network components used in the study. The role of each component is briefly explained in the later subsections.

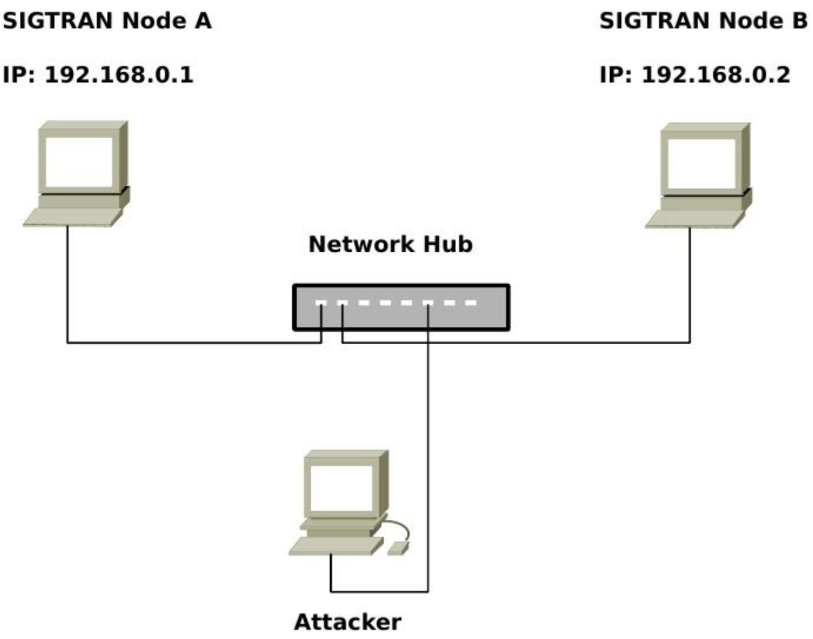


Figure 4.2: SIGTRAN Simulation Experimental Setup

Originating Node (A)

An HP Intel Duo Core 3.16, 3.17 GHz CPU computer running Windows 7 Enterprise 32bit configured to run as the Originating Signaling Gateway even though during the association the sending and receiving roles were reciprocatively reversed. In terms of the Dialogic terminology this particular node was referred to as the Mobile Application Part (MAP) Test Utility (MTU).

The application software running on this node included: Dialogic SS7 Development Package, Dialogic User Part Development Package and Dialogic M2PA, MTP3, SCCP and TCAP, MAP host binaries, for SIGTRAN configuration.

In this experiment, the static network configurations for this node were:

IP Address : 192.168.0.1

Subnet mask : 255.255.255.0

Default Gateway : 192.168.0.10

The system configuration file used was mtu.exe and this initiated a connection to the receiving node by constantly sending heartbeat signaling messages to the receiving node.

Destination Node (B)

The computer specifications for this node were similar to those of the originating node A. This computer was configured to run as Destination Signaling gateway so that it could respond to the heartbeat messages from the MTU. Similarly, this node was referred to as the Mobile Application Part (MAP) Test Responder (MTR) as per the Dialogic terminology.

Likewise application software running on this node included: Dialogic SS7 Development Package, Dialogic User Part Development Package and Dialogic M2PA, MTP3, SCCP and TCAP, MAP host binaries, for SIGTRAN configuration and mtr.exe is configured under system configuration.

In this study, the static network configurations for this node were:
IP Address : 192.168.0.2
Subnet mask : 255.255.255.0
Default Gateway : 192.168.0.10

Hacking Node

Two testing application software packages were installed on this node. These were Wireshark software and Ettercap.

As will be explained in the subsequent sections, Wireshark is a free and open-source packet analyser which captures packets in real time and displays them in human-readable format, and also Ettercap is a free and open source network security tool for man-in-the-middle attacks on a Local Area Network (LAN). Ettercap is able to perform attacks against the ARP protocol by positioning itself as ”man in the middle” and, once positioned as this, it is able to infect, replace, delete data in a connection kill a network connection etc.

This machine had no static IP address configured as it was a hacker's node and at the start of the experimentation did not readily have information regarding the network IP configurations of the target network nodes. The network interface for this machine was set in promiscuous mode *"(an IP network interface mode in which the network interface card reports every packet that it sees)"*.

Network Hub

A network hub is a physical connection and joins multiple computers or other network devices together to form a single network segment where all devices connected can communicate with each other. Unlike a network switch or router, a hub has no routing tables or intelligence on where to send information, as such the hub just broadcasts all network data across each connection.

The network hub used for this experiment was an AdvanceStack hp J2600A 10 Base-T Hub-12.

Wireshark software

Wireshark is a free and open-source multi-platform packet sniffing and analysing tool used for network troubleshooting, software and communications protocol development and education. It allows data examination from a live network or from a capture file on disk [32].

As a packet sniffer, Wireshark is itself passive as it only observes messages being sent and received by applications and protocols running on a network computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent/received from/by application and protocols executing on a computer.

The second component of Wireshark is the packet analysing ability, which displays the contents of all fields within a protocol message. In order to do so, Wireshark understands the structure of all messages exchanged by protocols.

In this study, Wireshark was used as a network sniffing software to expose some confidential network configuration information.

Ettercap Software

Ettercap is a multipurpose sniffer/interceptor/logger for switched LANs [33]. It is a versatile network manipulation tool. It uses its ability to easily perform man-in-the-middle (MITM) attacks in a switched LAN environment as the launch pad for many of its other functions.

Once Ettercap has inserted itself in the middle of a switched connection, it can capture and examine all communication between the two victim hosts, and subsequently take advantage of the network elements by performing some attacks such as character injection, packet filtering, automatic password collection for many common network protocols and killing of any connection.

In this experimentation, Ettercap was used to perform the Man-In-The-Middle attack on the target host nodes.

4.1.4 Testing Parameters

In order to accomplish the goal for this study, the investigation had to accurately evaluate the security vulnerabilities of a SIGTRAN network to adversities which would render the once closed SS7 signaling network open for attacks.

This study was based on a hacker having already obtained access into the internal packet-switched network of an operator which was made possible through so many ways like being assisted by disgruntled employees as well as remote attacks through compromised network elements such as IP-SS7 SGs.

However, it must be noted that the tests in this simulation were done under ideal and controlled laboratory environment as a result the results obtained may slightly differ to the ones that can be obtained from a live network environment.

The tests which were performed on the simulated SIGTRAN system to ascertain the vulnerabilities of IP networks to cyber-attacks were done in the following order:

Network IP Sniffing Test

Network sniffing is a passive security threat in which a machine separate from the intended destination reads data on a network. Passive security attacks are those that do not alter the normal flow of data on a communication link or inject data into the link. Sniffing threats target the lower layers of the networking infrastructure [34].

In this test, using Wireshark as sniffer software, the experiment aimed at uncovering some vital network information such as the IP addresses of remote network interfaces of the MTU and MTR, IP routing information and sequence numbers assigned to bytes on a TCP connection. Any knowledge of this information can be used by the malicious intruder in attacking the security of the network elements.

This experiment would assist in proving that the security of the SIGTRAN signaling network components is compromised through the IP network hence rendering SS7 signaling messages vulnerable to cyber-attacks.

Network Packet Capturing and Analysis Test

The aim of this test was to capture and analyse all the data packets that pass through the SIGTRAN network between the two distant target SIGTRAN network nodes. The test software for this experiment was also Wireshark.

The information of interest in this experiment will include the heart beat signaling messages between the MTU and the MTR, The type of protocol used between the two signaling nodes and the actual message content (MSU) sent between the two nodes.

This experiment would prove that both the security and privacy of the network users is compromised as a third party whose messages are not intended for is able to display and read them.

Man-In-The-Middle (MITM) Attack Test

This test was performed using Ettercap packet manipulation software and was aimed at demonstrating how an attacker can destabilise a network connection and perform a Denial of service (DoS) attack on the users between any two network's target nodes.

This test followed the Network IP sniffing test described above. Once the IP addresses of the target hosts were known through IP sniffing, the attacking node was configured with a static IP address of the same range as the target hosts. The attacking node then positioned itself as a router between the two target hosts of interest.

Using Ettercap, two attack scenarios were performed. One was the Address Resolution Protocol (ARP) poisoning and the other one Network Connection Killing.

In ARP poisoning, instead of routing the packets from one target host to the other, the hacking machine acting as a router drops those packets hence causing intermittent network time out. Sometimes a hostile attacker can decide to terminate a network connection of his victims and this can also be done using the network killing capabilities of Ettercap.

4.2 Conclusion

This chapter serves as a basic introduction to the subject of the vulnerabilities of SS7 signaling messages to cyber-attacks when transported over IP in the technologically merging environment and validates the need for this investigation by providing an overview of the problem statement, the objectives of the research, the methodology and configuration of the devices used in the experimentation that investigates the problem.

The previous work done on the subject shows that a vast amount of research effort has been put into the investigation of SIGTRAN transportation technology, however much of this focused on the performance and reliability characteristics of SIGTRAN's underlying transport protocol of SCTP. This chapter therefore validates the need for more research focus and further investigations into the security aspect of the SIGTRAN technology as the interworking between SS7 and IP networks become more relevant now than ever before.

Chapter 5

Experimentation

5.1 Introduction

An experiment is a test or investigation which is carried out with the goal of verifying, refuting or establishing the validity of a hypothesis. The experiments carried out in this study were aimed at providing evidence for or against the fact that IP networks render SS7 signaling messages exposed and vulnerable to cyber-attacks. These experiments were done by using a Dialogic SIGTRAN network simulation tool. This chapter therefore describes in details the system setup and configuration for this simulated Dialogic SIGTRAN network.

The experiment simulated an IP (whether private/public) network being used to backhaul traffic between two island SS7 networks using SIGTRAN protocols. Two peer SIGTRAN servers (nodes) were therefore deployed on either end of the SS7/IP network interconnection point. Much as the signaling points are identified by point codes in SS7 networks, the SIGTRAN nodes are identified by IP addresses. In order to demonstrate the signaling message exchanges between the two nodes, simple message services (SMSs) were exchanged between the two SIGTRAN nodes as SIGTRAN networks can be used to offload SMSs from the heavily overloaded SS7 signaling networks [16].

The IP addresses, signaling protocols and SMS messages being exchanged between the two SIGTRAN nodes were targeted and collected by a simulated hacking node connected into the IP network. Using this information, the attacker was able to launch cyber-attacks to the SS7 signaling messages and consequently brought down the whole SS7 network.

For the analysis, different testing conditions as discussed in subsection 4.1.4 on page 51 were considered.

5.2 Simulation Test Network Setup and Configuration

In setting up the Dialogic SIGTRAN simulation network two end computers configured as end point SIGTRAN network (servers) nodes A and B and a hacking computer connected to the same network through a network hub were used, as shown in Figure 4.2, subsection 4.1.3 on page 48. The two SIGTRAN nodes were running Dialogic SIGTRAN development application software and acted as the Signaling gateways on either end of the SS7/IP interconnection points and were identified on the network using the Class C private network addressing system.

5.2.1 Dialogic SIGTRAN Network Setup and Configuration

The dialogic software required to successfully run the simulated experiment was downloaded from: *http://www.dialogic.com/support/helpweb/signaling/software3.htm.* and included:

1. Dialogic SS7 Development Package
2. Dialogic M2PA, MTP3, SCCP and TCAP, MAP host binaries, for SIGTRAN configuration

Having installed the SS7 development software and copying all the required SIGTRAN protocol binaries such as the M2PA, M3UA MAP, TCAP, SCCP, etc. on the two SIGTRAN end nodes, the system and configuration files were edited in order to update the IP addresses together with the local and remote point codes. Node A was configured to initiate the associations and it is known as the MAP Test Utility (MTU) while node B responds to those association requests and is referred to as the MAP Test Responder (MTR).

Once the connection between the two SIGTRAN nodes was established, the MTU at constant intervals sent handshake (HEARTBEAT) signaling messages through to the MTR and the messages were always acknowledged back whith HEARTBEAT_ACK indicating that the connection between the two nodes was healthy.

The Dialogic SIGTRAN protocols using MTU and MTR applications were used to demonstrate the sending of MAP services in a GSM network.

5.2.2 Network Connectivity

A class C Addressing of the TCP/IP network configuration was used to connect the network devices together.

5.2.3 Sending Dialogue Messages between SIGTRAN Nodes

There was always an exchange of signaling handshake messages and other SIGTRAN protocols between the MTU and the MTR once the Dialogic application software was activated on both sides of the SIGTRAN end nodes.

Besides analysing only the HEARTBEAT and signaling protocol messages between the MTU and the MTR terminals during the experimentation, Short Message Service (SMS) messages were exchanged between the two signaling nodes. SMS messages are part of the MAP services in 3G networks and were transported over the IP network using SIGTRAN technology.

In using MTU to send SMS dialogue messages to MTR and vice versa, certain minimum mandatory criteria must first be met for the messages to successfully reach their intended destination and these are [35]:

- MTU mode operation - service being offered and is indicated by the letter "d" followed by any numeric symbol between 0 and 3.
- Remote point code - destination point code indicated by letter "a"
- Local point code - originating point code indicated by letter "g"
- International Mobile Subscriber Identity (IMSI) - indicated by letter "i"
- Short message - the text to be sent as short message indicated by letter "s"

With reference to subsection 2.1.5, the SS7/SIGTRAN protocol binaries used to complete the message transfering action above between the two peer signaling nodes are MAP, TCAP, SCCP, M2PA and SCTP.

5.3 TCP/IP Network Activity Sniffing Test

This test assessment was aimed at highlighting the security deficiencies of IP networks in transport SS7 signaling messages through the exposure of some private and confidential network information which is supposed to be known only to a few top network administrators and managers of Mobile Network Operators (MNOs). Through network sniffing the experiment aimed to demonstrate that critical network information can easily be in public domain by using the freely available network sniffing software tools from the internet such as Wireshark.

The confidential network information that was targeted in this test was the IP addresses of all the host nodes.

The results of this test would go a long way in providing evidence on whether IP networks are secure enough to transport SS7 signaling messages or IP networks render SS7 signaling messages vulnerable to cyber-attacks by exposing the critical network configuration information of the SIGTRAN nodes, the information of which can be used to launch further attacks against SS7 networks.

The experimental equipment setup for this test is shown in Figure 5.1.

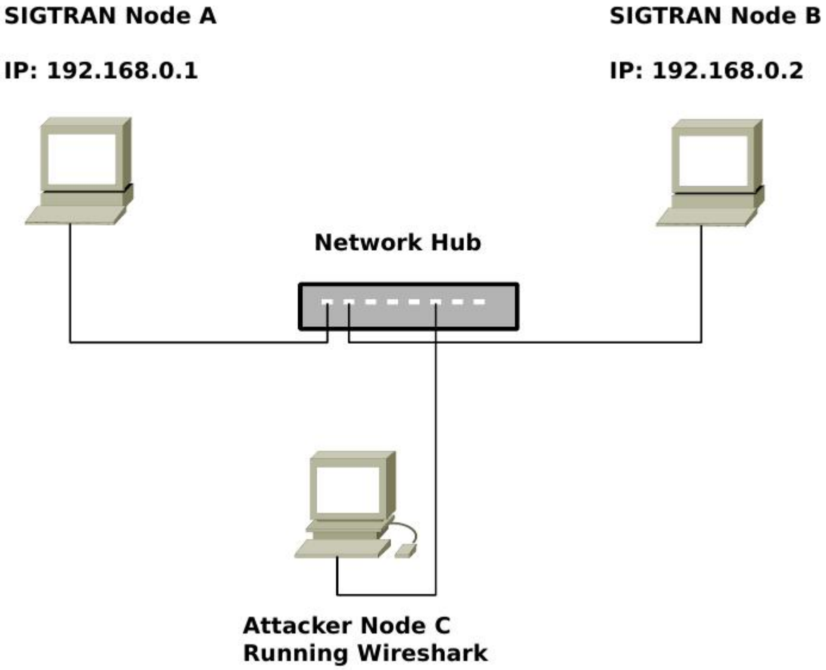


Figure 5.1: Network Sniffing Experiment Setup

Test Procedure

- The two SIGTRAN nodes A and B were configured with IP addresses 192.168.0.1 and 192.168.0.2 respectively.

- Node C represented a hacker who found access and connected in promiscuous mode to the same TCP/IP network pool as the two SIGTRAN nodes A and B which were transporting SS7 signaling messages over an IP network.

- Using Wireshark network sniffing software installed on his computer, the attacker sniffed the network to monitor the network activity between different network components and obtained critical network information such as the IP addresses of the different network host nodes.

- A Wireshark live capture of the network activity was taken and analysed.

5.3.1 Results Obtained

The results of this experiment which were extracted from a Wireshark screenshot (Appendix A) are shown in Table 5.1 below.

No.	Time	Source	Destination	Protocol	Length	Info
513	121.209087	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT
514	121.209329	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT_ACK
515	121.303826	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT
516	121.304158	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT_ACK
517	122.425905	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT
518	122.426152	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT_ACK
519	122.489419	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT
520	122.489754	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT_ACK

Table 5.1: Extracted Results of Wireshark TCP/IP Network Activity Sniffing Test

The results in Table 5.1 clearly display the following information:

1. Any data packet sent between the source node and the destination node was identified by the following fields:

   Frame number - number of packet transmitted since the beginning of the capture

   Time - time ”in seconds” a packet was sent since the beginning of capture

   Source - IP address of the originating node for the packet

   Destination - IP address of the destination node for the packet

   Protocol - digital rule for data exchange between two devices

   Length - the frame length of the packet in bytes

   Information - the type of information sent

2. There were only two host IP addresses associating (communicating) that were constantly exchanging roles of source and destination and vice versa. One host IP was 192.168.0.1 and the other host IP was 192.168.0.2.

3. The kind of information that was reciprocally exchanged between the two IP hosts was the handshake “HEARTBEAT” and “HEARTBEAT_ACK” signaling messages.

4. The signaling protocol that was used for message exchanges between the two hosts was Stream Control Transport Protocol (SCTP) which is an underlying reliable transport protocol binary for SIGTRAN networks above the IP layer.

The IP addresses obtained in the test results for this experiment compared favourably to the actual IP network configuration information obtained from the two SIGTRAN hosts' administrator command prompt window by running the command "ipconfig", shown in Appendices B and C.

From the IP address information captured in the Wireshark screenshot from the test results and having compared the information to the actual network configuration data for the two SIGTRAN host nodes; this experiment successfully demonstrated that SS7 is really vulnerable to cyber-attacks as confidential network configuration information such as IP addresses could easily be exposed through sniffing the IP network.

5.4 Network Packet Capturing and Analysis Test

Using the network sniffing and data capturing capabilities of Wireshark software, this experiment was aimed at capturing, displaying and analysing any MAP based services exchanged between the two end SIGTRAN nodes over the IP network.

This experiment involved exchanging of SMS dialogue messages (since SMS is part of MAP services) between the two SIGTRAN end nodes, subsection 5.2.3 on page 56. Two filter options, SCTP and SMS_GSM, of the Wireshark were used in order to display only the text messages. The contents of these dialogue messages were then analysed.

This experiment assessment was aimed at testing both the security and privacy issues of IP networks in transporting SS7 signaling messages and the test results of the experiment would assist in providing evidence, on whether the security and privacy of information of the SS7 network users can easily be compromised when SS7 networks interconnect with IP networks.

Figure 5.1 on page 58 shows the experiment setup for this test.

Test Procedure

- During this experiment, there were exchanges of SMS text messages between node A and node B using the procedure described in subsection 5.2.3. In total eight SMS conversations were exchanged between the nodes during the duration of the experiment with each node sending four of the messages to the other node.

- A simulated network hacker using node C was connected to the same TCP/IP network as the two SIGTRAN nodes A and B which were exchanging SS7 signaling and SMS text messages over IP.

- Using Wireshark network sniffing software installed on the intruder's computer, the attacker sniffed the network and captured all network activities which were taking place between the two SIGTRAN nodes. The attacker then displayed and analysed the information.

- Having identified some MAP based protocols in the captures during the analysis, the attacker filtered the MAP based protocols by setting up two filter options of SCTP and GSM SMS in the Wireshark filter option window.

- The filtered MAP messages were dissected further to get to the content of the information which was being exchanged between the end signaling nodes.
- The Wireshark live captures of the filtered and analysed GSM Message exchanges between the two end nodes were presented.

5.4.1 Results obtained

The test results for this experiment extracted from the Wireshark screenshot captures in Appendices D, E, F, G, H, I, J, K and L are shown in Tables 5.2, 5.3 and 5.4.

SCTP Capture Filter Option Results

No.	Time	Source	Destination	Protocol	Length	Info
1856	391.318295	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT
1857	391.318542	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT_ACK
1858	391.510624	2	1	GSM SMS	254	invoke forwardSM
1859	391.511255	192.168.0.1	192.168.0.2	SCTP	62	SACK
1860	391.521655	192.168.0.1	192.168.0.2	M2PA	78	User Data
1861	391.521903	192.168.0.2	192.168.0.1	SCTP	62	SACK
1862	391.529858	1	2	GSM MAP	154	returnResultLast
1863	391.530106	192.168.0.2	192.168.0.1	SCTP	62	SACK
1864	391.586059	192.168.0.2	192.168.0.1	M2PA	78	User Data
1865	391.586406	192.168.0.1	192.168.0.2	SCTP	62	SACK
1867	392.722392	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT
1868	392.722640	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT_ACK
1869	392.802503	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT

Table 5.2: Extracted Results of Wireshark SCTP Capture Filter Option

The information in Table 5.2 is an extract from a Wireshark capture screenshot in Appendix D, having set SCTP as a Capture Option in the capture filter of the Wireshark and displays the following:

1. There were two Hosts associating on the network with IPs 192.168.0.1 and 192.168.0.2.
2. There were different protocol types sending different information between the two nodes:
   - SCTP – Used for handshake signaling information (HEARTBEAT and HEARTBEAT_ACK).

- M2PA- Used for sending user datagrams in a peer-to-peer Host configuration of the SIGTRAN nodes.
- GSM MAP-GSM based Application used for sending the MAP services.
- GSM SMS-The Actual MAP service sent between the two Hosts (GSM SMS Text message).

3. The Selective Acknowledgement (SACK) feature of the SCTP, which is a congestion control mechanism, was activated due to the varying lengths of the datagrams received and the different protocols being exchanged between the two Hosts.

Through the use of SCTP capture filter the test was able to capture all the MAP related protocols involved in the sending of SMS Text messages starting from the handshake signaling messages between the two nodes, the M2PA user adaptation protocol used which shows that the nodes are connected in a peer-to-peer configuration and also the kind of MAP service (GSM SMS) being exchanged between the two nodes.

GSM_SMS Capture Filter Option Results

No.	Time	Source	Destination	Protocol	Length	Info
280	58.591333	1	2	GSM SMS	250	invoke forwardSM
397	82.402164	2	1	GSM SMS	218	invoke forwardSM
741	159.858250	1	2	GSM SMS	254	invoke forwardSM
1069	230.307168	2	1	GSM SMS	246	invoke forwardSM
1450	308.037542	1	2	GSM SMS	230	invoke forwardSM
1547	330.815084	2	1	GSM SMS	242	invoke forwardSM
1730	369.367199	1	2	GSM SMS	258	invoke forwardSM
1858	391.510624	2	1	GSM SMS	254	invoke forwardSM

Table 5.3: Extracted Results of Wireshark GSM_SMS Capture Filter Option

The information in Table 5.3 is an extract from a Wireshark capture screenshot in Appendix E of the first captured GSM SMS Text message, having set GSM_SMS as a Capture Option in the capture filter of the Wireshark and displays the following:

1. Only GSM SMS were filtered and displayed.
2. There were eight SMSs conversations which were exchanged between Host 1 and Host 2.

3. Whenever a particular message was selected, the content of that particular message was displayed in the second Wireshark window under User Data option.

Table 5.4 below displays the contents of all the eight Text messages exchanged between the two Hosts as captured by Wireshark in appendices E, F, G, H, I, J, K and L.

Frame No.	**Source**	**Destination**	**SMS Text Content**
280	1	2	## WHY STUDY VULNERABILITIES OF SS7 SIGNALING MESSAGES TO CYBER ATTACKS? ##
397	2	1	###### IT IT BECAUSE SS7 IS HERE TO STAY
741	1	2	########## SS7IS HERE TO STAY? WHT THIS HYPE ABOUT NEXT GENERATION NETWORKS?
1069	2	1	###### THOUGH CONSIDERED A LEGACY SYSTEM, SS7 WILL INTERWORK WITH THE IP
1450	1	2	########## SO HOW ARE THESE TWO TECHNOLOGIES MERGING?
1547	2	1	###### BY USING SIGTRAN, WHERE SS7 MESSAGES ARE TRANSPORTED OVER IP
1730	1	2	########## AND YOU THINK THE IP NETWORKS POSE SECURITY RISKS OF CYBER ATTACKS TO SS7?
1858	2	1	###### A BIGGER CYBER THREAT OFF COURSE, UNLESS THE IP NETWORKS ARE SECURE ENOUGH

Table 5.4: Content of Captured Messages

The number and content of the Wireshark captured Text messages displayed in this experiment are seen to be exactly the same as the messages which exchanged between the two SIGTRAN nodes as seen from the MTR print screenshots of each node in Appendix M and Appendix N. Appendix M shows four received SMS Text messages on Host 2 which were sent from Host 1 and Appendix N shows received SMS Text messages on Host 1 which were sent from Host 2.

From the results of this experiment, it can be deduced that; unless proper security measures are deployed throughout a SIGTRAN network, the privacy of both the SS7 signaling network information and subscriber data is compromised in an interconnected network infrastructure setup.

5.5 Man-In-The-Middle (MITM) Attack Test

This experiment was a follow up to the two previous experiments and aimed at demonstrating how a malicious attacker can use the vital network information obtained through network sniffing to his advantage and launch a series of attacks aimed at destabilising the operations of the network.

In this experiment Ettercap network packet manipulating software was used to perform the denial of service (DoS) attack on the IP network transporting SS7 signaling messages using SIGTRAN protocols.

The results of this experiment would assist in demonstrating that IP networks are susceptible to cyber-attacks. This experiment provided more evidence to argue that IP networks in their entirety are not secure enough to transport SS7 signaling messages.

Shown in Figure 5.2 is the setup for the experiment.

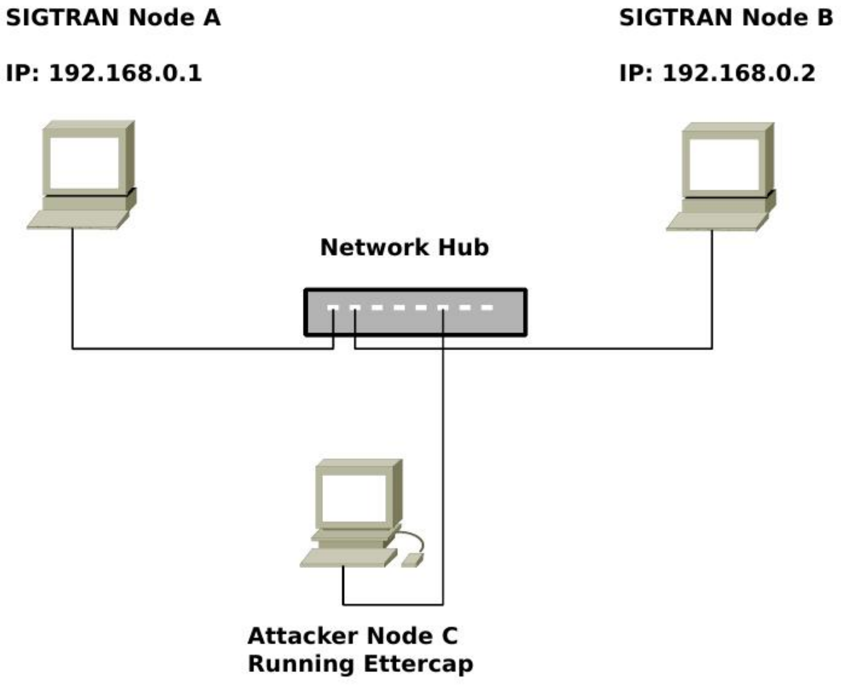


Figure 5.2: Man in the Middle Experiment Setup

Note:

In an IP network setup any configurable network device is identified on the network by two addresses:

- Internet Protocol (IP) address - which is associated with networking software and is normally assigned to a particular network device by the network administrator or automatically using the Dynamic Host Configuration protocol (DHCP) server.

- Media Access Control (MAC) address – physical or hardware address which is typically tied to a device's network interface adapter. Each network device has a unique MAC address which is hard wired to the device's network interface card.

The IP address is translated into the MAC address using the Address Resolution Protocol (ARP).

With reference to Figure 5.2, the MAC addresses for the three network computers (obtained by running a command "getmac" in the command prompt window on each computer) were as follows:

SIGTRAN Node A:	MAC Address	- 00:25:b3:d0:47:df (Hewlett_d0:47:df)
SIGTRAN Node B:	MAC Address	- 00:25:b3:d0:4f:b1 (Hewlett_d0:4f:b1)
Attacker Node C:	MAC Address	- 00:23:7d:c9:ed:94 (Hewlett_c9:ed:94)

Test Procedure

- Using the network IP addressing information obtained through sniffing with Wireshark, the attacker's computer was configured with a static IP of the same range as the target nodes. The intruder's computer was assigned an IP address 192.168.0.3.

- While equipped with Ettercap application software for network packet manipulation, the attacker was ready to launch attacks on his target nodes.

- The attacker, using Ettercap, scanned the whole network to try and identify the network hosts so that from the list of hosts, two hosts would be targeted for the Man In The Middle attack. Two hosts were identified and the host IP addresses were displayed.

- Once the targets were identified, the intruder's computer was positioned between the two target hosts.

- Finally the malicious intruder launched an attack on the victims through ARP poisoning.
- The communication between the two victim host SIGTRAN nodes during the ARP poisoning test was observed and captured on Wireshark.

5.5.1 Results Obtained

The test results for this experiment extracted from the Wireshark screenshot capture in Appendix M are shown in Table 5.5 on page 68.

The information in Table 5.5 is an extract from a Wireshark capture screenshot in Appendix O of the SIGTRAN network association activity between Host 1 and Host 2 immediately after the attacker had launched the ARP Poisoning MITM attack and shows that:

1. Frames number 9035, 9036 and 9037 showed a healthy SCTP handshake communication between Host 1(192.168.0.1) and Host 2(192.168.0.2) exchanging HEARTBEAT signaling messages.

2. In frame 9038 Host 2 sent a ping request to Host 1 using the Internet Control Message Protocol (ICMP) and likewise Host 1 to Host 2 in frame 9039.

3. In frame 9040 the two-way ARP poisoning had been launched. The Attacker Node C (MAC Address 00:23:7d:c9:ed:94), using ARP, sent a false broadcasting message to Host 1 (MAC address 00:25:b3:d0:47:df) advising that Host 2 (IP address 192.168.0.2) was now at a new MAC address 00:23:7d:c9:ed:94 while in essence the new MAC address was the attacker's own address.

4. Similarly, the attacker in frame 9041 sent a false broadcasting message to Host 2 (MAC address 00:25:b3:d0:4f:b1) advising that Host 1 (IP address 192.168.0.1) was now at a new MAC address 00:23:7d:c9:ed:94 which in fact was the attacker's own MAC address.

5. The attacker then was established as the Man-In-The-middle (MITM) between the two host nodes A and B where all the data packets between the nodes had to pass through the attacker.

6. With the new IP and MAC address reconfigurations, Host 1 and Host 2 continued exchanging information without knowing that the information was being directed to the MITM.

No.	Time	Source	Destination	Protocol	Length	Info
9035	1818.772358	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT_ACK
9036	1818.852914	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT
9037	1818.853159	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT_ACK
9038	1819.902980	192.168.0.2	192.168.0.1	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59562, ttl=64
9039	1819.903089	192.168.0.1	192.168.0.2	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59562, ttl=64
9040	1819.903186	Hewlett_c9:ed:94	Hewlett_d0:47:df	ARP	42	192.168.0.2 is at 00:23:7d:c9:ed:94
9041	1819.903285	Hewlett_c9:ed:94	Hewlett_d0:4f:b1	ARP	42	192.168.0.1 is at 00:23:7d:c9:ed:94
9042	1819.903500	192.168.0.1	192.168.0.2	ICMP	60	Echo (ping) reply id=0x7ee7, seq=32487/59562, ttl=128
9043	1819.903752	192.168.0.2	192.168.0.1	ICMP	60	Echo (ping) reply id=0x7ee7, seq=32487/59562, ttl=128
9044	1819.903757	192.168.0.2	192.168.0.1	ICMP	70	Destination unavailable (Protocol unreachable)
9045	1819.904133	192.168.0.1	192.168.0.2	ICMP	70	Destination unavailable (Protocol unreachable)
9046	1819.957447	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT
9047	1820.054375	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT
9048	1820.693993	192.168.0.1	239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1
9049	1821.158621	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT
9050	1821.255314	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT
9051	1821.903623	Hewlett_c9:ed:94	Hewlett_d0:47:df	ARP	42	192.168.0.2 is at 00:23:7d:c9:ed:94
9052	1821.903704	Hewlett_c9:ed:94	Hewlett_d0:4f:b1	ARP	42	192.168.0.1 is at 00:23:7d:c9:ed:94
9053	1822.562621	192.168.0.2	192.168.0.1	SCTP	60	ABORT
9054	1822.659356	192.168.0.1	192.168.0.2	SCTP	60	ABORT
9055	1823.657750	192.168.0.1	192.168.0.2	SCTP	82	INIT
9056	1823.704502	192.168.0.1	239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1
9057	1823.904050	Hewlett_c9:ed:94	Hewlett_d0:47:df	ARP	42	192.168.0.2 is at 00:23:7d:c9:ed:94
9058	1823.904129	Hewlett_c9:ed:94	Hewlett_d0:4f:b1	ARP	42	192.168.0.1 is at 00:23:7d:c9:ed:94
9059	1824.656298	192.168.0.1	192.168.0.2	SCTP	82	INIT

Table 5.5: Extract of Wireshark Results of Ettercap ARP Poisoning

7. The MITM , instead of forwarding to the intended destination, discarded all the data packets received from either host as a result the data packets from one host could not reach the other host therefore an error message “Destination unavailable (Protocol unreachable)” was reported using ICMP.

8. After several attempts to re-establish the SCTP association between the two hosts, the Dialogic application finally ABORTED.

After the association had aborted, Host node 192.168.0.1 (MTU) continuously tried to initiate the association with Host node 192.168.0.2 (MTR) back through repeated “CLOSED” and “CONNECTING” and this carried on until the ARP poisoning attack was stopped as shown in a print screen of the Dialogic SIGTRAN application terminal shown in Appendix P.

This experiment has demonstrated that a hacker with basic hacking skills and using simple and available hacking software from the internet can destabilise the operations of a SIGTRAN network.

5.6 Conclusion

The experimental tests carried out in this study exposed serious security concerns of the IP networks that support SS7. These IP network security weaknesses raise even more dilemma to thousands of telecommunications network operators who still have many legacy TDM-based SS7 systems as the IP networks are used to transport the once highly secured SS7 signaling messages using SIGTRAN protocols in a converging world.

Through the use of freely available sniffing and packet manipulating software packages from the Internet, the experiments have demonstrated that a malicious cyber-attacker, once found access into either a private or public IP network transporting SS7 signaling messages, can bring down the whole SS7 signaling network. The test results obtained in this study highlight the need for tighter security measures for SIGTRAN network nodes and the IP network as a whole if SS7 over IP transportation is to be successful. Some of the security measures are discussed in section 6.3.

It must be stated however that the SIGTRAN network deployment in a live environment comes about with many network security measures and solutions from the system suppliers, IT network security companies or off-the-shelf solutions to try and secure the SIGTRAN networks. Consequently professional hackers are constantly adjusting their tactics to try and breach any network security solutions a network operator might have deployed.

Chapter 6

Mitigating Factors against SIGTRAN Cyber-Attacks

6.1 Introduction

Presently, many Mobile Network Operators are interconnected through IP infrastructures, as they are cheaper and more efficient than traditional SS7 links, by means of new protocols based on IP layer like SIGTRAN. This new context exposes the mobile networks' SS7 signaling networks to new security threats. The results obtained from the experimentation tests carried out in this study confirm the IP networks' security vulnerabilities to cyber-attacks. It is therefore imperative that proper IP network security programs are implemented before any SIGTRAN deployments are effected by the network operators.

The implementation of network firewalls does not always block or analyse SCTP traffic and traditional Intrusion Detection Systems (IDSs) do not monitor SCTP traffic. Consequently, even simple attacks like scanning can go undetected. Implementation of appropriate security measures is mandatory to prevent malicious attacks to SIGTRAN networks.

Despite the mandatory SIGTRAN implementation security measures of secure tunnels based on either IP security (IPSEC) or Transport Layer Security (TLS) which are recommended to be established between SIGTRAN nodes in order to provide the equivalent of an isolated link such as used in a traditional SS7 network, the major difficulties to the implementation rest on the fact that all the involved systems should implement security correctly.

This chapter gives a brief description of the vulnerabilities and the possible attacks against SIGTRAN stack layers and preventative measures to such kinds of attacks are proposed.

6.2 SIGTRAN Targeted Attacks

The most common kinds of cyber-attacks to SIGTRAN based networks target the two lower transport levels of the SIGTRAN protocol stack, the IP and the SCTP. This is so because the upper layer protocols can only offer their services through the lower transport layers to the other end Signaling node.

The network IP sniffing and spoofing, packets capturing and man in the middle attacks demonstrated in Chapter 5 above are all examples of both the passive and active attacks that can target the SIGTRAN networks in order to disrupt services to network users.

Some of the attacks that affect SIGTRAN networks include but are not limited to:

Flooding Attack

Flooding is an example of DoS attacks where the attacker intentionally floods a particular node with unnecessary packets aimed at monopolising the resources of the victim host server to deprive the legitimate users of those resources. Hosts in SIGTRAN are unable to stop packets addressed to them. Once the host's network link becomes congested, the IP router responds to the overload by arbitrarily dropping packets.

A known example of flooding attack is the SYN Flooding. Normally in any TCP IP association, there is a three-way handshake (exchange of signaling messages) between the client and the server [42]. A client requesting services sends a Synchronise (SYN) message to the server and the server acknowledges with a SYN-ACK (Synchronisation Acknowledgement) message and lastly the client acknowledges back to the server with ACK message.

In SYN flooding attack, the client does not respond with ACK message back to the server once it receives the acknowledgement from the server. As a result the server will hold on for a longer period waiting for the client's acknowledgement hence tying the resources which could have been used by legitimate users.

Address Camping Attack

Also known as address stealing or squatting attack, this is a type of DoS attack based on the sharing of an IP address between two endpoints in an SCTP multi-homing scenario. In this kind of attack, the attacker knows in advance the IP address and the port used by the victim through IP sniffing and spoofing of the network but the port, if not already known, is guessed through brute forcing over 216 possible values.

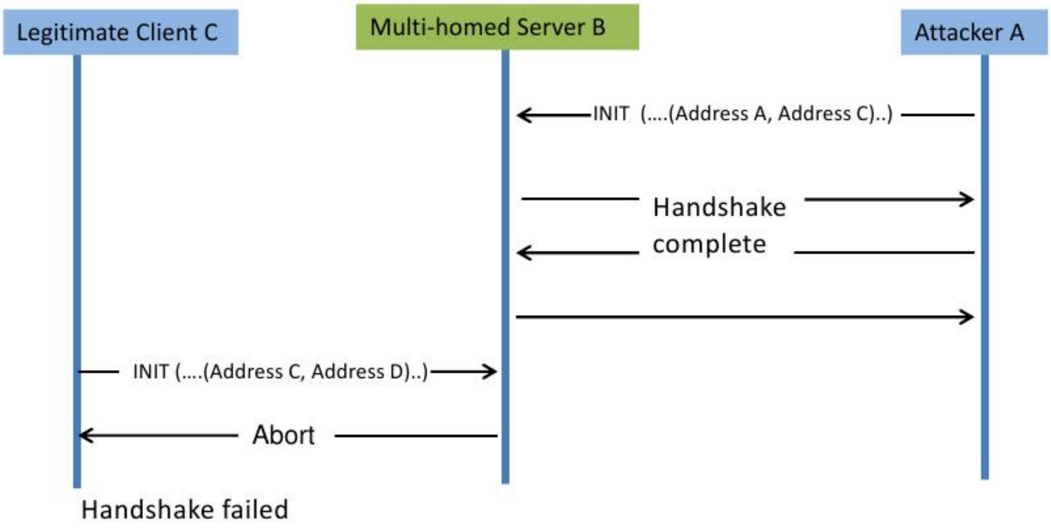


Figure 6.1: Address Camping Attack [43]

As seen from figure 6.1 above, Attacker A prevents a legitimate Client C from setting up an association with the Server B declaring the victim IP address (Address C) as a secondary IP address in the INIT message and the same port used by Client C. When Client C tries to create an association with the Server B, there will be an address conflict between the two associations (A-B and C-B) and the Server B will reject the INIT from Client C and respond with an ABORT message [43].

Bombing or Amplification Attack

This is a form of a Distributed Denial of Service (DDoS) based on a mechanism that causes an arbitrary SCTP endpoint to amplify (in number and/or size) packets sent to a victim. SCTP can suffer from several types of this attack.

In this kind of attack, the attacker sends packets containing the victim's address as the source address and an INIT chunk to a large number of SCTP endpoints. Each endpoint then replies with a packet containing an INIT-ACK chunk to the victim, which is most likely larger than the packet containing the INIT which will bombard the victim from many SCTP endpoints [37].

Association Redirection Attack

This attack allows an attacker to wrongly set up an association to a different endpoint [49]. This is an unexpected feature of the SCTP multi-homing and invoking this feature does not constitute an attack in itself but if not well understood by application designers, it could be exploited as a building block in application-level attacks.

6.3 Preventative Measures to SIGTRAN Targeted Attacks

There are many ways that can be suggested as the counter measures against the cyber-attacks targeting the SIGTRAN networks. However, this study concentrated on the solutions to the cyber-attacks highlighted in section 6.2. It must be stated though that some of the counter measures are generic and can apply to so many scenarios of attacks while others are specific to particular problems of intrusion.

The threat of sniffing comes from someone installing sniffing software on a machine normally on the network, as someone taking a sniffer into a room and plugging it into the network connections available there, or even installing an unauthorized network connection to sniff. To counter these options, the security of the operating system itself must be reliable to prevent the execution of unauthorized sniffing. Also the personnel who have access to the rooms in which network components are located must have high integrity and be trustworthy as well as deploying physical security to prevent untrustworthy and unauthorised people from gaining access to the network and server rooms.

As an improvement to the traditional TCP/IP, the SCTP layer of the SIGTRAN protocol provides natively some security features such as resistance against blind denial of service attacks (flooding, masquerading and improper monopolization of services) using two new features, state Cookies and the verification tag [38].

State Cookies are used to minimize the risks of resource exhaustion, guard against source address spoofing, and prevent connection hijacking and Distributed Denial of Service (DDoS) attacks [50]. State cookies are a four-way hand shake procedure implemented in SCTP. This new feature prevents attackers from establishing connections without using them and in that way hindering legitimate users from establishing a connection.

A verification tag is an SCTP packet header containing a random 32-bit value that indicates whether a packet belongs to a certain association. If it does not, it is dropped. A new Verification Tag value must be used each time the endpoint tears down and then re-establishes an association to the same peer. This parameter has been introduced to prevent replay and man-in-the-middle attacks and to reduce the risk of off-path spoofing attack. Despite these new features, several other attacks could still be carried out against SCTP layer of the SIGTRAN Protocol stack [38].

Network spoofing and tampering together with some passive and active attacks can be prevented by using IPSEC tunnels at IP layer [51]. It must be noted however that the usage of IPSEC could raise some issues when SCTP multi-homing is implemented where an SCTP endpoint could handle more than one IP address and consequently more than one IPSEC tunnels should be set-up.

To avoid the bombing or amplification attack, an SCTP endpoint should not send multiple packets in response to a single packet. The chunks not fitting in this packet should be dropped [38].

Some other attack prevention counter measures relate to the overall IP network configuration and security features such as deploying network firewalls, network segmentation and partitioning using network routers, bridges and switches.

6.4 Conclusion

SIGTRAN networks have now become very popular with many mobile network operators because of the many operational and social benefits that they offer. This being the case though, there are so many cyber risks that come along through the use of the SIGTRAN transport protocol suite that if not properly managed can lead to devastating effects to both the network operators and the service users.

Chapter 7

Conclusions and Recommendations

7.1 Introduction

The purpose of this study was to provide an answer to the key research question: "Are SS7 signaling messages vulnerable to cyber–attacks due to interconnection with IP networks?" In order to achieve this several experimental tests were conducted on a simulated SIGTRAN network to establish if the security and confidentiality of SS7 signaling messages was compromised as they get transported over IP networks.

7.2 Key Findings and Conclusions

After a thorough analysis of the results which were obtained from all the three tests carried out in this study it can be argued with certainty that "YES", IP networks pose greater risks of cyber-attacks to SS7 signaling networks in SIGTRAN interfaced interconnected network environment. Vulnerabilities in SS7 based mobile networks allow an intruder with basic skills to perform dangerous attacks that may lead to direct subscriber financial loss, confidential data leakage or disruption of communication services.

The tests in this study revealed the following:

- Confidential SIGTRAN network configuration information such as node IP addresses can easily be exposed by a passive cyber attacker using network sniffing software like Wireshark.
- SIGTRAN network activities and protocols being exchanged between nodes can easily be

monitored using the network sniffing tools.

- It is possible to capture, display and analyse the SS7 signaling messages being exchanged between SIGTRAN network nodes.
- The information obtained from passive cyber-attacks such as IP addressing can be used by an intruder with malicious intentions to launch a DoS attack to a SIGTRAN node on the network.

The results from the different tests carried out in this study highlighted the risks of exposure to adversaries of the highly confidential SS7 network information as the SS7 signaling messages are being transported between island SS7 networks over IP networks using SIGTRAN. Although considered as being a passive kind of cyber-attack, the information collected through network sniffing such as the source and destination IP addresses of the associating nodes can be used to plan and launch subsequent attacks to the SIGTRAN nodes.

The magnitude of the cyber risks as demonstrated in this study cannot be underestimated. Knowing that the test tools used in the experiments for this study are freely available on the internet, it is scary to imagine what hacking software professional network hackers have at their disposal to successfully accomplish their missions.

It must be noted that there is no "One size fits all" kind of solution when it comes to securing the SIGTRAN networks against different kinds of cyber-attacks. Even though it is mandatory for all SIGTRAN nodes to support IPSEC in the IP transport layer as addressed in the Internet Draft "Security Considerations for SIGTRAN Protocols" [39], this becomes a problem in the nodes which are configured in a multi-homing mode. Therefore the network administrators must always remain vigilant against any potential sources and forms of attacks.

7.3 Recommendations and Future Work

The results show that there are many security risks in migrating SS7 based services to IP. As with any other network security program, there is no silver bullet that can eliminate all potential cyber threats to the SS7 network which might arise as a result of the interconnection with the IP network. A full-blown attack on mobile network's SS7 network infrastructure has the potential for catastrophic results that can affect multiple audiences and in today's hyper connected world it could be viewed as a national infrastructure attack.

There is no turning back in as far as network convergence is concerned. In view of this, this study recommends the following:

- Mobile service operators in conjunction with the IP network providers have to invest in security at the same rate as capacity.
- Mobile service providers who were used to isolated and secure SS7 networks must adapt to changes in the threat landscape, and be prepared to ensure network availability.
- Since new threats may have potential for catastrophe, the mobile network providers should adapt security programs and procedures to withstand those threats, while assuring the same level of service and preventing any major service outages.
- Vetting of personnel members who are entrusted with taking care of critical network infrastructure to avoid sabotage.

Bibliography

[1] Kameswari Kotapati, Peng Liu, Yan Sun, Thomas F. LaPorta, *A Taxonomy of Cyber Attacks on 3G Networks*, The Pennsylvania State University, University Park, PA 16802 USA.

[2] R. Shockey, *ENUM: Phone numbers meet the net, Communications Convergence*, July 2001.

[3] K. D. Gradischnig, St. Kramer, M. Tuxen, *Loadsharing – A key to the reliability of SS7-networks*, DRCN 2000.

[4] ITU-T Recommendation Q.9 (http://www.itu.int/rec/T-REC-Q.9-198811-I/en), Accessed November 2014.

[5] Richard J. Manterfield *Telecommunications Signaling (IEE Telecommunications Series)*, 1999.

[6] ITU-T Recommendation Q.766, *Performance objectives in the integrated services digital network application*, 03/93.

[7] ITU-T Recommendation Q.2144, *B-ISDN Signaling ATM adaptation layer – Layer management for the SAAL at the network node interface*, 10/95.

[8] ITU-T recommendation Q.706, *Specifications of Signaling System No. 7. Message Transfer Part. Signaling Performance*, 1996.

[9] ITU-T recommendation Q.709, *Specifications of Signaling System No. 7. Message Transfer Part. Hypothetical Signaling Reference Connection*, Rev.1, 1993.

[10] David Prince, *Sigtran Implementation*, Tekelec, April 2007.

[11] Guy Redmill (SS7 Product Manager Brooktrout Technology), *An Introduction to SS7* White Paper July 2001.

[12] *Global mobile Suppliers Association* (http://www.gsacom.com/about/index.php4), Last accessed on 5 October 2013.

[13] *User Data Protocol* (http://www.faqs.org/rfcs/rfc768), Accessed November 2014.

[14] http://www.en.wikipedia.org/wiki/Transmission_Control_Protocol_Applicability, Last accessed October 2014.

[15] http://www.artesyncp.com/pdf/wp_sigtran.pdf, Last accessed November 2014.

[16] Mia Immonen, *Signaling over IP — A Step Closer to an All IP Network*, Royal Institute of Technology, 2005.

[17] Jim Darroch (Protocol Development Manager), *Introduction to Sigtran*, Artesyn Communication Products, 2004.

[18] *3rd Generation Partnership Project*, http://www.qtc.jp/3GPP/Specs/29801-700.pdf, Release 7, page 6.

[19] *SS7-over-IP Networks Using SIGTRAN.* 910-4925-001 Revision B, June 2007.

[20] G. Lorenz, T. Moore, G. Manes, J. Hale, S. Shenoi, *Securing SS7 Telecommunications Networks*, 2001.

[21] *Scanning SS7 Networks and Telecom Backbones*, http://www.ethicalhackernet.blogspot.com/2010/08/scanning-ss7-networks-and telecom.html, Last accessed October 2014.

[22] Klaus D. Gradischnig and Michael Tuxen, *Signaling transport over IP-based networks using IETF standards*, 2001.

[23] Dong W. Kang, Joo H. Oh, Chae T. Im, Wan S. Yi and Yoo J. Won, *A Practical Attack on Mobile Data Network Using IP Spoofing*, July 2013.

[24] Hemant Sengar, Duminda Wijesekera, Sushil Jajodia and Ram Dantu, *SS7 Over IP: Signaling Interworking Vulnerabilities*, IEEE Network, November/December 2006.

[25] *SS7 and Sigtran Protocols*, http://www.sigtran.org, Accessed 20 September 2014.

[26] *SCTP Download Page*, http://www.sctp.de/sctp-download.html, Last accessed 20 September 2014.

[27] *Overview of the Kame Project*, http://www.kame.net/project-overview.html, Last accessed 22 September 2014.

[28] *Linux Kernel Stream Control Transmission Protocol Tools*, http://www.lksctp.source forge.net/, Last accessed 14 September 2014.

[29] *Sun Microsystems*, http://www.playground.sun.com/sctp/, Last accessed 18 September 2014.

[30] *OpenSS7*, http://www.openss7.org/, last accessed 28 Septenber 2014.

[31] *VOIP Wiki*, http://www.voip-info.org/wiki/view/Dialogic, last accessed 5 September 2014.

[32] *Wireshark*, http://www.sectools.org/tool/wireshark/, Last accessed 7 September 2014.

[33] Ornaghi, Alberto, and Marco Valleri, *Ettercap*, http://ettercap.sourceforge.net, March 31, 2004.

[34] *IP Spoofing and Sniffing*, http://www.techiwarehouse.com/engine/423a5281/IP-Spoofing-and-Sniffing, Last accessed December 2014.

[35] *Dialogic*, http://www.dialogic.com/.../media/manuals/ss7/cd/GenericInfo/GeneralDocume ntation/U30SSS03-MTU-MTR-UG.pdf, Last accessed January 2015.

[36] *Creating Next-Generation Signaling Gateways*, http://www.iphase.com/documents/whitepapers/ Creating%20Next-Generation%20Signaling%20Gateways%20with%20ATCA.pdf, Last Accessed November 2014.

[37] *Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem.*

[38] RFC 3788, *Security considerations for SIGTRAN protocols*, http://www.ietf.org/rfc/rfc3788.txt, Last accessed December 2014.

[39] J. Loughney, M. Tuexen, J. Pastor-Balbas , *Security Considerations for SIGTRAN Protocols*, Internet Draft draftietf-sigtran-security-02.txt (Work in Progress), IETF, January 2003.

[40] Monica Paolini, *"Wireless Security in LTE Networks"*, Senza Fili Consulting, LLC, 2012.

[41] *Rutgers School of Arts and Sciences*, http://www.cs.rutgers.edu/martin/teaching/fall04/cs552/ readings/ss7.pdf, Last accessed October 2014.

[42] An Active Detecting Method against SYN Flooding Attack (http://www.utdallas.edu/edsha/papers/bin/synflood.pdf), Last accessed December 2014.

[43] Shaojian Fu and Mohammed Atiquzzaman, *SCTP: State of the Art in Research, Products, and Technical Challenges*, University of Oklahoma, IEEE Communications Magazine, April 2004.

[44] Introduction to SS7 Signaling, Training Document Nokia Networks Oy, TC Finland. Issue Jan 2002.

[45] Paul Stalvig, *Introduction to the Stream Control Transmission Protocol (SCTP): The next generation of the Transmission Control Protocol (TCP)*, Technical Marketing Manager F5 Networks Inc, Oct 2007.

[46] Introduction to SS7 Signaling, Whitepaper Patton Electronics Company, 2012 (http://www.patton.com/whitepapers/Intro_to_SS7_Tutorial.pdf).

[47] Tutorial on Signaling System 7 (SS7), Performance Technologies, 2000-2003 (http://www.eurecom.fr/ dacier/Teaching/Eurecom/Intro_computer_nets/Recommended/ss7.pdf).

[48] *Signaling Transport Working Group*, http://www.hill2dot0.com/wiki/index.php?title=SIGTRAN.

[49] Tuomas Aura, Pekka Nikander and Gonzalo Camarillo, *Effects of Mobility and Multi-homing on Transport-Protocol Security*, 2009.

[50] International Journal of principles and applications of Information science and technology Vol.2, No.1,*A Secure 4-Way Handshake in 802.11i using cookies*,July 2008.

[51] Journal of Computers Vol.2 No.4, *Secure End-to-End Transport Over SCTP*, June 2007.

[52] Oracle Communications EAGLE Signaling Platform: *An Intelligent Evolution to 4G Networks*, An Oracle White Paper, January 2014.

[53] *European Telecommunications Standards Institute*, http://www.etsi.org/index.php/servirces/plugtests, Accessed October 2014.

[54] Mathew Stafford, *Signaling and Switching for Packet Telephony*, Artech House Teleccommunications Library, Boston 2004

[55] Ram Dantu, Sonia Fahmy, Henning Schulzrinne and Joao Cangussu, *Issues and challenges in securing VoIP*, Elsevier Ltd, 2009.

[56] U.C Meena, R. Saji Kumar and J.M. Suri, *Study Paper on Interconnect Issues in IP Networks*, Telecom Engineering Centre (Department of Telecommunications), Government of India.

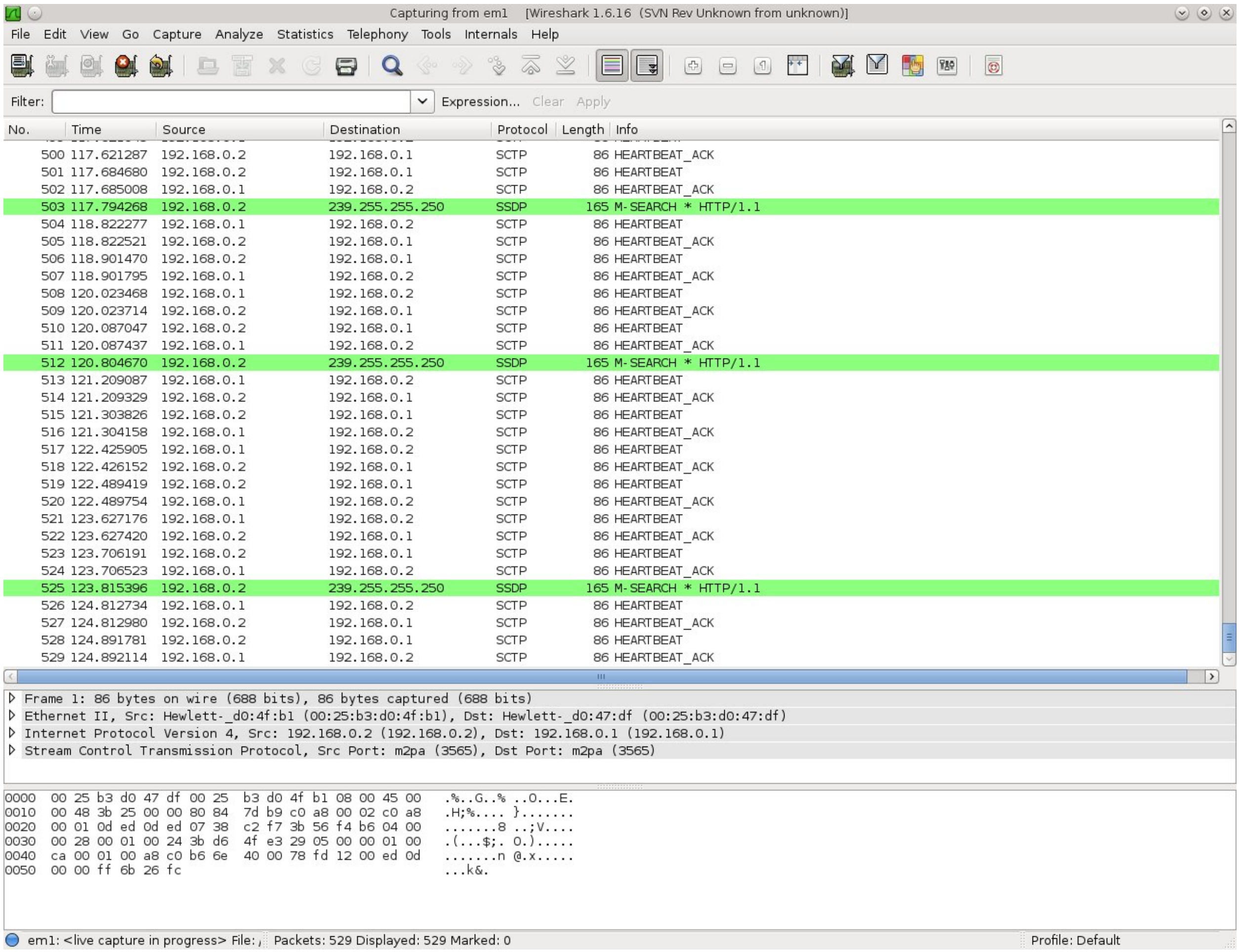
[57] ATIS Security Summit Report, *Security of Service Provider Infrastructure in an Era of Convergence*, February 4-5, 2003.

[58] Ravishankar Bhaskarrao Borgaonkar, *Security Analysis of Femtocell-Enabled Cellular Network Architecture*, Technische Universitat Berlin, 2013.

[59] Rahul Choudhari and Somanath Tripathy, *SCTP-Sec: A secure Transmission Control Protocol*, 2007.

Appendix A

Network IP Capture Screenshot



```
No.  Time       Source       Destination      Protocol Length Info
 500 117.621287 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT_ACK
 501 117.684680 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT
 502 117.685008 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT_ACK
 503 117.794268 192.168.0.2  239.255.255.250  SSDP       165 M-SEARCH * HTTP/1.1
 504 118.822277 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT
 505 118.822521 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT_ACK
 506 118.901470 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT
 507 118.901795 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT_ACK
 508 120.023468 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT
 509 120.023714 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT_ACK
 510 120.087047 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT
 511 120.087437 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT_ACK
 512 120.804670 192.168.0.2  239.255.255.250  SSDP       165 M-SEARCH * HTTP/1.1
 513 121.209087 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT
 514 121.209329 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT_ACK
 515 121.303826 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT
 516 121.304158 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT_ACK
 517 122.425905 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT
 518 122.426152 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT_ACK
 519 122.489419 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT
 520 122.489754 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT_ACK
 521 123.627176 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT
 522 123.627420 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT_ACK
 523 123.706191 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT
 524 123.706523 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT_ACK
 525 123.815396 192.168.0.2  239.255.255.250  SSDP       165 M-SEARCH * HTTP/1.1
 526 124.812734 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT
 527 124.812980 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT_ACK
 528 124.891781 192.168.0.2  192.168.0.1      SCTP        86 HEARTBEAT
 529 124.892114 192.168.0.1  192.168.0.2      SCTP        86 HEARTBEAT_ACK
```

```
▷ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
▷ Ethernet II, Src: Hewlett-_d0:4f:b1 (00:25:b3:d0:4f:b1), Dst: Hewlett-_d0:47:df (00:25:b3:d0:47:df)
▷ Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
▷ Stream Control Transmission Protocol, Src Port: m2pa (3565), Dst Port: m2pa (3565)
```

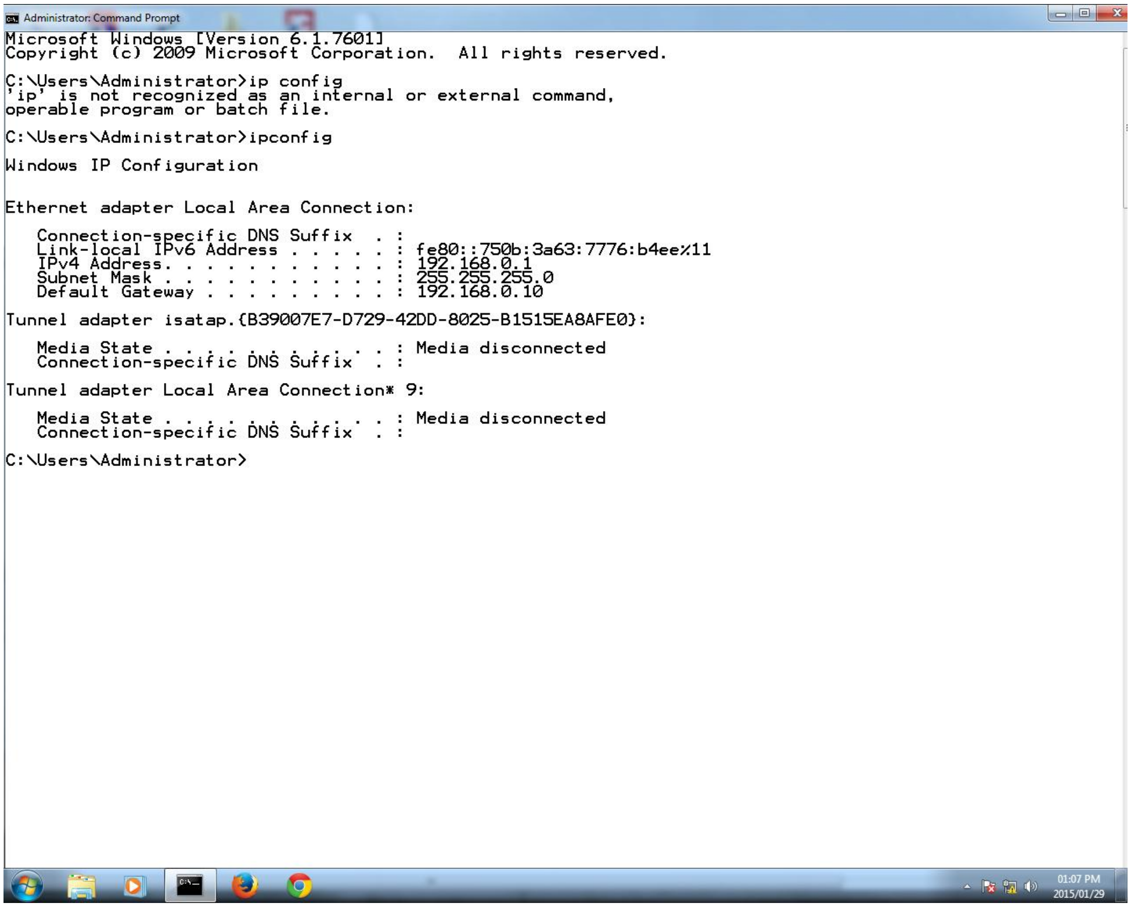
```
0000  00 25 b3 d0 47 df 00 25  b3 d0 4f b1 08 00 45 00   .%..G..% ..O...E.
0010  00 48 3b 25 00 00 80 84  7d b9 c0 a8 00 02 c0 a8   .H;%.... }.......
0020  00 01 0d ed 0d ed 07 38  c2 f7 3b 56 f4 b6 04 00   .......8 ..;V....
0030  00 28 00 01 00 24 3b d6  4f e3 29 05 00 00 01 00   .(...$;. O.).....
0040  ca 00 01 00 a8 c0 b6 6e  40 00 78 fd 12 00 ed 0d   .......n @.x.....
0050  00 00 ff 6b 26 fc                                  ...k&.
```

em1: <live capture in progress> File: Packets: 529 Displayed: 529 Marked: 0 Profile: Default

Figure A.1: Screenshot of Wireshark Network IP Capture

Appendix B

MTU Server Network Configuration Screenshot

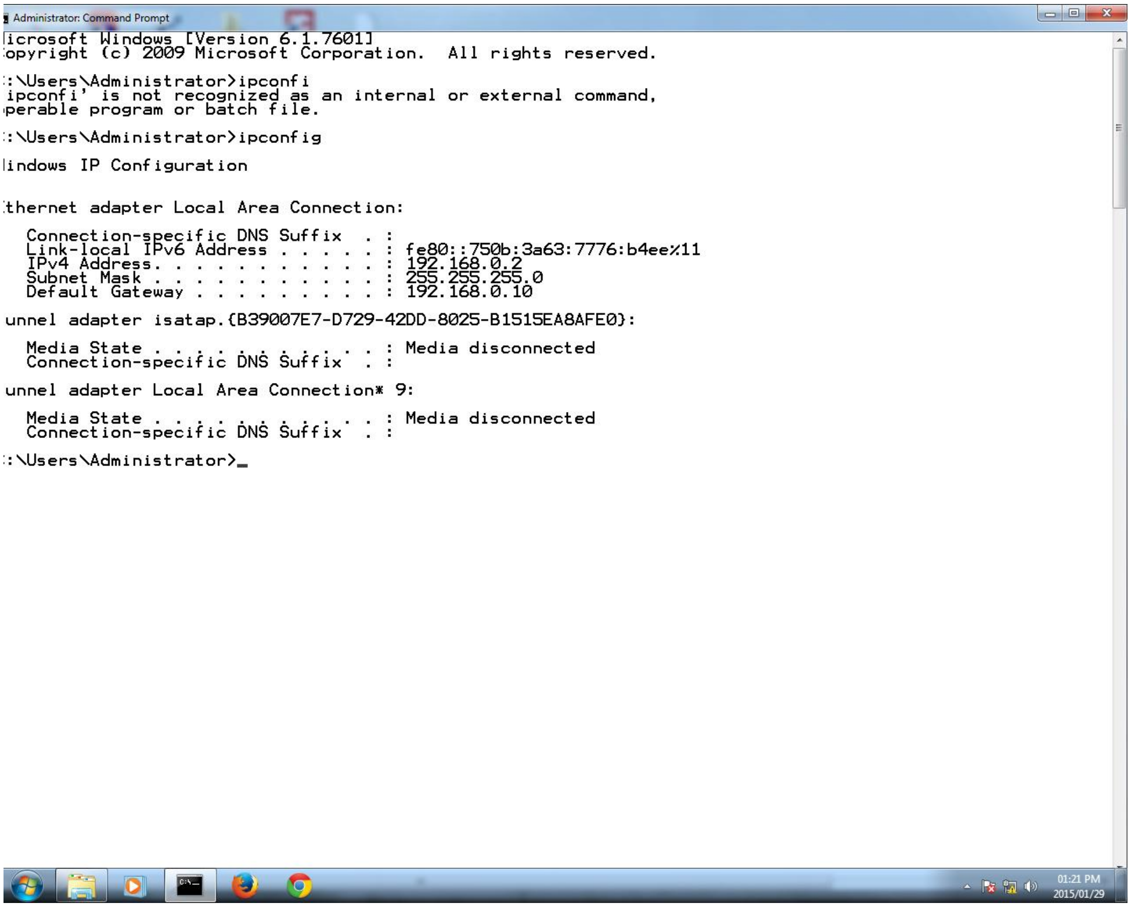


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ip config
'ip' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::750b:3a63:7776:b4ee%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.10

Tunnel adapter isatap.{B39007E7-D729-42DD-8025-B1515EA8AFE0}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Administrator>
```

Figure B.1: MTU Server Network Configuration Screenshot

Appendix C

MTR IP Network Configuration Screenshot

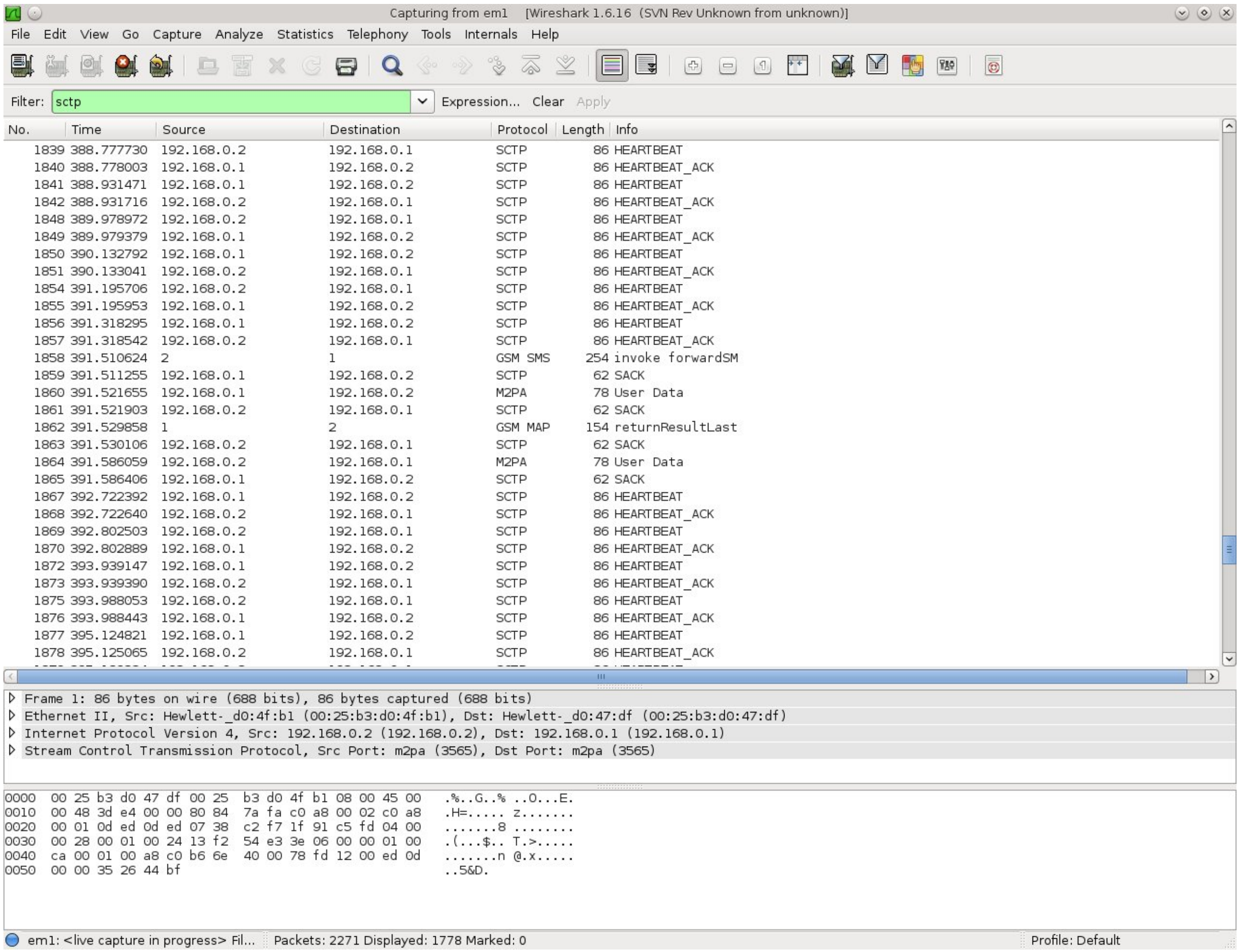


```
icrosoft Windows [Version 6.1.7601]
opyright (c) 2009 Microsoft Corporation.  All rights reserved.

:\Users\Administrator>ipconfi
ipconfi' is not recognized as an internal or external command,
perable program or batch file.

:\Users\Administrator>ipconfig

indows IP Configuration


thernet adapter Local Area Connection:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::750b:3a63:7776:b4ee%11
  IPv4 Address. . . . . . . . . . . : 192.168.0.2
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : 192.168.0.10

unnel adapter isatap.{B39007E7-D729-42DD-8025-B1515EA8AFE0}:

  Media State . . . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

unnel adapter Local Area Connection* 9:

  Media State . . . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

:\Users\Administrator>_
```

Figure C.1: MTR IP Network Configuration Screenshot

Appendix D

SCTP Capture Filter Screenshot



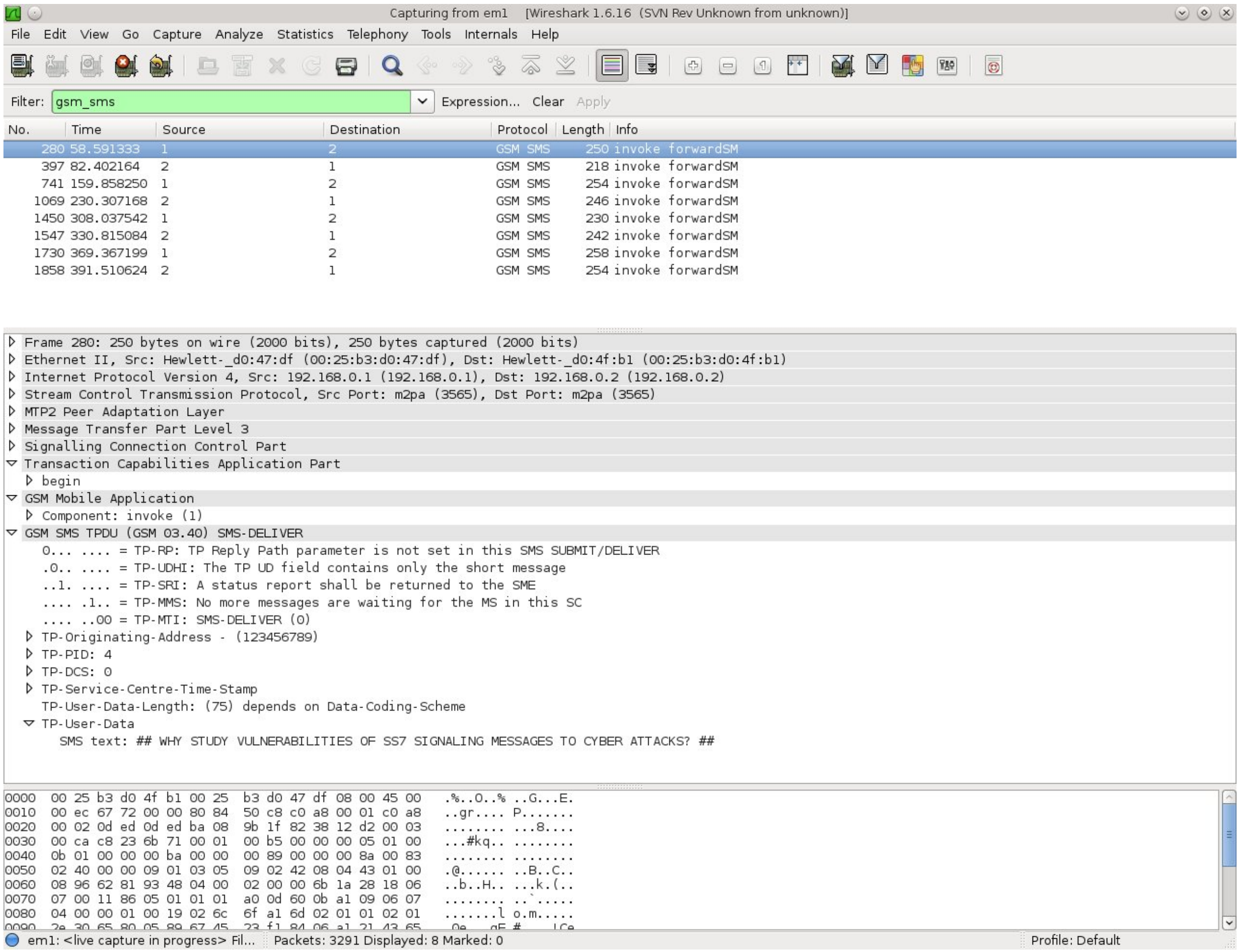
Capturing from em1 [Wireshark 1.6.16 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply
Profile: Default

```
Filter: sctp

No.   Time       Source        Destination   Protocol Length Info
 1839 388.777730 192.168.0.2   192.168.0.1   SCTP         86 HEARTBEAT
 1840 388.778003 192.168.0.1   192.168.0.2   SCTP         86 HEARTBEAT_ACK
 1841 388.931471 192.168.0.1   192.168.0.2   SCTP         86 HEARTBEAT
 1842 388.931716 192.168.0.2   192.168.0.1   SCTP         86 HEARTBEAT_ACK
 1848 389.978972 192.168.0.2   192.168.0.1   SCTP         86 HEARTBEAT
 1849 389.979379 192.168.0.1   192.168.0.2   SCTP         86 HEARTBEAT_ACK
 1850 390.132792 192.168.0.1   192.168.0.2   SCTP         86 HEARTBEAT
 1851 390.133041 192.168.0.2   192.168.0.1   SCTP         86 HEARTBEAT_ACK
 1854 391.195706 192.168.0.2   192.168.0.1   SCTP         86 HEARTBEAT
 1855 391.195953 192.168.0.1   192.168.0.2   SCTP         86 HEARTBEAT_ACK
 1856 391.318295 192.168.0.1   192.168.0.2   SCTP         86 HEARTBEAT
 1857 391.318542 192.168.0.2   192.168.0.1   SCTP         86 HEARTBEAT_ACK
 1858 391.510624 2             1             GSM SMS     254 invoke forwardSM
 1859 391.511255 192.168.0.1   192.168.0.2   SCTP         62 SACK
 1860 391.521655 192.168.0.1   192.168.0.2   M2PA         78 User Data
 1861 391.521903 192.168.0.2   192.168.0.1   SCTP         62 SACK
 1862 391.529858 1             2             GSM MAP     154 returnResultLast
 1863 391.530106 192.168.0.2   192.168.0.1   SCTP         62 SACK
 1864 391.586059 192.168.0.2   192.168.0.1   M2PA         78 User Data
 1865 391.586406 192.168.0.1   192.168.0.2   SCTP         62 SACK
 1867 392.722392 192.168.0.1   192.168.0.2   SCTP         86 HEARTBEAT
 1868 392.722640 192.168.0.2   192.168.0.1   SCTP         86 HEARTBEAT_ACK
 1869 392.802503 192.168.0.2   192.168.0.1   SCTP         86 HEARTBEAT
 1870 392.802889 192.168.0.1   192.168.0.2   SCTP         86 HEARTBEAT_ACK
 1872 393.939147 192.168.0.1   192.168.0.2   SCTP         86 HEARTBEAT
 1873 393.939390 192.168.0.2   192.168.0.1   SCTP         86 HEARTBEAT_ACK
 1875 393.988053 192.168.0.2   192.168.0.1   SCTP         86 HEARTBEAT
 1876 393.988443 192.168.0.1   192.168.0.2   SCTP         86 HEARTBEAT_ACK
 1877 395.124821 192.168.0.1   192.168.0.2   SCTP         86 HEARTBEAT
 1878 395.125065 192.168.0.2   192.168.0.1   SCTP         86 HEARTBEAT_ACK

▷ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
▷ Ethernet II, Src: Hewlett-_d0:4f:b1 (00:25:b3:d0:4f:b1), Dst: Hewlett-_d0:47:df (00:25:b3:d0:47:df)
▷ Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
▷ Stream Control Transmission Protocol, Src Port: m2pa (3565), Dst Port: m2pa (3565)

0000  00 25 b3 d0 47 df 00 25  b3 d0 4f b1 08 00 45 00   .%..G..% ..O...E.
0010  00 48 3d e4 00 00 80 84  7a fa c0 a8 00 02 c0 a8   .H=..... z.......
0020  00 01 0d ed 0d ed 07 38  c2 f7 1f 91 c5 fd 04 00   .......8 ........
0030  00 28 00 01 00 24 13 f2  54 e3 3e 06 00 00 01 00   .(...$.. T.>.....
0040  ca 00 01 00 a8 c0 b6 6e  40 00 78 fd 12 00 ed 0d   .......n @.x.....
0050  00 00 35 26 44 bf                                  ..5&D.

em1: <live capture in progress> Fil...   Packets: 2271 Displayed: 1778 Marked: 0
```

Figure D.1: Screenshot of the Wireshark SCTP Capture Filter

Appendix E

GSM SMS Text Message 1 Screenshot


Capturing from em1 [Wireshark 1.6.16 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply
Profile: Default

Filter: gsm_sms

```
No.   Time        Source   Destination   Protocol  Length Info
  280 58.591333   1        2             GSM SMS     250 invoke forwardSM
  397 82.402164   2        1             GSM SMS     218 invoke forwardSM
  741 159.858250  1        2             GSM SMS     254 invoke forwardSM
 1069 230.307168  2        1             GSM SMS     246 invoke forwardSM
 1450 308.037542  1        2             GSM SMS     230 invoke forwardSM
 1547 330.815084  2        1             GSM SMS     242 invoke forwardSM
 1730 369.367199  1        2             GSM SMS     258 invoke forwardSM
 1858 391.510624  2        1             GSM SMS     254 invoke forwardSM
```

```
▷ Frame 280: 250 bytes on wire (2000 bits), 250 bytes captured (2000 bits)
▷ Ethernet II, Src: Hewlett-_d0:47:df (00:25:b3:d0:47:df), Dst: Hewlett-_d0:4f:b1 (00:25:b3:d0:4f:b1)
▷ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.2 (192.168.0.2)
▷ Stream Control Transmission Protocol, Src Port: m2pa (3565), Dst Port: m2pa (3565)
▷ MTP2 Peer Adaptation Layer
▷ Message Transfer Part Level 3
▷ Signalling Connection Control Part
▽ Transaction Capabilities Application Part
  ▷ begin
▽ GSM Mobile Application
  ▷ Component: invoke (1)
▽ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..1. .... = TP-SRI: A status report shall be returned to the SME
    .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▷ TP-Originating-Address - (123456789)
  ▷ TP-PID: 4
  ▷ TP-DCS: 0
  ▷ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (75) depends on Data-Coding-Scheme
  ▽ TP-User-Data
      SMS text: ## WHY STUDY VULNERABILITIES OF SS7 SIGNALING MESSAGES TO CYBER ATTACKS? ##
```

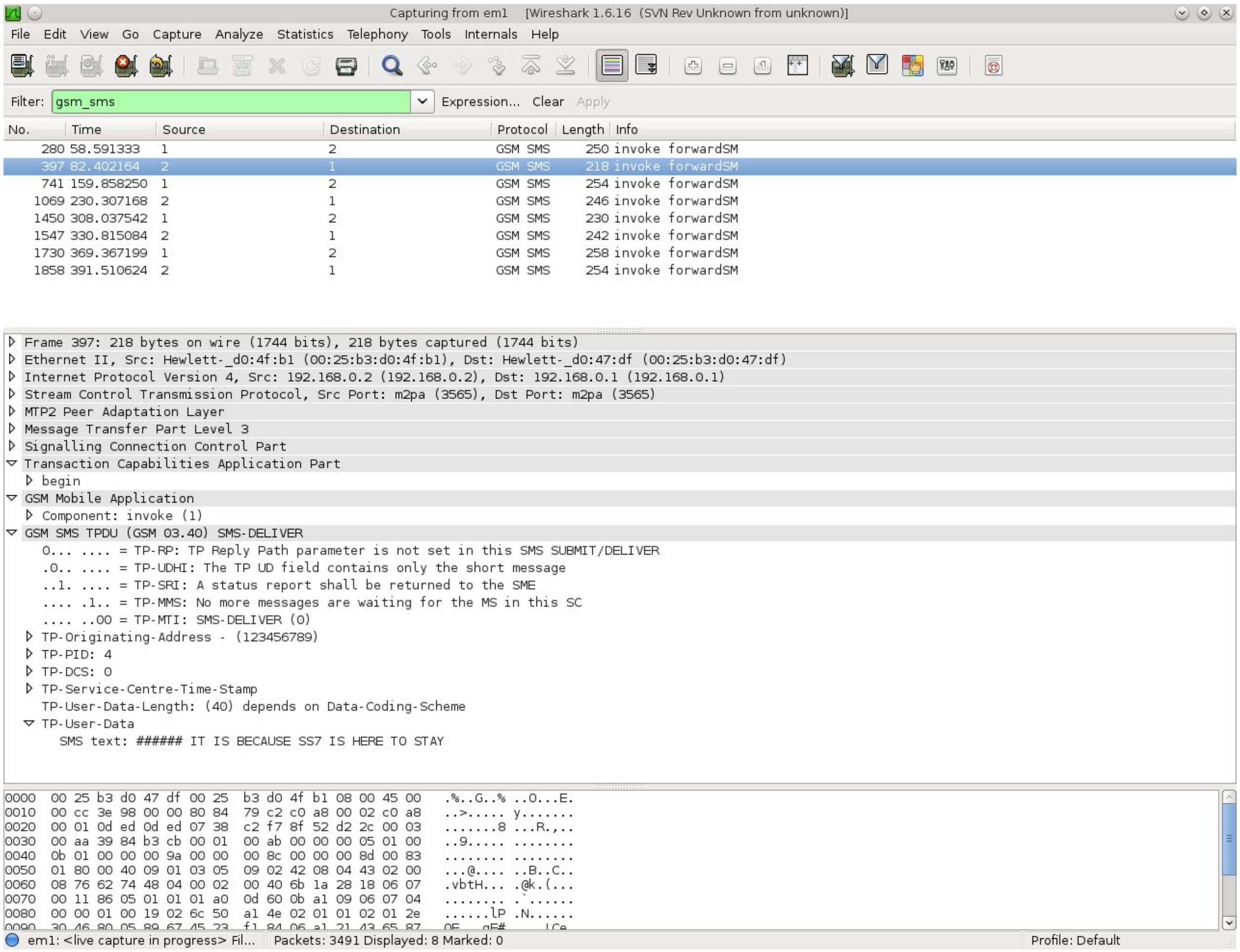
```
0000  00 25 b3 d0 4f b1 00 25  b3 d0 47 df 08 00 45 00   .%..O..% ..G...E.
0010  00 ec 67 72 00 00 80 84  50 c8 c0 a8 00 01 c0 a8   ..gr.... P.......
0020  00 02 0d ed 0d ed ba 08  9b 1f 82 38 12 d2 00 03   ........ ...8....
0030  00 ca c8 23 6b 71 00 01  00 b5 00 00 00 05 01 00   ...#kq.. ........
0040  0b 01 00 00 00 ba 00 00  00 89 00 00 00 8a 00 83   ........ ........
0050  02 40 00 00 09 01 03 05  09 02 42 08 04 43 01 00   .@...... ..B..C..
0060  08 96 62 81 93 48 04 00  02 00 00 6b 1a 28 18 06   ..b..H.. ...k.(..
0070  07 00 11 86 05 01 01 01  a0 0d 60 0b a1 09 06 07   ........ ..`.....
0080  04 00 00 01 00 19 02 6c  6f a1 6d 02 01 01 02 01   .......l o.m.....
0090  2e 30 65 80 05 89 67 45  23 f1 84 06 a1 21 43 65   .0e...gE #....!Ce
```

```
em1: <live capture in progress> Fil...   Packets: 3291 Displayed: 8 Marked: 0
```

Figure E.1: GSM SMS Text Message 1 Wireshark Screenshot

Appendix F

GSM SMS Text Message 2 Screenshot


Capturing from em1 [Wireshark 1.6.16 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: gsm_sms

```
No.     Time        Source                 Destination            Protocol  Length Info
    280 58.591333   1                      2                      GSM SMS      250 invoke forwardSM
    397 82.402164   2                      1                      GSM SMS      218 invoke forwardSM
    741 159.858250  1                      2                      GSM SMS      254 invoke forwardSM
   1069 230.307168  2                      1                      GSM SMS      246 invoke forwardSM
   1450 308.037542  1                      2                      GSM SMS      230 invoke forwardSM
   1547 330.815084  2                      1                      GSM SMS      242 invoke forwardSM
   1730 369.367199  1                      2                      GSM SMS      258 invoke forwardSM
   1858 391.510624  2                      1                      GSM SMS      254 invoke forwardSM
```

```
▷ Frame 397: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits)
▷ Ethernet II, Src: Hewlett-_d0:4f:b1 (00:25:b3:d0:4f:b1), Dst: Hewlett-_d0:47:df (00:25:b3:d0:47:df)
▷ Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
▷ Stream Control Transmission Protocol, Src Port: m2pa (3565), Dst Port: m2pa (3565)
▷ MTP2 Peer Adaptation Layer
▷ Message Transfer Part Level 3
▷ Signalling Connection Control Part
▽ Transaction Capabilities Application Part
  ▷ begin
▽ GSM Mobile Application
  ▷ Component: invoke (1)
▽ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..1. .... = TP-SRI: A status report shall be returned to the SME
    .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▷ TP-Originating-Address - (123456789)
  ▷ TP-PID: 4
  ▷ TP-DCS: 0
  ▷ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (40) depends on Data-Coding-Scheme
  ▽ TP-User-Data
      SMS text: ###### IT IS BECAUSE SS7 IS HERE TO STAY
```

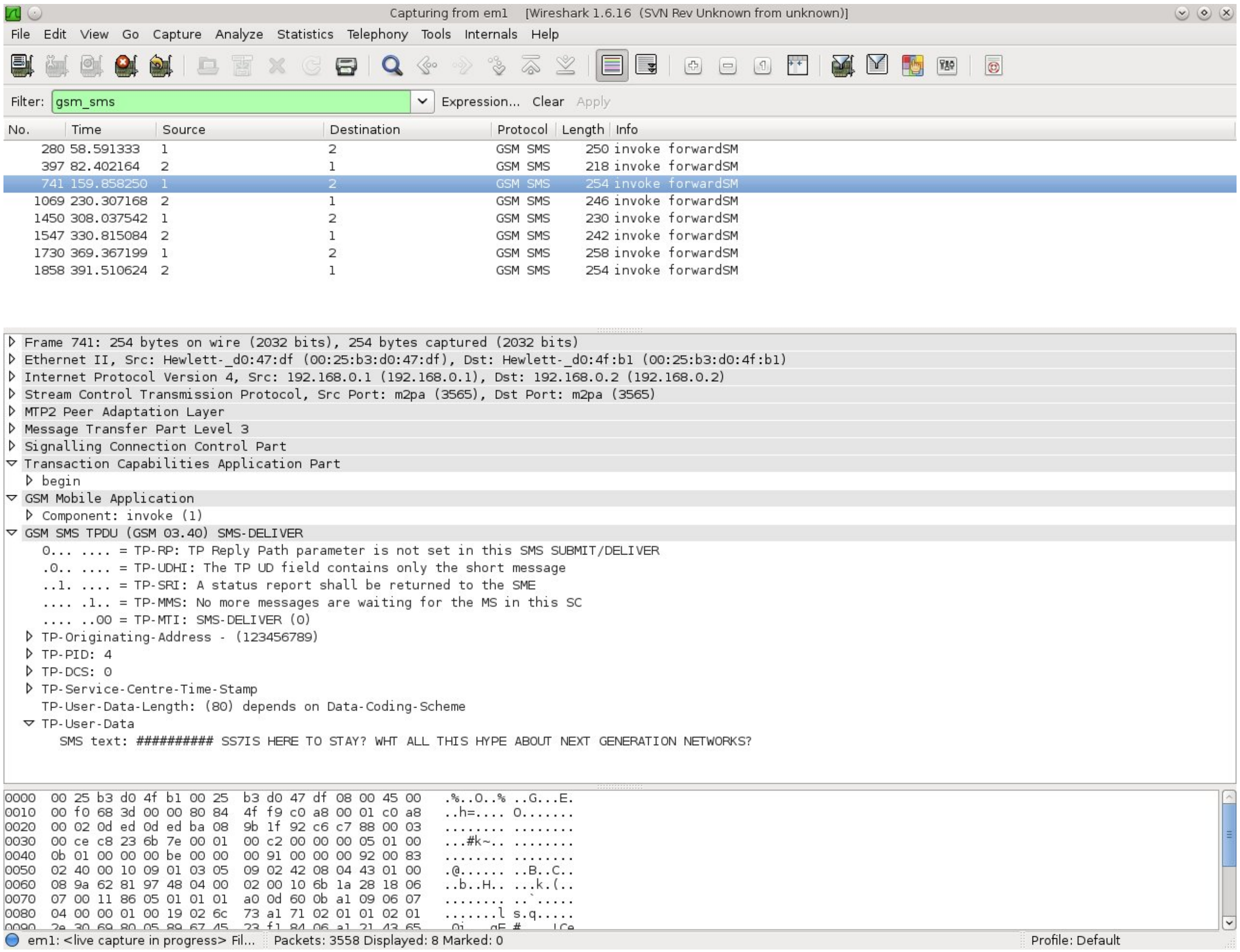
```
0000  00 25 b3 d0 47 df 00 25  b3 d0 4f b1 08 00 45 00   .%..G..% ..O...E.
0010  00 cc 3e 98 00 00 80 84  79 c2 c0 a8 00 02 c0 a8   ..>..... y.......
0020  00 01 0d ed 0d ed 07 38  c2 f7 8f 52 d2 2c 00 03   .......8 ...R.,..
0030  00 aa 39 84 b3 cb 00 01  00 ab 00 00 00 05 01 00   ..9..... ........
0040  0b 01 00 00 00 9a 00 00  00 8c 00 00 00 8d 00 83   ........ ........
0050  01 80 00 40 09 01 03 05  09 02 42 08 04 43 02 00   ...@.... ..B..C..
0060  08 76 62 74 48 04 00 02  00 40 6b 1a 28 18 06 07   .vbtH... .@k.(...
0070  00 11 86 05 01 01 01 a0  0d 60 0b a1 09 06 07 04   ........ .`......
0080  00 00 01 00 19 02 6c 50  a1 4e 02 01 01 02 01 2e   ......lP .N......
0090  30 46 80 05 89 67 45 23  f1 84 06 a1 21 43 65 87   0F...gE# ....!Ce.
```

em1: <live capture in progress> Fil... Packets: 3491 Displayed: 8 Marked: 0 Profile: Default

Figure F.1: GSM SMS Text Message 2 Wireshark screenshot

Appendix G

GSM SMS Text Message 3 Screenshot


Capturing from em1 [Wireshark 1.6.16 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

Filter: gsm_sms

```
No.    Time        Source  Destination  Protocol  Length Info
  280  58.591333   1       2            GSM SMS   250 invoke forwardSM
  397  82.402164   2       1            GSM SMS   218 invoke forwardSM
  741 159.858250   1       2            GSM SMS   254 invoke forwardSM
 1069 230.307168   2       1            GSM SMS   246 invoke forwardSM
 1450 308.037542   1       2            GSM SMS   230 invoke forwardSM
 1547 330.815084   2       1            GSM SMS   242 invoke forwardSM
 1730 369.367199   1       2            GSM SMS   258 invoke forwardSM
 1858 391.510624   2       1            GSM SMS   254 invoke forwardSM
```

```
▷ Frame 741: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits)
▷ Ethernet II, Src: Hewlett-_d0:47:df (00:25:b3:d0:47:df), Dst: Hewlett-_d0:4f:b1 (00:25:b3:d0:4f:b1)
▷ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.2 (192.168.0.2)
▷ Stream Control Transmission Protocol, Src Port: m2pa (3565), Dst Port: m2pa (3565)
▷ MTP2 Peer Adaptation Layer
▷ Message Transfer Part Level 3
▷ Signalling Connection Control Part
▽ Transaction Capabilities Application Part
  ▷ begin
▽ GSM Mobile Application
  ▷ Component: invoke (1)
▽ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..1. .... = TP-SRI: A status report shall be returned to the SME
    .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▷ TP-Originating-Address - (123456789)
  ▷ TP-PID: 4
  ▷ TP-DCS: 0
  ▷ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (80) depends on Data-Coding-Scheme
  ▽ TP-User-Data
      SMS text: ########## SS7IS HERE TO STAY? WHT ALL THIS HYPE ABOUT NEXT GENERATION NETWORKS?
```

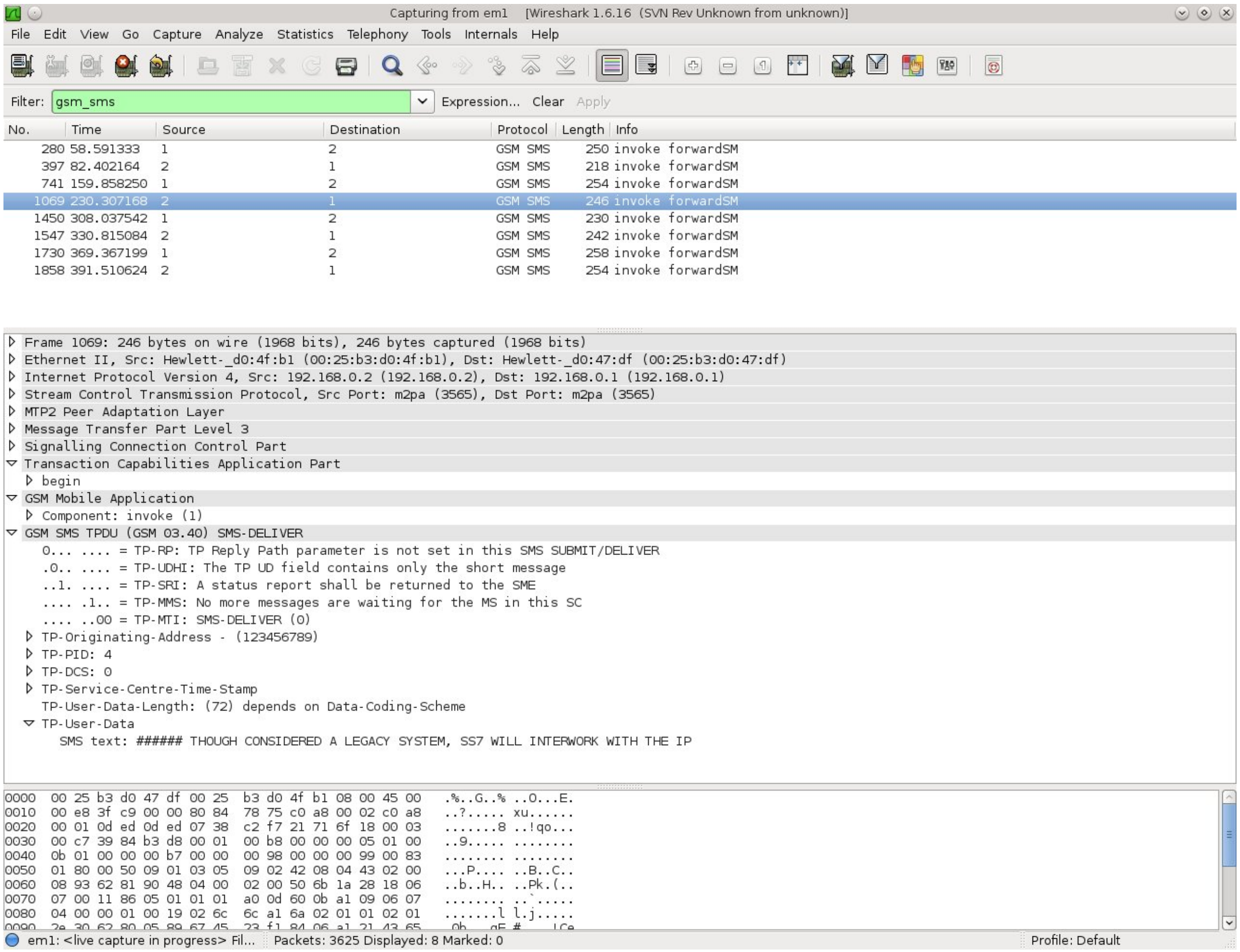
```
0000  00 25 b3 d0 4f b1 00 25  b3 d0 47 df 08 00 45 00   .%..O..% ..G...E.
0010  00 f0 68 3d 00 00 80 84  4f f9 c0 a8 00 01 c0 a8   ..h=.... O.......
0020  00 02 0d ed 0d ed ba 08  9b 1f 92 c6 c7 88 00 03   ........ ........
0030  00 ce c8 23 6b 7e 00 01  00 c2 00 00 00 05 01 00   ...#k~.. ........
0040  0b 01 00 00 00 be 00 00  00 91 00 00 00 92 00 83   ........ ........
0050  02 40 00 10 09 01 03 05  09 02 42 08 04 43 01 00   .@...... ..B..C..
0060  08 9a 62 81 97 48 04 00  02 00 10 6b 1a 28 18 06   ..b..H.. ...k.(..
0070  07 00 11 86 05 01 01 01  a0 0d 60 0b a1 09 06 07   ........ ..`.....
0080  04 00 00 01 00 19 02 6c  73 a1 71 02 01 01 02 01   .......l s.q.....
0090  2e 30 69 80 05 89 67 45  23 f1 84 06 a1 21 43 65   .0i...gE #....!Ce
```

em1: <live capture in progress> Fil... Packets: 3558 Displayed: 8 Marked: 0 Profile: Default

Figure G.1: GSM SMS Text Message 3 Wireshark Screenshot

Appendix H

GSM SMS Text Message 4 Screenshot


Capturing from em1 [Wireshark 1.6.16 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: gsm_sms

```
No.   Time        Source  Destination  Protocol  Length Info
  280 58.591333   1       2            GSM SMS      250 invoke forwardSM
  397 82.402164   2       1            GSM SMS      218 invoke forwardSM
  741 159.858250  1       2            GSM SMS      254 invoke forwardSM
 1069 230.307168  2       1            GSM SMS      246 invoke forwardSM
 1450 308.037542  1       2            GSM SMS      230 invoke forwardSM
 1547 330.815084  2       1            GSM SMS      242 invoke forwardSM
 1730 369.367199  1       2            GSM SMS      258 invoke forwardSM
 1858 391.510624  2       1            GSM SMS      254 invoke forwardSM
```

```
▷ Frame 1069: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits)
▷ Ethernet II, Src: Hewlett-_d0:4f:b1 (00:25:b3:d0:4f:b1), Dst: Hewlett-_d0:47:df (00:25:b3:d0:47:df)
▷ Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
▷ Stream Control Transmission Protocol, Src Port: m2pa (3565), Dst Port: m2pa (3565)
▷ MTP2 Peer Adaptation Layer
▷ Message Transfer Part Level 3
▷ Signalling Connection Control Part
▽ Transaction Capabilities Application Part
  ▷ begin
▽ GSM Mobile Application
  ▷ Component: invoke (1)
▽ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..1. .... = TP-SRI: A status report shall be returned to the SME
    .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▷ TP-Originating-Address - (123456789)
  ▷ TP-PID: 4
  ▷ TP-DCS: 0
  ▷ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (72) depends on Data-Coding-Scheme
  ▽ TP-User-Data
      SMS text: ###### THOUGH CONSIDERED A LEGACY SYSTEM, SS7 WILL INTERWORK WITH THE IP
```

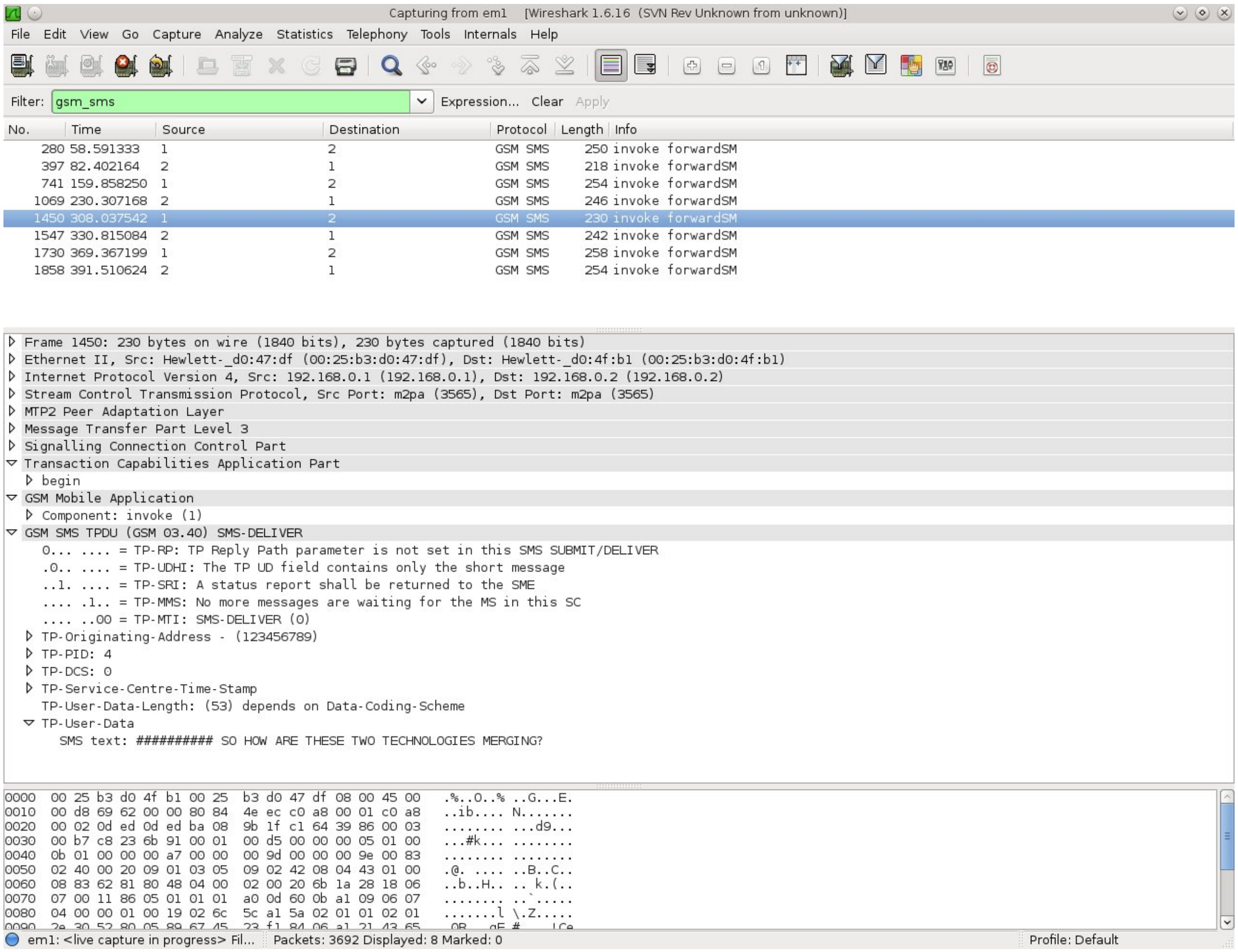
```
0000  00 25 b3 d0 47 df 00 25  b3 d0 4f b1 08 00 45 00   .%..G..% ..O...E.
0010  00 e8 3f c9 00 00 80 84  78 75 c0 a8 00 02 c0 a8   ..?..... xu......
0020  00 01 0d ed 0d ed 07 38  c2 f7 21 71 6f 18 00 03   .......8 ..!qo...
0030  00 c7 39 84 b3 d8 00 01  00 b8 00 00 00 05 01 00   ..9..... ........
0040  0b 01 00 00 00 b7 00 00  00 98 00 00 00 99 00 83   ........ ........
0050  01 80 00 50 09 01 03 05  09 02 42 08 04 43 02 00   ...P.... ..B..C..
0060  08 93 62 81 90 48 04 00  02 00 50 6b 1a 28 18 06   ..b..H.. ..Pk.(..
0070  07 00 11 86 05 01 01 01  a0 0d 60 0b a1 09 06 07   ........ ..`.....
0080  04 00 00 01 00 19 02 6c  6c a1 6a 02 01 01 02 01   .......l l.j.....
0090  2e 30 62 80 05 89 67 45  23 f1 84 06 a1 21 43 65   .0b...gE #....!Ce
```

em1: <live capture in progress> Fil... Packets: 3625 Displayed: 8 Marked: 0 Profile: Default

Figure H.1: GSM SMS Text Message 4 Wireshark screenshot

Appendix I

GSM SMS Text Message 5 Screenshot



Capturing from em1 [Wireshark 1.6.16 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: gsm_sms

```
No.     Time         Source      Destination    Protocol  Length  Info
    280 58.591333    1           2              GSM SMS      250 invoke forwardSM
    397 82.402164    2           1              GSM SMS      218 invoke forwardSM
    741 159.858250   1           2              GSM SMS      254 invoke forwardSM
   1069 230.307168   2           1              GSM SMS      246 invoke forwardSM
   1450 308.037542   1           2              GSM SMS      230 invoke forwardSM
   1547 330.815084   2           1              GSM SMS      242 invoke forwardSM
   1730 369.367199   1           2              GSM SMS      258 invoke forwardSM
   1858 391.510624   2           1              GSM SMS      254 invoke forwardSM
```

```
▷ Frame 1450: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits)
▷ Ethernet II, Src: Hewlett-_d0:47:df (00:25:b3:d0:47:df), Dst: Hewlett-_d0:4f:b1 (00:25:b3:d0:4f:b1)
▷ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.2 (192.168.0.2)
▷ Stream Control Transmission Protocol, Src Port: m2pa (3565), Dst Port: m2pa (3565)
▷ MTP2 Peer Adaptation Layer
▷ Message Transfer Part Level 3
▷ Signalling Connection Control Part
▽ Transaction Capabilities Application Part
  ▷ begin
▽ GSM Mobile Application
  ▷ Component: invoke (1)
▽ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..1. .... = TP-SRI: A status report shall be returned to the SME
    .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▷ TP-Originating-Address - (123456789)
  ▷ TP-PID: 4
  ▷ TP-DCS: 0
  ▷ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (53) depends on Data-Coding-Scheme
  ▽ TP-User-Data
      SMS text: ########## SO HOW ARE THESE TWO TECHNOLOGIES MERGING?
```

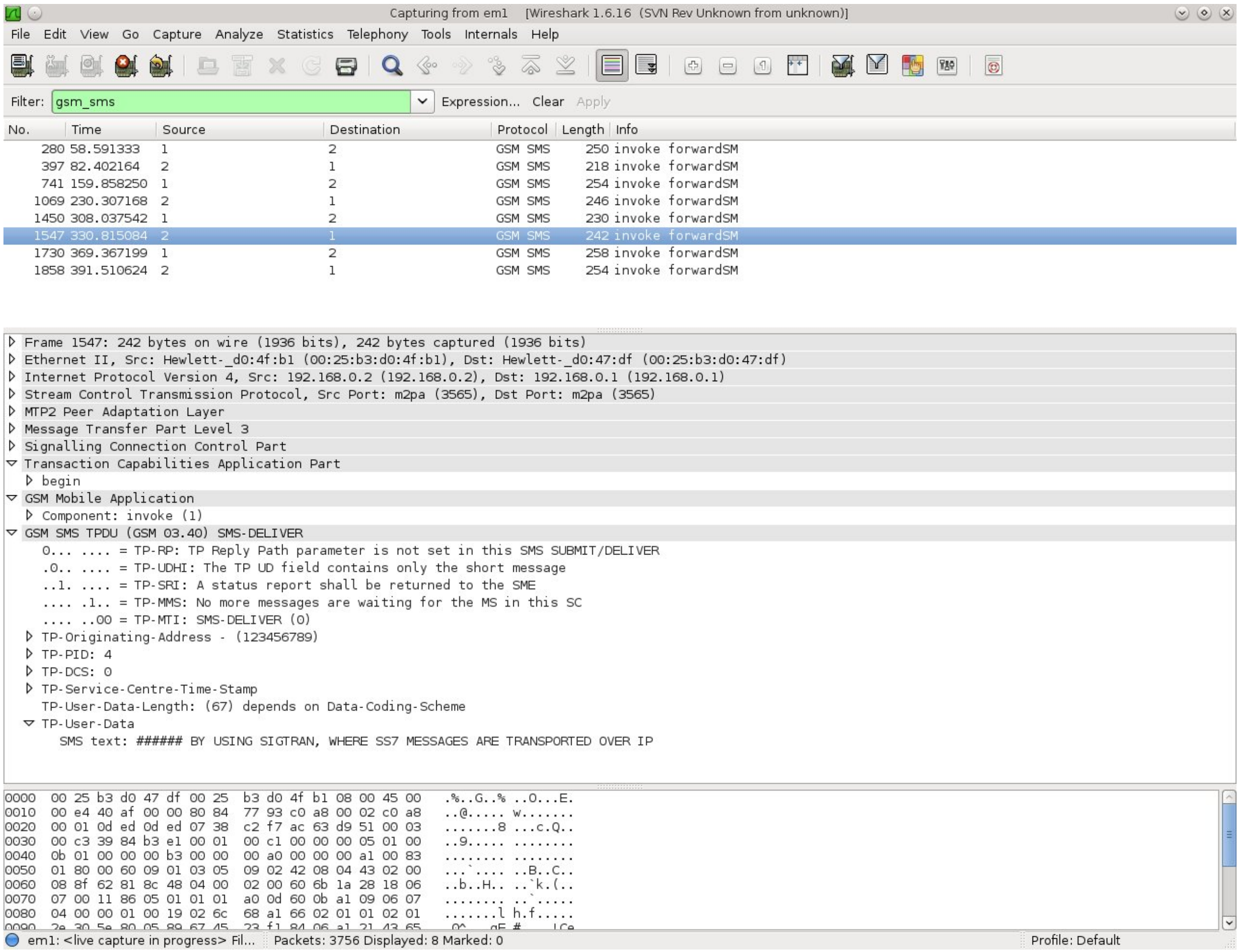
```
0000  00 25 b3 d0 4f b1 00 25  b3 d0 47 df 08 00 45 00   .%..O..% ..G...E.
0010  00 d8 69 62 00 00 80 84  4e ec c0 a8 00 01 c0 a8   ..ib.... N.......
0020  00 02 0d ed 0d ed ba 08  9b 1f c1 64 39 86 00 03   ........ ...d9...
0030  00 b7 c8 23 6b 91 00 01  00 d5 00 00 00 05 01 00   ...#k... ........
0040  0b 01 00 00 00 a7 00 00  00 9d 00 00 00 9e 00 83   ........ ........
0050  02 40 00 20 09 01 03 05  09 02 42 08 04 43 01 00   .@. .... ..B..C..
0060  08 83 62 81 80 48 04 00  02 00 20 6b 1a 28 18 06   ..b..H.. .. k.(..
0070  07 00 11 86 05 01 01 01  a0 0d 60 0b a1 09 06 07   ........ ..`.....
0080  04 00 00 01 00 19 02 6c  5c a1 5a 02 01 01 02 01   .......l \.Z.....
0090  2e 30 52 80 05 89 67 45  23 f1 84 06 a1 21 43 65   .0R...gE #....!Ce
```

em1: <live capture in progress> Fil... Packets: 3692 Displayed: 8 Marked: 0 Profile: Default

Figure I.1: GSM SMS Text Message 5 Wireshark screenshot

Appendix J

GSM SMS Text Message 6 Screenshot


Capturing from em1 [Wireshark 1.6.16 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: gsm_sms
Expression... Clear Apply

```
No.  Time        Source  Destination  Protocol  Length  Info
 280 58.591333   1       2            GSM SMS   250 invoke forwardSM
 397 82.402164   2       1            GSM SMS   218 invoke forwardSM
 741 159.858250  1       2            GSM SMS   254 invoke forwardSM
1069 230.307168  2       1            GSM SMS   246 invoke forwardSM
1450 308.037542  1       2            GSM SMS   230 invoke forwardSM
1547 330.815084  2       1            GSM SMS   242 invoke forwardSM
1730 369.367199  1       2            GSM SMS   258 invoke forwardSM
1858 391.510624  2       1            GSM SMS   254 invoke forwardSM
```

```
▷ Frame 1547: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
▷ Ethernet II, Src: Hewlett-_d0:4f:b1 (00:25:b3:d0:4f:b1), Dst: Hewlett-_d0:47:df (00:25:b3:d0:47:df)
▷ Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
▷ Stream Control Transmission Protocol, Src Port: m2pa (3565), Dst Port: m2pa (3565)
▷ MTP2 Peer Adaptation Layer
▷ Message Transfer Part Level 3
▷ Signalling Connection Control Part
▽ Transaction Capabilities Application Part
  ▷ begin
▽ GSM Mobile Application
  ▷ Component: invoke (1)
▽ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..1. .... = TP-SRI: A status report shall be returned to the SME
    .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▷ TP-Originating-Address - (123456789)
  ▷ TP-PID: 4
  ▷ TP-DCS: 0
  ▷ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (67) depends on Data-Coding-Scheme
  ▽ TP-User-Data
      SMS text: ###### BY USING SIGTRAN, WHERE SS7 MESSAGES ARE TRANSPORTED OVER IP
```

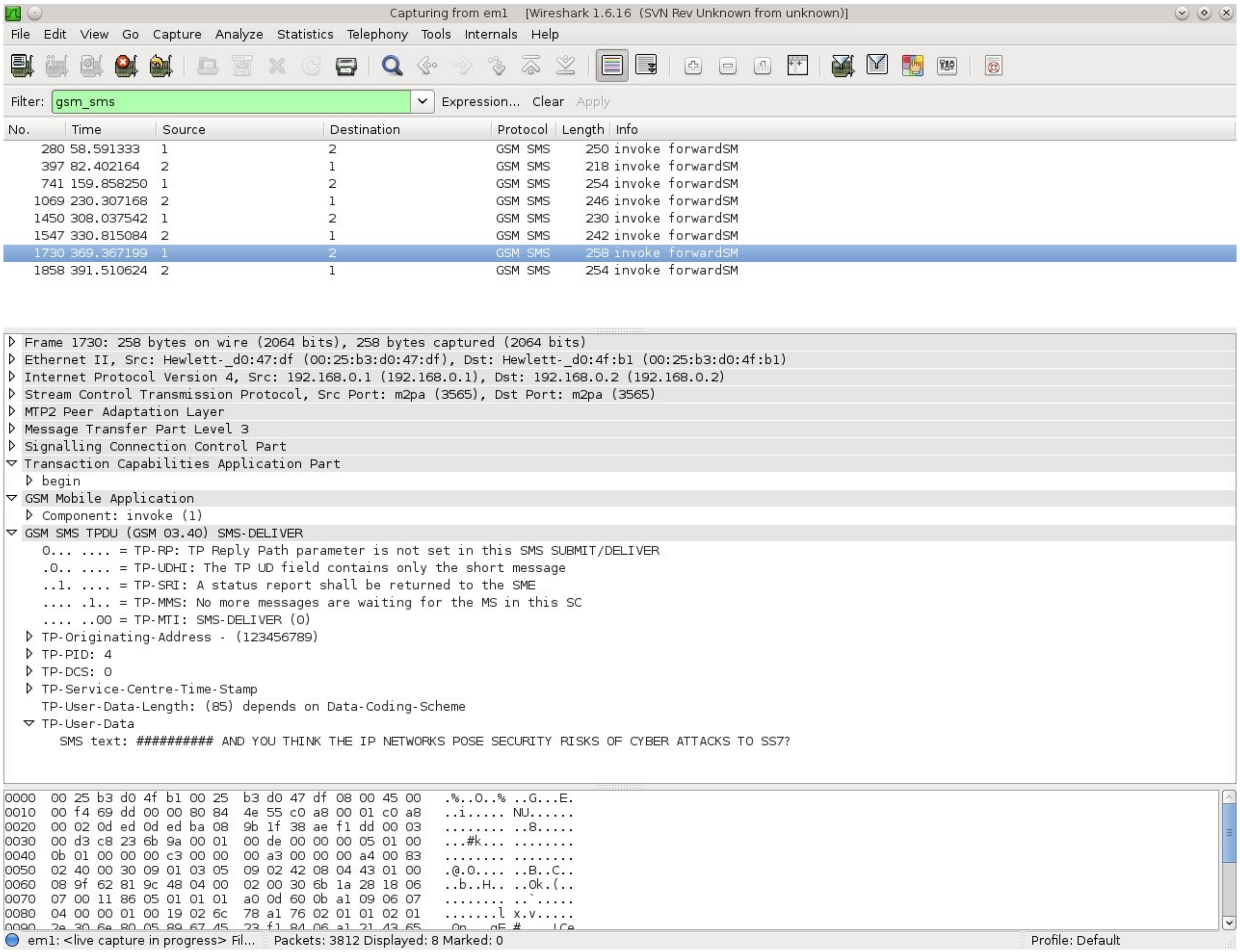
```
0000  00 25 b3 d0 47 df 00 25  b3 d0 4f b1 08 00 45 00   .%..G..% ..O...E.
0010  00 e4 40 af 00 00 80 84  77 93 c0 a8 00 02 c0 a8   ..@..... w.......
0020  00 01 0d ed 0d ed 07 38  c2 f7 ac 63 d9 51 00 03   .......8 ...c.Q..
0030  00 c3 39 84 b3 e1 00 01  00 c1 00 00 00 05 01 00   ..9..... ........
0040  0b 01 00 00 00 b3 00 00  00 a0 00 00 00 a1 00 83   ........ ........
0050  01 80 00 60 09 01 03 05  09 02 42 08 04 43 02 00   ...`.... ..B..C..
0060  08 8f 62 81 8c 48 04 00  02 00 60 6b 1a 28 18 06   ..b..H.. ..`k.(..
0070  07 00 11 86 05 01 01 01  a0 0d 60 0b a1 09 06 07   ........ ..`.....
0080  04 00 00 01 00 19 02 6c  68 a1 66 02 01 01 02 01   .......l h.f.....
0090  2e 30 5e 80 05 89 67 45  23 f1 84 06 a1 21 43 65   .0^...gE #....!Ce
```

em1: <live capture in progress> Fil... Packets: 3756 Displayed: 8 Marked: 0 Profile: Default

Figure J.1: GSM SMS Text Message 6 Wireshark screenshot

Appendix K

GSM SMS Text Message 7 Screenshot


Capturing from em1 [Wireshark 1.6.16 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

Filter: gsm_sms

```
No.   Time        Source  Destination  Protocol  Length Info
  280 58.591333   1       2            GSM SMS   250 invoke forwardSM
  397 82.402164   2       1            GSM SMS   218 invoke forwardSM
  741 159.858250  1       2            GSM SMS   254 invoke forwardSM
 1069 230.307168  2       1            GSM SMS   246 invoke forwardSM
 1450 308.037542  1       2            GSM SMS   230 invoke forwardSM
 1547 330.815084  2       1            GSM SMS   242 invoke forwardSM
 1730 369.367199  1       2            GSM SMS   258 invoke forwardSM
 1858 391.510624  2       1            GSM SMS   254 invoke forwardSM
```

```
▷ Frame 1730: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits)
▷ Ethernet II, Src: Hewlett-_d0:47:df (00:25:b3:d0:47:df), Dst: Hewlett-_d0:4f:b1 (00:25:b3:d0:4f:b1)
▷ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.2 (192.168.0.2)
▷ Stream Control Transmission Protocol, Src Port: m2pa (3565), Dst Port: m2pa (3565)
▷ MTP2 Peer Adaptation Layer
▷ Message Transfer Part Level 3
▷ Signalling Connection Control Part
▽ Transaction Capabilities Application Part
  ▷ begin
▽ GSM Mobile Application
  ▷ Component: invoke (1)
▽ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..1. .... = TP-SRI: A status report shall be returned to the SME
    .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▷ TP-Originating-Address - (123456789)
  ▷ TP-PID: 4
  ▷ TP-DCS: 0
  ▷ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (85) depends on Data-Coding-Scheme
  ▽ TP-User-Data
      SMS text: ########## AND YOU THINK THE IP NETWORKS POSE SECURITY RISKS OF CYBER ATTACKS TO SS7?
```

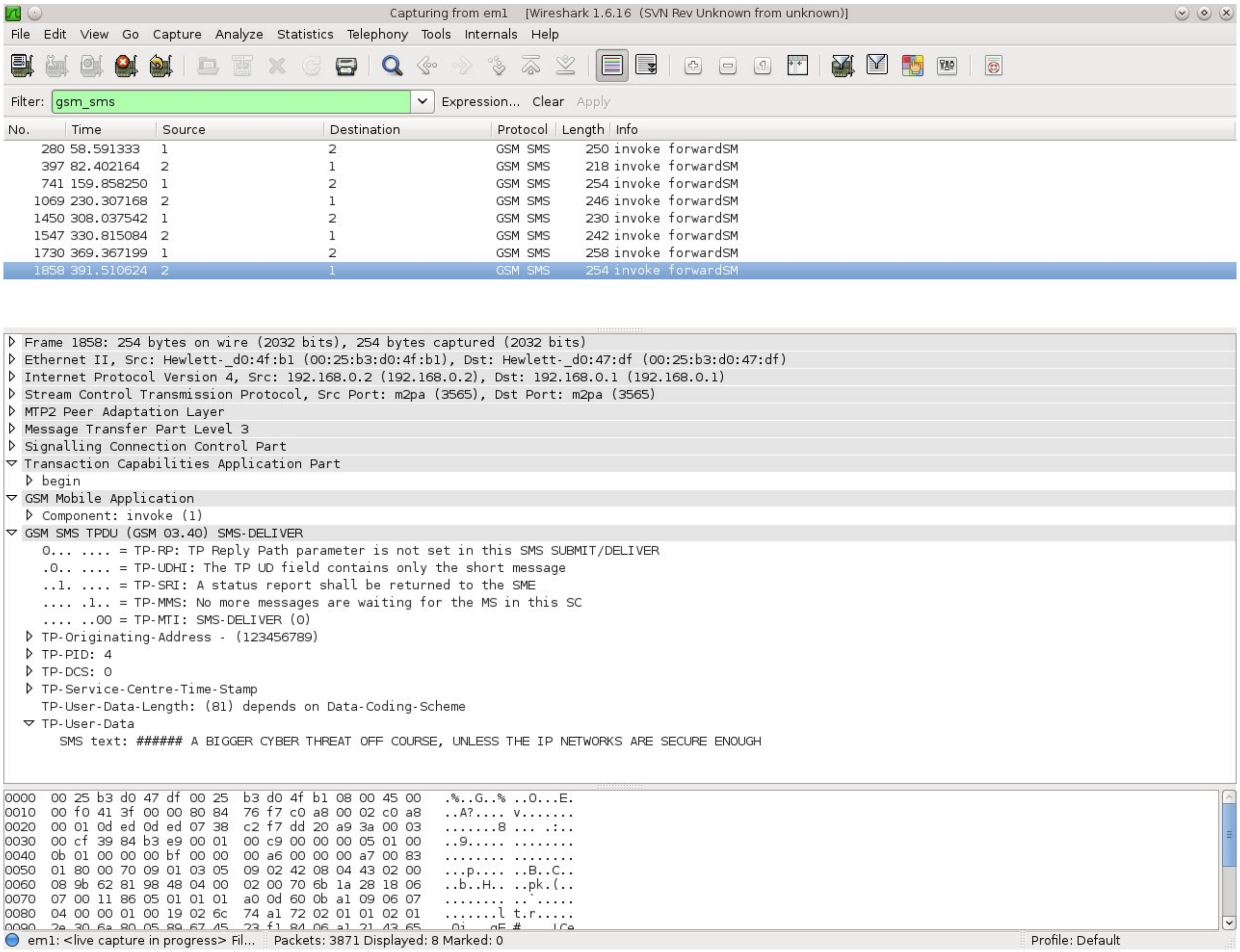
```
0000  00 25 b3 d0 4f b1 00 25  b3 d0 47 df 08 00 45 00   .%..O..% ..G...E.
0010  00 f4 69 dd 00 00 80 84  4e 55 c0 a8 00 01 c0 a8   ..i..... NU......
0020  00 02 0d ed 0d ed ba 08  9b 1f 38 ae f1 dd 00 03   ........ ..8.....
0030  00 d3 c8 23 6b 9a 00 01  00 de 00 00 00 05 01 00   ...#k... ........
0040  0b 01 00 00 00 c3 00 00  00 a3 00 00 00 a4 00 83   ........ ........
0050  02 40 00 30 09 01 03 05  09 02 42 08 04 43 01 00   .@.0.... ..B..C..
0060  08 9f 62 81 9c 48 04 00  02 00 30 6b 1a 28 18 06   ..b..H.. ..0k.(..
0070  07 00 11 86 05 01 01 01  a0 0d 60 0b a1 09 06 07   ........ ..`.....
0080  04 00 00 01 00 19 02 6c  78 a1 76 02 01 01 02 01   .......l x.v.....
0090  2e 30 6e 80 05 89 67 45  23 f1 84 06 a1 21 43 65   .0n...gE #....!Ce
```

em1: <live capture in progress> Fil... Packets: 3812 Displayed: 8 Marked: 0 Profile: Default

Figure K.1: GSM SMS Text Message 7 Wireshark screenshot

Appendix L

GSM SMS Text Message 8 Screenshot



Capturing from em1 [Wireshark 1.6.16 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: gsm_sms
Expression... Clear Apply

```
No.  Time        Source  Destination  Protocol  Length  Info
 280 58.591333   1       2            GSM SMS      250 invoke forwardSM
 397 82.402164   2       1            GSM SMS      218 invoke forwardSM
 741 159.858250  1       2            GSM SMS      254 invoke forwardSM
1069 230.307168  2       1            GSM SMS      246 invoke forwardSM
1450 308.037542  1       2            GSM SMS      230 invoke forwardSM
1547 330.815084  2       1            GSM SMS      242 invoke forwardSM
1730 369.367199  1       2            GSM SMS      258 invoke forwardSM
1858 391.510624  2       1            GSM SMS      254 invoke forwardSM
```

```
▷ Frame 1858: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits)
▷ Ethernet II, Src: Hewlett-_d0:4f:b1 (00:25:b3:d0:4f:b1), Dst: Hewlett-_d0:47:df (00:25:b3:d0:47:df)
▷ Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
▷ Stream Control Transmission Protocol, Src Port: m2pa (3565), Dst Port: m2pa (3565)
▷ MTP2 Peer Adaptation Layer
▷ Message Transfer Part Level 3
▷ Signalling Connection Control Part
▽ Transaction Capabilities Application Part
  ▷ begin
▽ GSM Mobile Application
  ▷ Component: invoke (1)
▽ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..1. .... = TP-SRI: A status report shall be returned to the SME
    .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▷ TP-Originating-Address - (123456789)
  ▷ TP-PID: 4
  ▷ TP-DCS: 0
  ▷ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (81) depends on Data-Coding-Scheme
  ▽ TP-User-Data
      SMS text: ###### A BIGGER CYBER THREAT OFF COURSE, UNLESS THE IP NETWORKS ARE SECURE ENOUGH
```

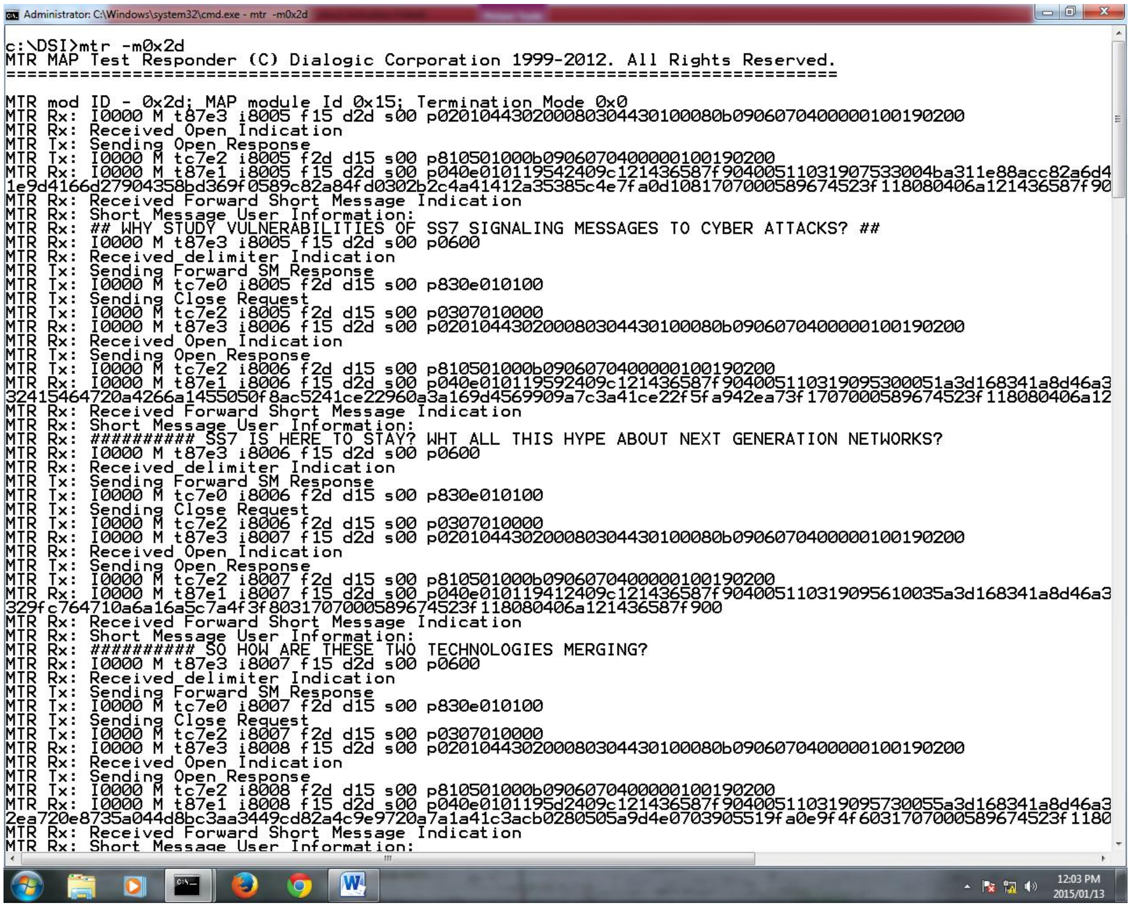
```
0000  00 25 b3 d0 47 df 00 25  b3 d0 4f b1 08 00 45 00   .%..G..% ..O...E.
0010  00 f0 41 3f 00 00 80 84  76 f7 c0 a8 00 02 c0 a8   ..A?.... v.......
0020  00 01 0d ed 0d ed 07 38  c2 f7 dd 20 a9 3a 00 03   .......8 ... .:..
0030  00 cf 39 84 b3 e9 00 01  00 c9 00 00 00 05 01 00   ..9..... ........
0040  0b 01 00 00 00 bf 00 00  00 a6 00 00 00 a7 00 83   ........ ........
0050  01 80 00 70 09 01 03 05  09 02 42 08 04 43 02 00   ...p.... ..B..C..
0060  08 9b 62 81 98 48 04 00  02 00 70 6b 1a 28 18 06   ..b..H.. ..pk.(..
0070  07 00 11 86 05 01 01 01  a0 0d 60 0b a1 09 06 07   ........ ..`.....
0080  04 00 00 01 00 19 02 6c  74 a1 72 02 01 01 02 01   .......l t.r.....
0090  2e 30 6a 80 05 89 67 45  23 f1 84 06 a1 21 43 65   .0j...gE #....!Ce
```

em1: <live capture in progress> Fil...
Packets: 3871 Displayed: 8 Marked: 0
Profile: Default

Figure L.1: GSM SMS Text Message 8 Wireshark screenshot

Appendix M

MTR Received Messages Screenshot

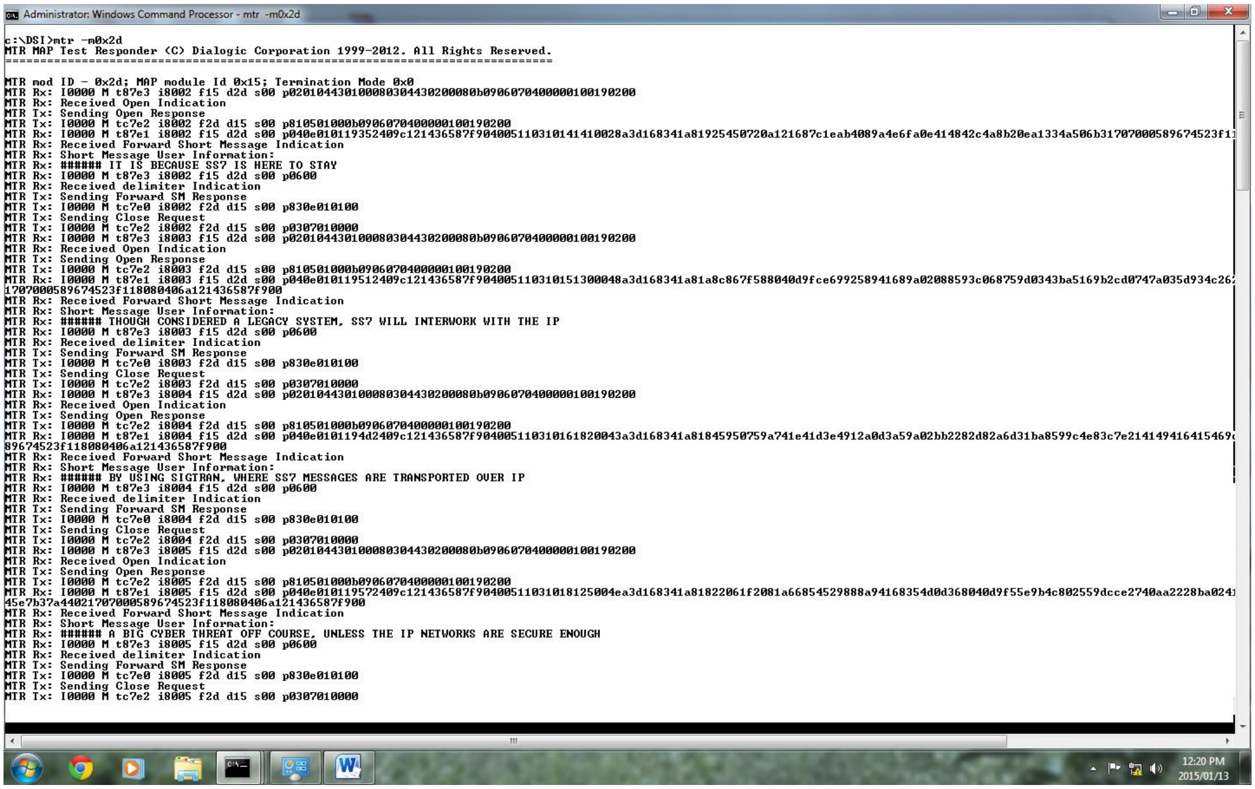


```
c:\DSI>mtr -m0x2d
MTR MAP Test Responder (C) Dialogic Corporation 1999-2012. All Rights Reserved.
===============================================================================

MTR mod ID - 0x2d; MAP module Id 0x15; Termination Mode 0x0
MTR Rx: I0000 M t87e3 i8005 f15 d2d s00 p0201044302000803044301000800b09060704000001001902000
MTR Rx: Received Open Indication
MTR Tx: Sending Open Response
MTR Tx: I0000 M tc7e2 i8005 f2d d15 s00 p810501000b09060704000001001902000
MTR Rx: I0000 M t87e1 i8005 f15 d2d s00 p040e010119542409c121436587f904005110319075330004ba311e88acc82a6d4
1e9d4166d27904358bd369f0589c82a84fd0302b2c4a41412a35385c4e7fa0d108170700058967452 3f118080406a121436587f90
MTR Rx: Received Forward Short Message Indication
MTR Rx: Short Message User Information:
MTR Rx: ## WHY STUDY VULNERABILITIES OF SS7 SIGNALING MESSAGES TO CYBER ATTACKS? ##
MTR Rx: I0000 M t87e3 i8005 f15 d2d s00 p0600
MTR Rx: Received delimiter Indication
MTR Tx: Sending Forward SM Response
MTR Tx: I0000 M tc7e0 i8005 f2d d15 s00 p830e010100
MTR Tx: Sending Close Request
MTR Tx: I0000 M tc7e2 i8005 f2d d15 s00 p0307010000
MTR Rx: I0000 M t87e3 i8006 f15 d2d s00 p0201044302000803044301000800b09060704000001001902000
MTR Rx: Received Open Indication
MTR Tx: Sending Open Response
MTR Tx: I0000 M tc7e2 i8006 f2d d15 s00 p810501000b09060704000001001902000
MTR Rx: I0000 M t87e1 i8006 f15 d2d s00 p040e010119592409c121436587f904005110319095300051a3d168341a8d46a3
32415464720a4266a1455050f8ac5241ce22960a3a169d4569909a7c3a41ce22f5fa942ea73f170700058967452 3f118080406a12
MTR Rx: Received Forward Short Message Indication
MTR Rx: Short Message User Information:
MTR Rx: ########## SS7 IS HERE TO STAY? WHT ALL THIS HYPE ABOUT NEXT GENERATION NETWORKS?
MTR Rx: I0000 M t87e3 i8006 f15 d2d s00 p0600
MTR Rx: Received delimiter Indication
MTR Tx: Sending Forward SM Response
MTR Tx: I0000 M tc7e0 i8006 f2d d15 s00 p830e010100
MTR Tx: Sending Close Request
MTR Tx: I0000 M tc7e2 i8006 f2d d15 s00 p0307010000
MTR Rx: I0000 M t87e3 i8007 f15 d2d s00 p0201044302000803044301000800b09060704000001001902000
MTR Rx: Received Open Indication
MTR Tx: Sending Open Response
MTR Tx: I0000 M tc7e2 i8007 f2d d15 s00 p810501000b09060704000001001902000
MTR Rx: I0000 M t87e1 i8007 f15 d2d s00 p040e010119412409c121436587f904005110319095610035a3d168341a8d46a3
329fc764710a6a16a5c7a4f3f8031707000589674523f118080406a121436587f900
MTR Rx: Received Forward Short Message Indication
MTR Rx: Short Message User Information:
MTR Rx: ########## SO HOW ARE THESE TWO TECHNOLOGIES MERGING?
MTR Rx: I0000 M t87e3 i8007 f15 d2d s00 p0600
MTR Rx: Received delimiter Indication
MTR Tx: Sending Forward SM Response
MTR Tx: I0000 M tc7e0 i8007 f2d d15 s00 p830e010100
MTR Tx: Sending Close Request
MTR Tx: I0000 M tc7e2 i8007 f2d d15 s00 p0307010000
MTR Rx: I0000 M t87e3 i8008 f15 d2d s00 p0201044302000803044301000800b09060704000001001902000
MTR Rx: Received Open Indication
MTR Tx: Sending Open Response
MTR Tx: I0000 M tc7e2 i8008 f2d d15 s00 p810501000b09060704000001001902000
MTR Rx: I0000 M t87e1 i8008 f15 d2d s00 p040e0101195d2409c121436587f904005110319095730055a3d168341a8d46a3
2ea720e8735a044d8bc3aa3449cd82a4c9e9720a7a1a41c3acb0280505a9d4e0703905519fa0e9f4f6031707000589674523f1180
MTR Rx: Received Forward Short Message Indication
MTR Rx: Short Message User Information:
```

Figure M.1: Screenshot of MTR Received Messages

Appendix N

MTU Received Messages Screenshot

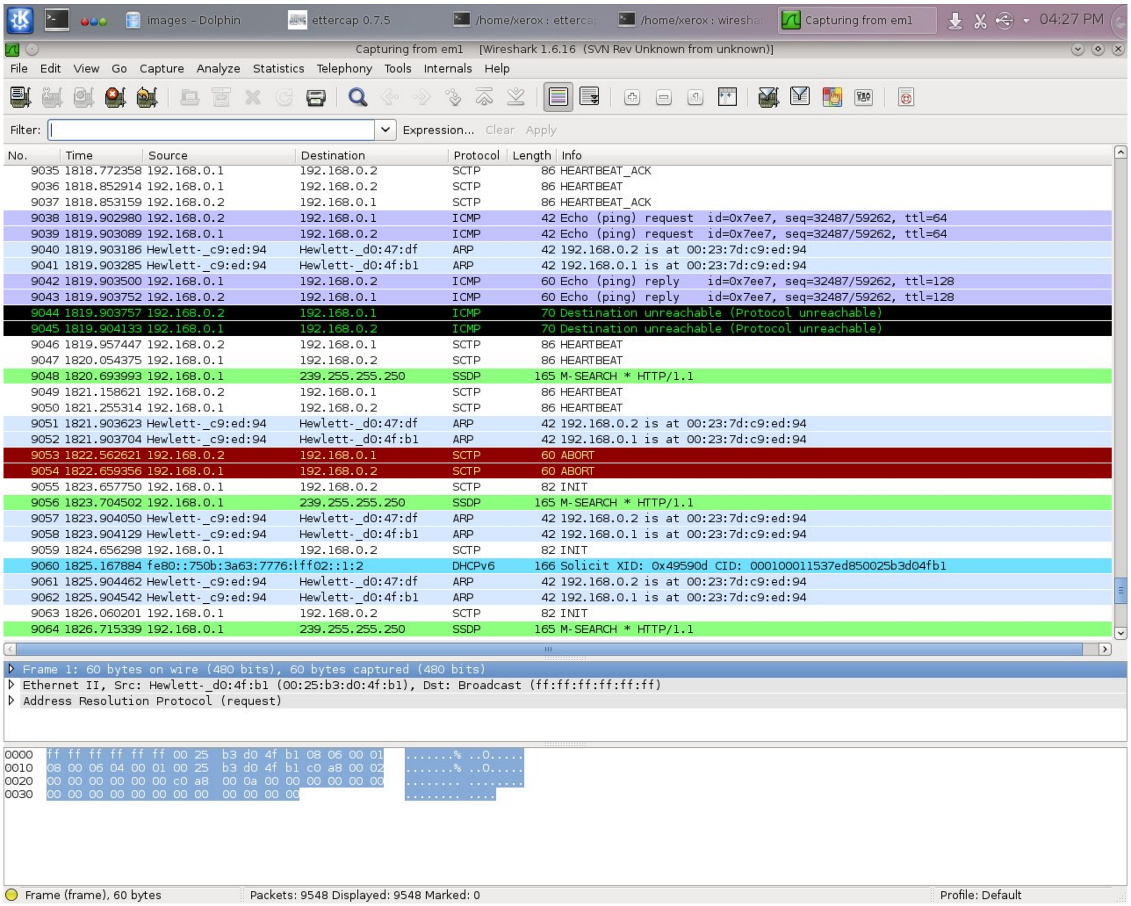


```
c:\DSI>mtr -m0x2d
MTR MAP Test Responder (C) Dialogic Corporation 1999-2012. All Rights Reserved.
================================================================================

MTR mod ID - 0x2d; MAP module Id 0x15; Termination Mode 0x0
MTR Rx: I0000 M t87e3 i8002 f15 d2d s00 p02010443010008030443020008 0b09060704000001001902 00
MTR Rx: Received Open Indication
MTR Tx: Sending Open Response
MTR Tx: I0000 M tc7e2 i8002 f2d d15 s00 p810501000b09060704000001001902 00
MTR Rx: I0000 M t87e1 i8002 f15 d2d s00 p040e010119352409c121436587f904005110310141410028a3d168341a81925450720a121687c1eab4089a4e6fa0e414842c4a8b20ea1334a506b31707000589674523f11
MTR Rx: Received Forward Short Message Indication
MTR Rx: Short Message User Information:
MTR Rx: ###### IT IS BECAUSE SS7 IS HERE TO STAY
MTR Rx: I0000 M t87e3 i8002 f15 d2d s00 p0600
MTR Rx: Received delimiter Indication
MTR Tx: Sending Forward SM Response
MTR Tx: I0000 M tc7e0 i8002 f2d d15 s00 p830e010100
MTR Tx: Sending Close Request
MTR Tx: I0000 M tc7e2 i8002 f2d d15 s00 p0307010000
MTR Rx: I0000 M t87e3 i8003 f15 d2d s00 p020104430100080304430200080b0906070400000100190200
MTR Rx: Received Open Indication
MTR Tx: Sending Open Response
MTR Tx: I0000 M tc7e2 i8003 f2d d15 s00 p810501000b0906070400000100190200
MTR Rx: I0000 M t87e1 i8003 f15 d2d s00 p040e010119512409c121436587f904005110310151300048a3d168341a81a8c867f588040d9fce699258941689a02088593c068759d0343ba5169b2cd0747a035d934c262
1707000589674523f118080406a121436587f900
MTR Rx: Received Forward Short Message Indication
MTR Rx: Short Message User Information:
MTR Rx: ###### THOUGH CONSIDERED A LEGACY SYSTEM, SS7 WILL INTERWORK WITH THE IP
MTR Rx: I0000 M t87e3 i8003 f15 d2d s00 p0600
MTR Rx: Received delimiter Indication
MTR Tx: Sending Forward SM Response
MTR Tx: I0000 M tc7e0 i8003 f2d d15 s00 p830e010100
MTR Tx: Sending Close Request
MTR Tx: I0000 M tc7e2 i8003 f2d d15 s00 p0307010000
MTR Rx: I0000 M t87e3 i8004 f15 d2d s00 p020104430100080304430200080b0906070400000100190200
MTR Rx: Received Open Indication
MTR Tx: Sending Open Response
MTR Tx: I0000 M tc7e2 i8004 f2d d15 s00 p810501000b0906070400000100190200
MTR Rx: I0000 M t87e1 i8004 f15 d2d s00 p040e0101194d2409c121436587f904005110310161820043a3d168341a81845950759a741e41d3e4912a0d3a59a02bb2282d82a6d31ba8599c4e83c7e214149416415469c
89674523f118080406a121436587f900
MTR Rx: Received Forward Short Message Indication
MTR Rx: Short Message User Information:
MTR Rx: ###### BY USING SIGTRAN, WHERE SS7 MESSAGES ARE TRANSPORTED OVER IP
MTR Rx: I0000 M t87e3 i8004 f15 d2d s00 p0600
MTR Rx: Received delimiter Indication
MTR Tx: Sending Forward SM Response
MTR Tx: I0000 M tc7e0 i8004 f2d d15 s00 p830e010100
MTR Tx: Sending Close Request
MTR Tx: I0000 M tc7e2 i8004 f2d d15 s00 p0307010000
MTR Rx: I0000 M t87e3 i8005 f15 d2d s00 p020104430100080304430200080b0906070400000100190200
MTR Rx: Received Open Indication
MTR Tx: Sending Open Response
MTR Tx: I0000 M tc7e2 i8005 f2d d15 s00 p810501000b0906070400000100190200
MTR Rx: I0000 M t87e1 i8005 f15 d2d s00 p040e010119572409c121436587f90400511031018125004ea3d168341a81822061f2081a66854529888a94168354d0d368040d9f55e9b4c802559dcce2740aa2228ba0241
45e7b37a4402170700058967452 3f118080406a121436587f900
MTR Rx: Received Forward Short Message Indication
MTR Rx: Short Message User Information:
MTR Rx: ###### A BIG CYBER THREAT OFF COURSE, UNLESS THE IP NETWORKS ARE SECURE ENOUGH
MTR Rx: I0000 M t87e3 i8005 f15 d2d s00 p0600
MTR Rx: Received delimiter Indication
MTR Tx: Sending Forward SM Response
MTR Tx: I0000 M tc7e0 i8005 f2d d15 s00 p830e010100
MTR Tx: Sending Close Request
MTR Tx: I0000 M tc7e2 i8005 f2d d15 s00 p0307010000
```

Figure N.1: Screenshot of MTU Received Messages

Appendix O

Ettercap ARP Poisoning Screenshot


images – Dolphin
ettercap 0.7.5
/home/xerox : ettercap
/home/xerox : wireshar
Capturing from em1
04:27 PM
Capturing from em1 [Wireshark 1.6.16 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
9035	1818.772358	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT_ACK
9036	1818.852914	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT
9037	1818.853159	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT_ACK
9038	1819.902980	192.168.0.2	192.168.0.1	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64
9039	1819.903089	192.168.0.1	192.168.0.2	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64
9040	1819.903186	Hewlett-_c9:ed:94	Hewlett-_d0:47:df	ARP	42	192.168.0.2 is at 00:23:7d:c9:ed:94
9041	1819.903285	Hewlett-_c9:ed:94	Hewlett-_d0:4f:b1	ARP	42	192.168.0.1 is at 00:23:7d:c9:ed:94
9042	1819.903500	192.168.0.1	192.168.0.2	ICMP	60	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=128
9043	1819.903752	192.168.0.2	192.168.0.1	ICMP	60	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=128
9044	1819.903757	192.168.0.2	192.168.0.1	ICMP	70	Destination unreachable (Protocol unreachable)
9045	1819.904133	192.168.0.1	192.168.0.2	ICMP	70	Destination unreachable (Protocol unreachable)
9046	1819.957447	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT
9047	1820.054375	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT
9048	1820.693993	192.168.0.1	239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1
9049	1821.158621	192.168.0.2	192.168.0.1	SCTP	86	HEARTBEAT
9050	1821.255314	192.168.0.1	192.168.0.2	SCTP	86	HEARTBEAT
9051	1821.903623	Hewlett-_c9:ed:94	Hewlett-_d0:47:df	ARP	42	192.168.0.2 is at 00:23:7d:c9:ed:94
9052	1821.903704	Hewlett-_c9:ed:94	Hewlett-_d0:4f:b1	ARP	42	192.168.0.1 is at 00:23:7d:c9:ed:94
9053	1822.562621	192.168.0.2	192.168.0.1	SCTP	60	ABORT
9054	1822.659356	192.168.0.1	192.168.0.2	SCTP	60	ABORT
9055	1823.657750	192.168.0.1	192.168.0.2	SCTP	82	INIT
9056	1823.704502	192.168.0.1	239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1
9057	1823.904050	Hewlett-_c9:ed:94	Hewlett-_d0:47:df	ARP	42	192.168.0.2 is at 00:23:7d:c9:ed:94
9058	1823.904129	Hewlett-_c9:ed:94	Hewlett-_d0:4f:b1	ARP	42	192.168.0.1 is at 00:23:7d:c9:ed:94
9059	1824.656298	192.168.0.1	192.168.0.2	SCTP	82	INIT
9060	1825.167884	fe80::750b:3a63:7776:	ff02::1:2	DHCPv6	166	Solicit XID: 0x49590d CID: 000100011537ed850025b3d04fb1
9061	1825.904462	Hewlett-_c9:ed:94	Hewlett-_d0:47:df	ARP	42	192.168.0.2 is at 00:23:7d:c9:ed:94
9062	1825.904542	Hewlett-_c9:ed:94	Hewlett-_d0:4f:b1	ARP	42	192.168.0.1 is at 00:23:7d:c9:ed:94
9063	1826.060201	192.168.0.1	192.168.0.2	SCTP	82	INIT
9064	1826.715339	192.168.0.1	239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1

```
▷ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▷ Ethernet II, Src: Hewlett-_d0:4f:b1 (00:25:b3:d0:4f:b1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)
```

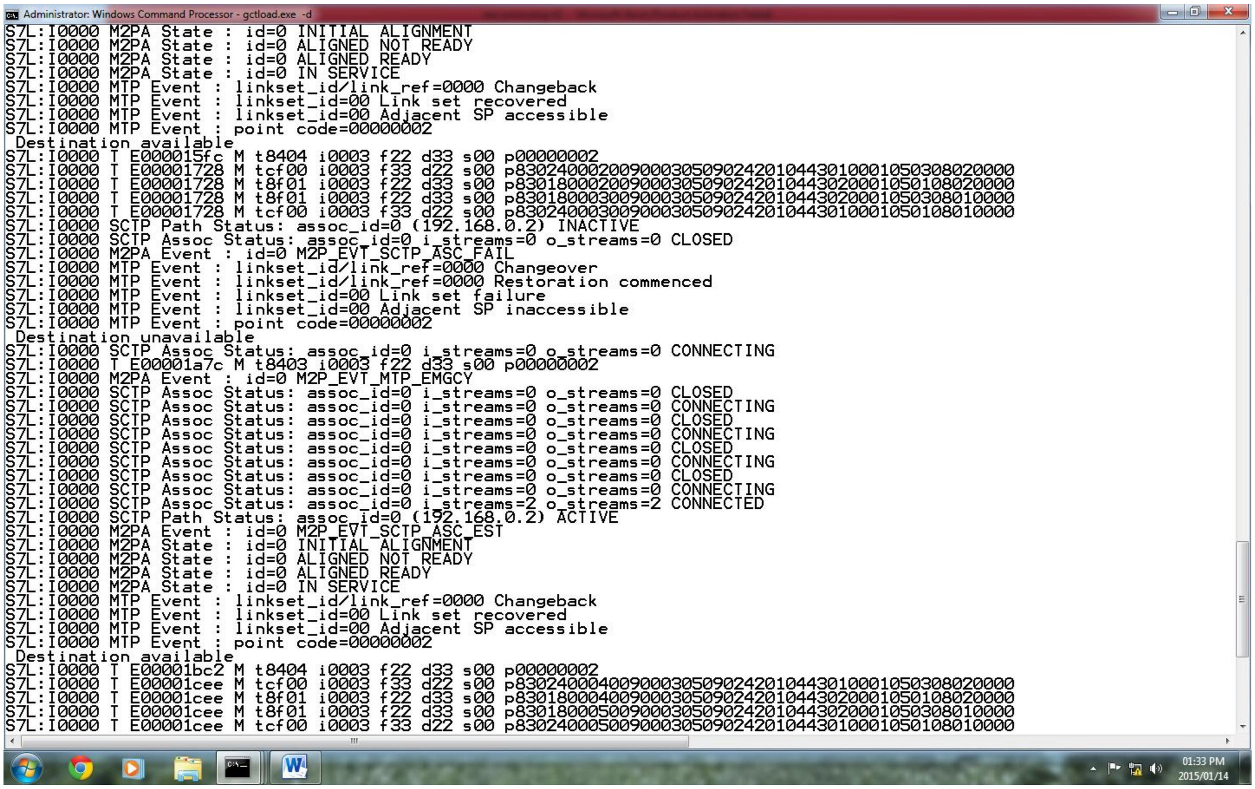
```
0000  ff ff ff ff ff ff 00 25  b3 d0 4f b1 08 06 00 01   .......% ..O.....
0010  08 00 06 04 00 01 00 25  b3 d0 4f b1 c0 a8 00 02   .......% ..O.....
0020  00 00 00 00 00 00 c0 a8  00 0a 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Frame (frame), 60 bytes   Packets: 9548 Displayed: 9548 Marked: 0   Profile: Default

Figure O.1: Wireshark Screenshot of Ettercap ARP Poisoning

Appendix P

MTU ARP Poisoning Screenshot



```
S7L:I0000 M2PA State : id=0 INITIAL ALIGNMENT
S7L:I0000 M2PA State : id=0 ALIGNED NOT READY
S7L:I0000 M2PA State : id=0 ALIGNED READY
S7L:I0000 M2PA State : id=0 IN SERVICE
S7L:I0000 MTP Event : linkset_id/link_ref=0000 Changeback
S7L:I0000 MTP Event : linkset_id=00 Link set recovered
S7L:I0000 MTP Event : linkset_id=00 Adjacent SP accessible
S7L:I0000 MTP Event : point code=00000002
 Destination available
S7L:I0000 T E000015fc M t8404 i0003 f22 d33 s00 p00000002
S7L:I0000 T E00001728 M tcf00 i0003 f33 d22 s00 p830240002009000305090242010443010001050308020000
S7L:I0000 T E00001728 M t8f01 i0003 f22 d33 s00 p830180002009000305090242010443020001050108020000
S7L:I0000 T E00001728 M t8f01 i0003 f22 d33 s00 p830180003009000305090242010443020001050308010000
S7L:I0000 T E00001728 M tcf00 i0003 f33 d22 s00 p830240003009000305090242010443010001050108010000
S7L:I0000 SCTP Path Status: assoc_id=0 (192.168.0.2) INACTIVE
S7L:I0000 SCTP Assoc Status: assoc_id=0 i_streams=0 o_streams=0 CLOSED
S7L:I0000 M2PA Event : id=0 M2P_EVT_SCTP_ASC_FAIL
S7L:I0000 MTP Event : linkset_id/link_ref=0000 Changeover
S7L:I0000 MTP Event : linkset_id/link_ref=0000 Restoration commenced
S7L:I0000 MTP Event : linkset_id=00 Link set failure
S7L:I0000 MTP Event : linkset_id=00 Adjacent SP inaccessible
S7L:I0000 MTP Event : point code=00000002
 Destination unavailable
S7L:I0000 SCTP Assoc Status: assoc_id=0 i_streams=0 o_streams=0 CONNECTING
S7L:I0000 T E00001a7c M t8403 i0003 f22 d33 s00 p00000002
S7L:I0000 M2PA Event : id=0 M2P_EVT_MTP_EMGCY
S7L:I0000 SCTP Assoc Status: assoc_id=0 i_streams=0 o_streams=0 CLOSED
S7L:I0000 SCTP Assoc Status: assoc_id=0 i_streams=0 o_streams=0 CONNECTING
S7L:I0000 SCTP Assoc Status: assoc_id=0 i_streams=0 o_streams=0 CLOSED
S7L:I0000 SCTP Assoc Status: assoc_id=0 i_streams=0 o_streams=0 CONNECTING
S7L:I0000 SCTP Assoc Status: assoc_id=0 i_streams=0 o_streams=0 CLOSED
S7L:I0000 SCTP Assoc Status: assoc_id=0 i_streams=0 o_streams=0 CONNECTING
S7L:I0000 SCTP Assoc Status: assoc_id=0 i_streams=0 o_streams=0 CLOSED
S7L:I0000 SCTP Assoc Status: assoc_id=0 i_streams=0 o_streams=0 CONNECTING
S7L:I0000 SCTP Assoc Status: assoc_id=0 i_streams=2 o_streams=2 CONNECTED
S7L:I0000 SCTP Path Status: assoc_id=0 (192.168.0.2) ACTIVE
S7L:I0000 M2PA Event : id=0 M2P_EVT_SCTP_ASC_EST
S7L:I0000 M2PA State : id=0 INITIAL ALIGNMENT
S7L:I0000 M2PA State : id=0 ALIGNED NOT READY
S7L:I0000 M2PA State : id=0 ALIGNED READY
S7L:I0000 M2PA State : id=0 IN SERVICE
S7L:I0000 MTP Event : linkset_id/link_ref=0000 Changeback
S7L:I0000 MTP Event : linkset_id=00 Link set recovered
S7L:I0000 MTP Event : linkset_id=00 Adjacent SP accessible
S7L:I0000 MTP Event : point code=00000002
 Destination available
S7L:I0000 T E00001bc2 M t8404 i0003 f22 d33 s00 p00000002
S7L:I0000 T E00001cee M tcf00 i0003 f33 d22 s00 p830240004009000305090242010443010001050308020000
S7L:I0000 T E00001cee M t8f01 i0003 f22 d33 s00 p830180004009000305090242010443020001050108020000
S7L:I0000 T E00001cee M t8f01 i0003 f22 d33 s00 p830180005009000305090242010443020001050308010000
S7L:I0000 T E00001cee M tcf00 i0003 f33 d22 s00 p830240005009000305090242010443010001050108010000
```

Figure P.1: MTU Dialogic Application Screenshot after ARP Poisoning