Master Thesis
Electrical Engineering
Thesis No: MEE10:76
Sep 2010

Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution

Nadeem Ahmad *(771102-5598)*

M. Kashif Habib *(800220-7010)*

School of Engineering
Department of Telecommunication
Blekinge Institute of Technology
SE - 371 79 Karlskrona
Sweden

This report is to be submitted to Department of Telecommunication Systems, at School of Electrical Engineering, Blekinge Institute of Technology, as a requisite to obtain degree in Master's of Electrical Engineering emphasis on Telecommunication/Internet System (session 2008-2010).

Contact information

Author(s):

- ***M. Kashif Habib***

  E-post: muhb08@student.bth.se, m_kashif_habib@hotmail.com

- ***Nadeem Ahmad***

  E-post: naah08@student.bth.se, nadeem.baloch@gmail.com

University Supervisor:

Karel De Vogeleer

E-post: karel.de.vogeleer@bth.se

University Examiner:

Professor Adrian Popescu

E-post: adrian.popescu@bth.se

School of Engineering
Blekinge Institute of Technology (BTH)
SE - 371 79 *Karlskrona, Sweden*

Internet : www.bth.se
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

Acknowledgement

In The Name of **ALLAH**, the Most Beneficial and Merciful. We are very thankful to all those who have helped us in giving us support throughout performing our thesis. First of all we would like to thank our university supervisor, who cultivated our mind with skills, providing us this opportunity to complete master degree thesis with complete support and guidance during entire period. His comments and proper feedback made us achieve this goal. We are both extraordinary thankful to our parents who had been praying during our degree studies and in hard times. Special thanks to Mikeal Åsman and Lena Magnusson for complete assistance in study throughout our master degree.

Kashif & Nadeem

Abstract

Communication of confidential data over the internet is becoming more frequent every day. Individuals and organizations are sending their confidential data electronically. It is also common that hackers target these networks. In current times, protecting the data, software and hardware from viruses is, now more than ever, a need and not just a concern. What you need to know about networks these days? How security is implemented to ensure a network? How is security managed? In this paper we will try to address the above questions and give an idea of where we are now standing with the security of the network.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

1.1 Motivation

"In this age of universal electronic connectivity when world is becoming a global village, different threats like viruses and hackers, eavesdropping and fraud, undeniably there is no time at which security does not matter.

Volatile growth in computer systems and networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This leads to a sharp awareness of the need to protect data and resources to disclosure, to guarantee the authenticity of data and messages, and protection of systems from network-based attacks". [1]

There are those who believe that security problems faced by home users are greatly overstated, and that the security only concerned about business computers that have significant data with them. And many believe that only broad band users or people with high speed connections need to be considered.

Truth is that majority of computer systems including business ones have not any threat about the data which they contains, rather these compromised systems are often used for practical purpose, such as to launch a DDOS attack in opposition to the other networks. [2]

Securing a network is a complicated job, historically only experienced and qualified experts can deal with it. However, as more and more people become agitated, there is a need of more lethargic people who can understand the basics of network security world.

Different levels of security are appropriate for different organizations. Organizations and individuals can ensure better security by using systematic approach that includes analysis, design, implementation and maintenance. The analysis phase requires that you thoroughly investigate your entire network, both software and hardware, from inside and outside. This helps to establish if there are or may be vulnerabilities. An analysis shows you a clear picture that what is in place today and what you may require for tomorrow. [3]

1.2 Goal/Aim

The main focus of this dissertation is to come up with a better understanding of network security applications and standards. Focus will be on applications and standards that are widely used and have been widely deployed.

1.3 Methodology

To achieve our goals we will investigate following parameters.

- ✓ Networks and protocols
- ✓ Security threats and vulnerabilities
- ✓ Security attacks
- ✓ Security countermeasures techniques and tools
- ✓ Security solutions
- ✓ Extracting results on the basis of simulations results.

Chapter 2

NETWORKS AND PROTOCOLS

In this chapter we will describe the basic concept of data communication network. The network layer protocols are the major part in a communication network. This chapter includes the description of the role of network layer protocols in a communication model; it also explains the functional parameters of these protocols in different level of data communication. These parameters are in the form of protocol header fields. We will study the header field of these protocols and analyze that how an attacker can use or change these protocol header fields to accomplish his/her malicious goals. The in-depth study of the structure of OSI layer protocols & TCP/IP layer protocols can carry out this objective.

2.1 Network

The network consists of collection of systems connected to each other through any communication channel. The communication channel may consist of any physical "wired" or logical "wireless" medium and of any electronic device known as node. Computers and printers are some of the examples of nodes in a computer network and if we talk about the telecommunication network these may be mobile phones, connecting towers equipment and main control units. The characteristic of a node in the network is that; it has its own identity in the form of its unique network identification.

The main functionality of any network is to divide resources among the nodes. The network under certain rules finds resources and then shares it between the nodes in such a way that authenticity and security issues are guaranteed.

The rules for communication among network nodes are the network protocols. A protocol is the complete set of rules governing the interaction between two systems [4]. It varies for varying different working assignments between nodes communication.

2.2 The Open System Interconnected Model (OSI)

In 1997, The International Standard Organization (ISO) designed a standard communication framework for heterogeneous systems in network. As per functionality of communication system in open world, this system is called Open System Interconnection Model (OSI). The OSI reference model provides a framework to break down complex inter-networks into such components that can more easily be understood and utilized [4]. The purpose of OSI is to allow any computer anywhere in the world to communicate with any other, as long as both follow the OSI standards [5].

The OSI reference model is exploited into seven levels. Every level in OSI Model has its own working functionality; these levels are isolated but on the other hand cascaded to each other and have communication functionality in a proper flow between them. With reference to above standard communication framework, this set of layers known as OSI layers. Functionality of each layer is different from each and each layer has different level and labels. (Shown in fig 2.1)

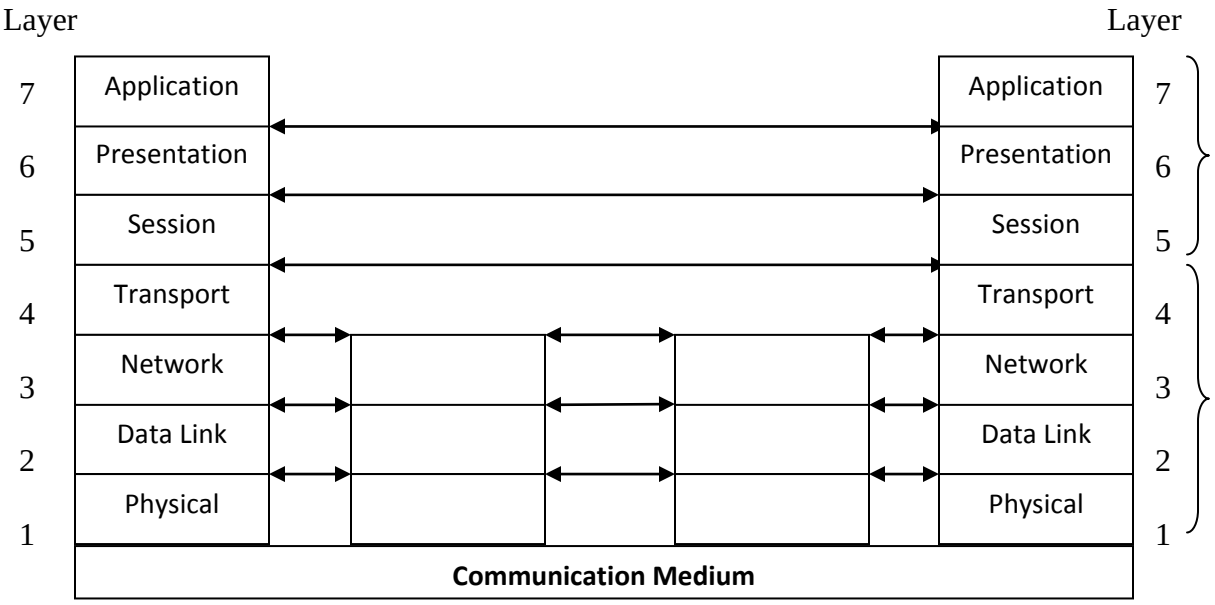

Fig 2.1: OSI Reference Model Layer Architecture

On the other hand if we see the system architecture of OSI, three level of abstraction is explicitly recognized; the architecture, the service specifications, and the protocols specifications (see fig 2.2) [5]. The OSI service specifications are responsible for specific services between user and system in a specific layer. Parallel OSI protocol specifications are responsible that, which type of protocol is running against the specific communication service. So it is clear that the combination of these two parts become OSI system architecture.

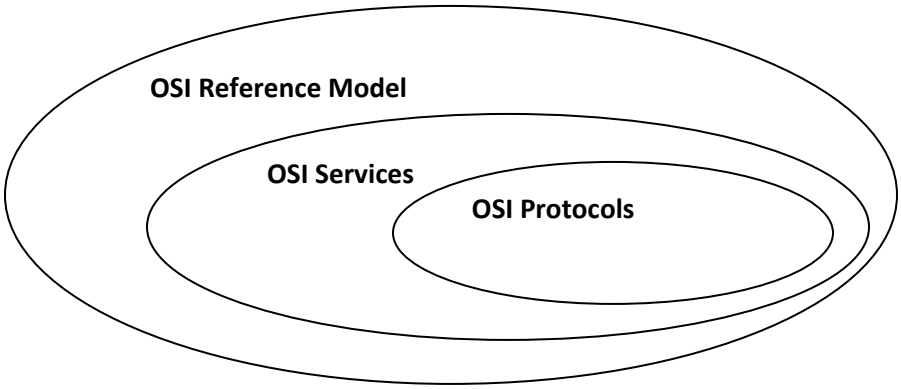

Fig 2.2: OSI System Architecture

It is patent that the OSI reference model consists of seven layers and each layer offers different functionalities, different services with different protocols. Whereas each layer, with the exception of the

lowest, covers a lower layer, effectively isolating them from higher layers functions.[6].Similarly the design principle of information hiding; the lower layer are concerned with greater level of details, upper layer are independent of these details. Within each layer, both services are provided to the next higher layer and the protocol to the peer layer in other system are provided [8] (see fig 2.3). Therefore we may say that as any change occurs in any layer-N, then it may effect only on its lowest layers-N-1. Due to isolation, the higher layers-N+1 is not affected or it can say that remaining reference model will not effect.

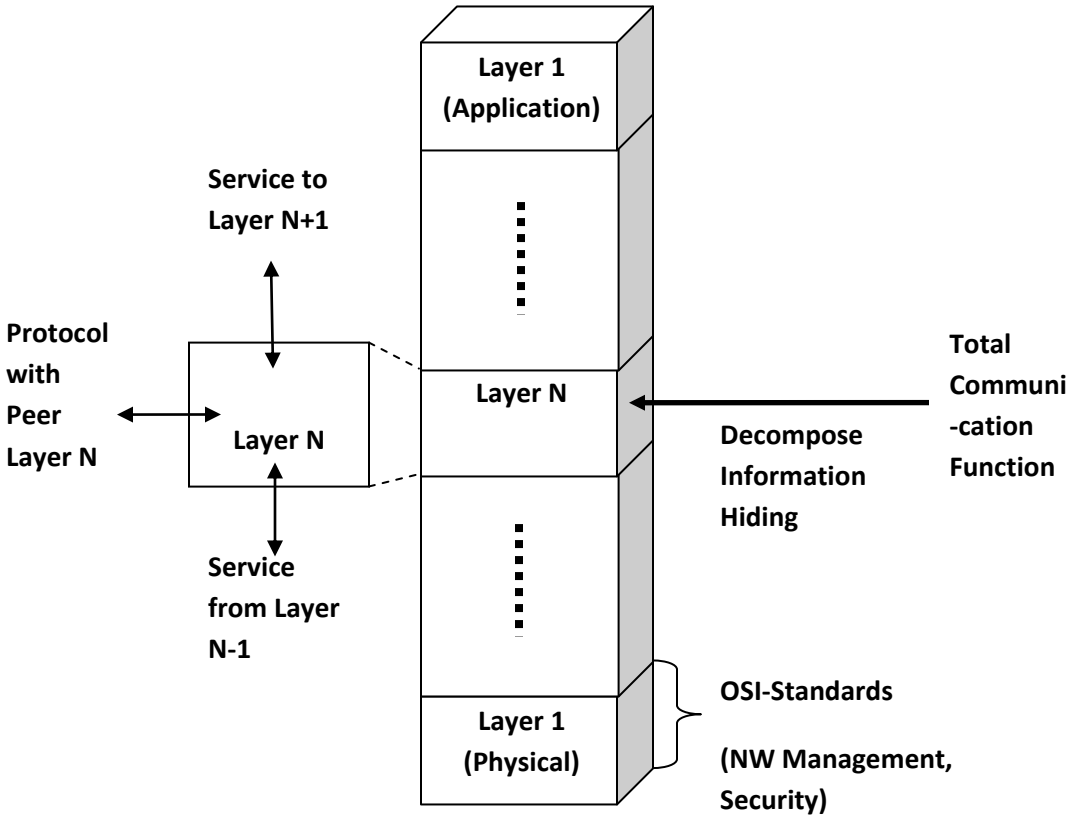

Fig 2.3: OSI Framework Architecture

Physical Layer

The lowest layer in OSI model is Physical Layer; it facilitates the connectivity between system interface cards and physical mediums. This layer understands and transforms electrical/electronic signals in the form of bits. So that it administrates physical *"wire"* and/or logical "*wireless"* connection establishment between the hardware interface cards and communication medium; example of physical layer standard includes RS-232, V.24 and V.35 interfaces [6].

Data Link Layer

In OSI Reference Model the Data Link Layer is the second layer**.** Data Link layer is responsible for control methods which provides proper format of data and it can access data flow errors in physical

layer. The data format in data link layer is in the form of frames. Therefore we say that the data link layer is responsible for defining data formats to include the entity by which information is transported. Error control procedures and other link control procedures may occur in physical layer [6]. Like cyclic redundancy check (CRC); the error checking mechanism that run at the time of transmission of a frame from source side. The same mechanism will run at the destination side if they found any difference after comparison then receiver makes a request to source to send that frame again.
Data link layer is responsible for following service [7].

- *Encapsulation*
- *Frame Synchronization*
- *Logical link control (LLC)*
    - *Error control*
    - *Flow control*
- *Media Access Control (MAC)*
    - *Collision Detection*
    - *Physical Addressing*

The data link layer is further subdivided into two layers, Logical link Control (LLC) and Media Access Control. The logical link control is responsible for flow control and error detection in data. Whereas media access control is responsible for controlling the traffic congestion and physical address reorganization.

Network Layer

The third layer in OSI Reference Model is the Network Layer. This layer is responsible to make a logical connection between source and destination. The data at this layer is in the form of packets. The network layer protocols provide the following services

Connection mode:

The network layer has two types of connection between source and destination, first one is known as connectionless communication which does not provide connection acknowledgement. The example of connectionless communication is Internet Protocol (IP). The second type of connection is connection-oriented which provides connection acknowledgement. TCP is an example of this connection.

IP Addressing:

In computer networks every node has its own unique ID. By this unique ID sender and receiver always make right connection. This is because of the functionality of network layer protocol, which has source address and destination address in their header fields. So there is less chance of packet loss, traffic congestion and broadcasting.

Transport Layer

The fourth layer in OSI reference model is Transport Layer. It contains two types of protocols, first is Transport Control Protocol (TCP) which is connection oriented protocol and supports some upper layer protocols like HTTP and SMTP. The second is User Datagram Protocol (UDP) which is a connection less protocol. Like TCP it also supports some upper layer protocols such as DNS, SNMP and FTP. The main thing in transport layer protocols is that they have port addresses in their header fields.

Session Layer

The fifth layer in OSI Reference Model is Session Layer. The Session Layer is responsible for session management i.e. start and end of sessions between end-user applications [7]. It is used in applications like live TV, video conferencing, VoIP etc, in which sender establishes multiple sessions with receiver before sending the data. Session Initiation protocols (SIP) is an example.

Presentation Layer

The sixth layer in OSI Reference Model is Presentation Layer. This layer is responsible for presentation of transmitted/received data in graphical mode. Data compression and decompression is the main functionality of this layer. The data encryption is done before transmission in presentation layer.

Application Layer

The seventh and the last layer of OSI Reference Model is Application Layer. This layer organizes all system level applications like FTP, E-mail services etc.

2.3 TCP/IP Protocol Suite

The TCP/IP Protocol Suite was developed before OSI reference model [9]. The OSI reference model consists of seven layers whereas TCP/IP protocol suite has only four layers (fig 2.4) [10]. In comparison to OSI reference model, TCP Suite has high level of communication traffic awareness between sources to destination. The TCP/IP Suite has administrative communication controlled and reliable data processing. It has dozens of layer components and communication set of rules which provide reliable service performance and data security [11].

Each layer in TCP/IP suite is responsible for a specific communication service and all these layers are cascaded and support each other (fig 2.5) [11]. The main protocols of this suite are TCP and UDP, which exist in transport layer. TCP is an acknowledgeable protocol that provides reliability in data transmission while UDP is non acknowledgeable protocol and is used in data streaming services like video conferencing, VOIP, etc.

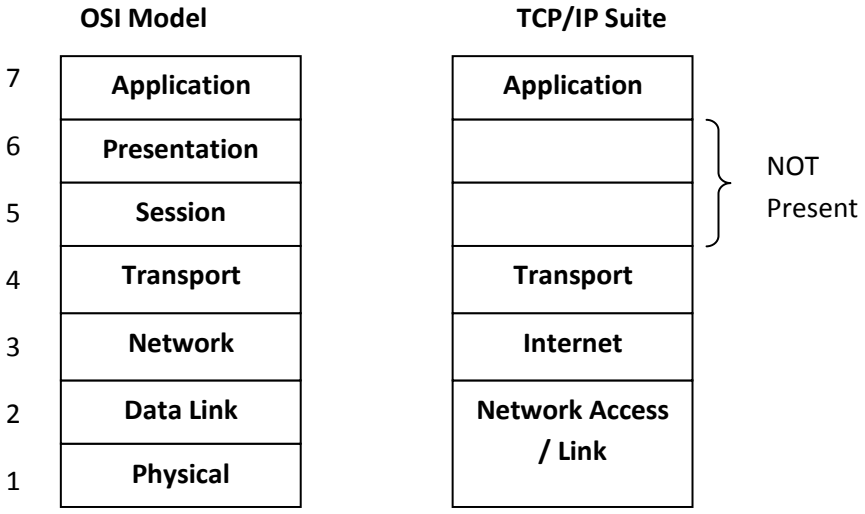

Fig 2.4: Layer difference between OSI and TCP/IP Suite

The layer structure of TCP/IP suite is similar to OSI Model. In TCP/IP Suite the Link Layer covers the last two layers (physical and data link layer) of OSI model. Presentation and Session Layers of OSI model

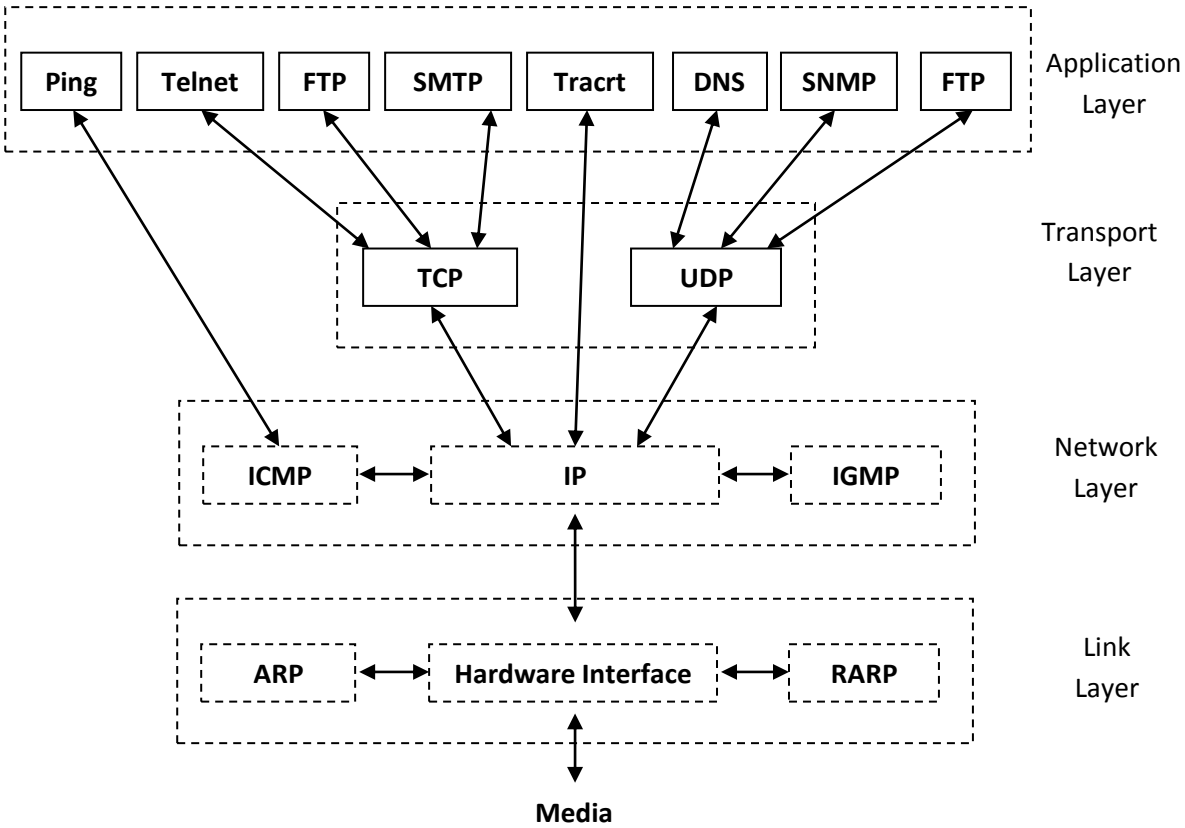

Fig 2.5: Different Layers Protocols in TCP/IP suite

do not exist in TCP/IP protocol suite. [12]

2.3.1 Link Layer

This layer is also known as data link layer or network interface layer. Link layer interfaces the network interface card and the communication medium. The important role of link layer is address resolution that provides mapping between two different forms of addresses with ARP and RARP protocols (see fig 2.6) [11]. For proper functionality; it has complete information of network interface cards, i.e. driver details and kernel information. It interprets between two systems in network for the sake of information of source address and destination address from software address to hardware address to send information on physical medium, because the kernel only recognizes the hardware address of network interface cards not the IP address or Physical address. Address resolution Protocols (ARP) translates an IP Address to a Hardware Address whereas Reverse Address Resolution Protocol (RARP) converts a hardware address to IP Address [6]. (See fig 2.6)

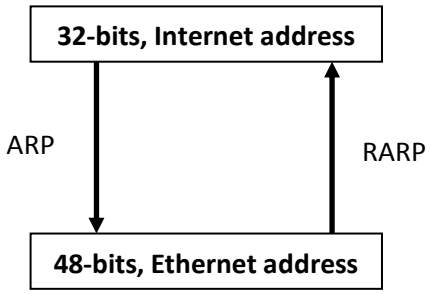

Fig 2.6: Resolution Protocols Working Scenarios

2.3.1.1 Address Resolution Protocol

The interpretation of data transmitted to communication medium from network layer depends on ARP and RARP link layer protocols. Network layer has source and destination address which is also called the logical address or 32-bits of IP Address, but before sending the information on a network via communication medium it is required to change this address IP address into 48-bits of hardware address which is also called Ethernet address or MAC Address. The reason for changing the address is that, the communication medium is directly connected to the Ethernet interface cards and it may assess the data via serial communication lines [6].

ARP operation; a network device during transmission in a communication medium performs sequence of operations [11]. Packet format of ARP is also clarified this (fig 2.7) [6].

- *ARP request: A broadcast request in the form of Ethernet frames for the whole network. Request is basically a query for getting a hardware address against an appropriate IP.*
- *ARP reply: Appropriate hardware address generates a send back rep; response to sender against its query, in the form of its hardware address with its IP address.*
- *Exchange: request-reply information.*

- *Send: IP datagram to destination host.*

In Data link layer, Ethernet and Token ring have the same hardware length, as well if it sends a query request then operation has 1 notation and in query response that has changed to in notation of 2.

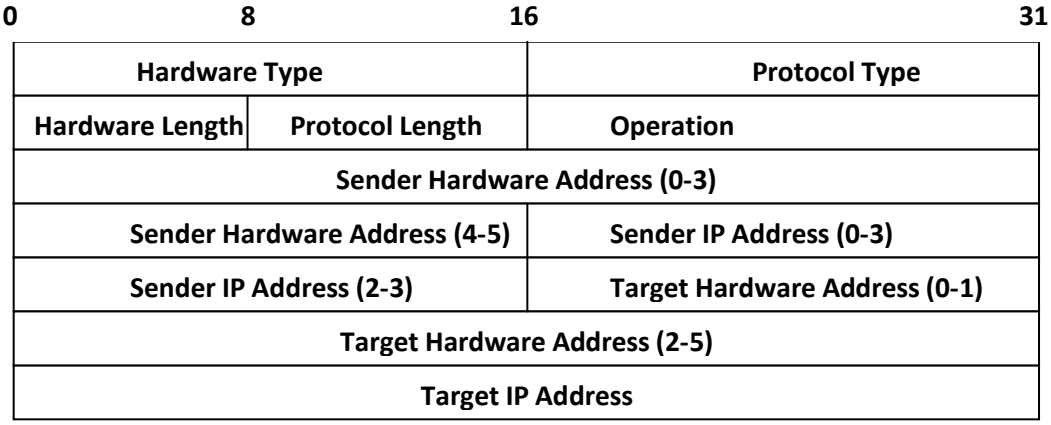

Fig 2.7: ARP Packet

2.3.1.2 Reverse Address Resolution Protocol

RARP packet format and operation is similar to ARP operation but has reverse working functionality. RARP generates a query for IP address against appropriate MAC address. This design is for diskless workstation which has a big usage in corporate environment [11]. In this scenario the diskless workstation can get their IP address from server against their specific hardware addresses.

2.3.2 Internet Layer

The second layer of TCP/IP suite protocol structure is Internet or network layer. It generates a service request to Data Link layer protocol and provides services against Transport layer application request.
The role of internet layer protocol (IP) is very important in internetworking data transmission and in receiving prospects; datagram delivery is the main task of this layer. (Fig 2.8)

2.3.2.1 Internet protocol

Internet protocol is an important protocol of the internet layer as well for the whole internetworking communication. The protocol structure of internet layer is IP datagram and each IP datagram consists of the source IP address and destination IP address which is of 32-bit physical address. [11]. Consider the layer traffic scenario; it receives UDP/TCP segment request form transport layer and add some layer information tags as a prefix and convert it into IP datagram [6]. That is concerned with the exact datagram delivery in the form of source and destination IP address. Figure 2.9 shows the whole datagram packet.

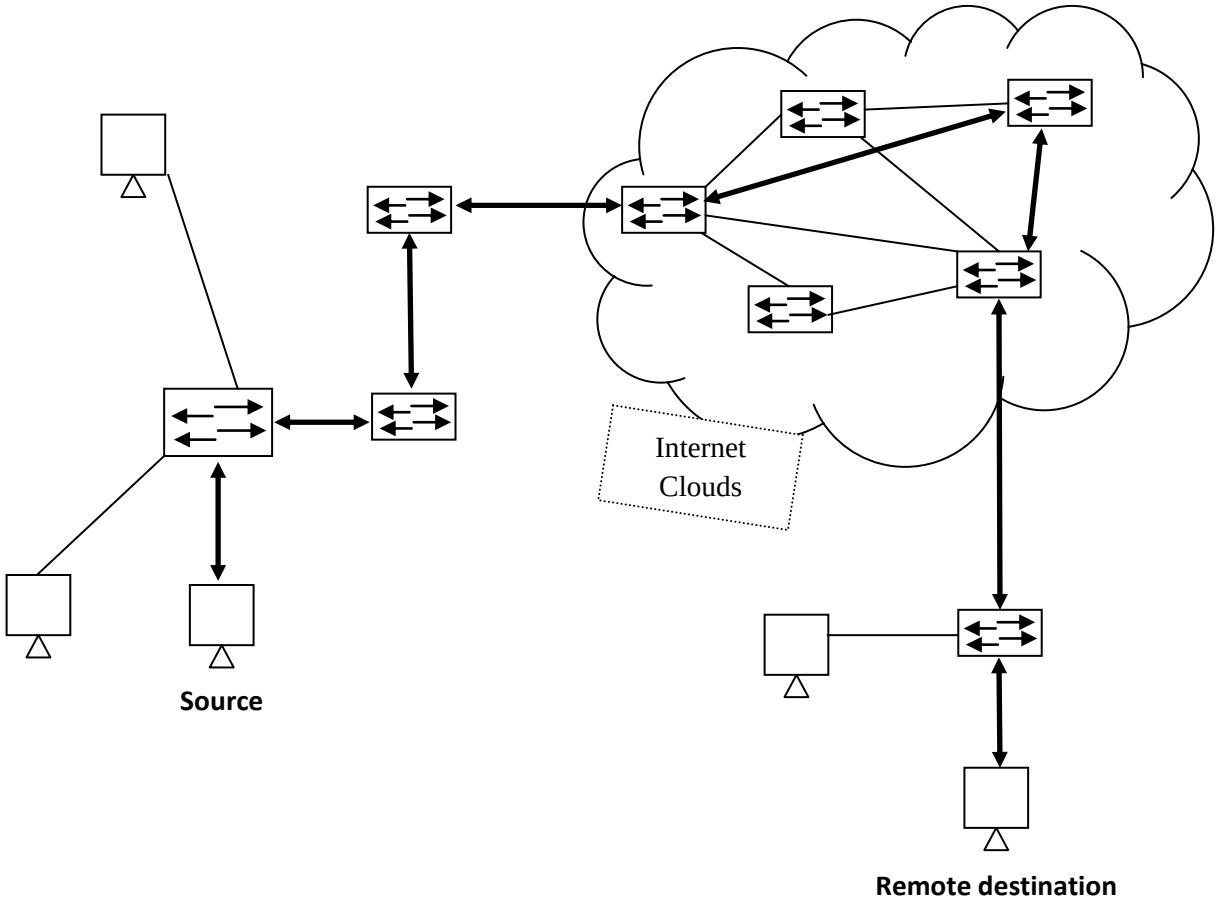

Fig 2.8: IP Datagram Delivery

The "*version"* notifies the current IP version that exists in IP datagram; either it is version 4 or 6. The "*type of service"* indicates multiple services like delay, throughput and cost etc. *"Time to live"* is a

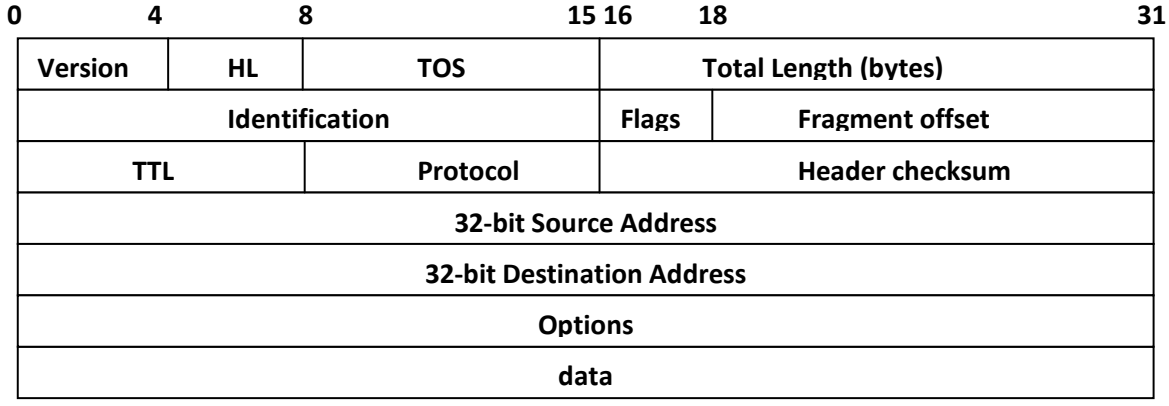

Fig 2.9: IP Datagram

countdown counter that gradually down to zero. Two conditions exists here, either packet successfully reached to its destination or discarded before TTL reached to zero. If TTL counter reaches to 0 IP packet discarded from the network. The main advantage of TTL is that it overcomes the network traffic congestion issue. *"Flags"* contain 3 bit length as shown in IP datagram figure; they play an important role in successfully transmission of data packet at destination end.

The 32-bit *"source address"* and *"destination address"* are the physical addresses of source and destination. These fields perform an efficient role to hitch-hike of IP traffic on network. A hacker can exploit the IP datagram by make some changes in it when the packet is traveling in communication medium in the form of hex code. Hacker can do this with the help of any network sniffing application or by use of TCP-dump and mapping application.

By using TCP-dump, malicious hacker can see the IP header datagram information and then can change the values by his/her malicious mind. Let's take an example [13]

Examine the IP traffic with TCP-dump application gives all necessary information which could help in malicious act. This is the output of TCP-dump and it is in Hex-code for better understanding we may change it into binary and decimal code. From the figure 2.10 the information we can get; IP version (either 4 or 6), total length of IP packet, TTL of the packet, type of protocol either TCP or UDP, source and destination address.

4500 00b2 4ea6 2000 8006 ee3f c0a8 4803 c0a8 4804

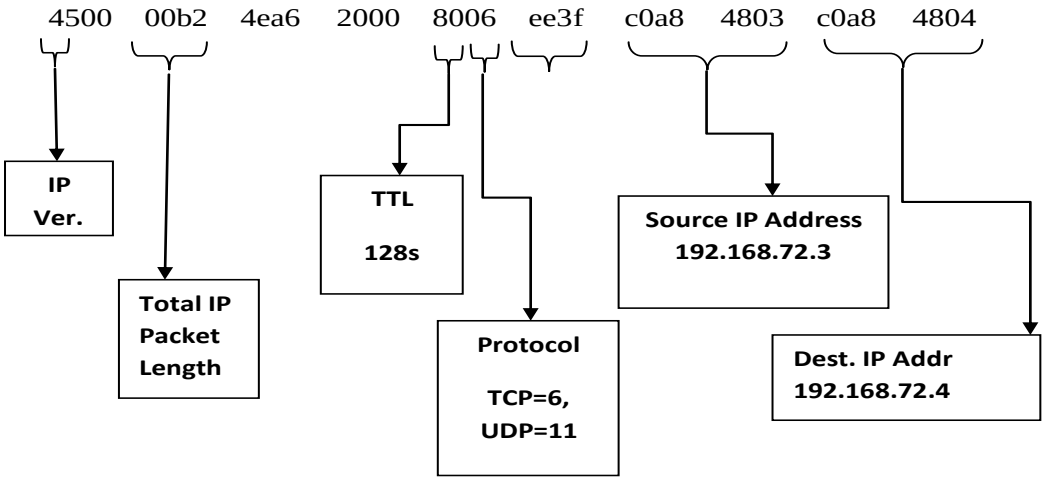

Fig 2.10: TCP dump Output of IP Datagram

2.3.2.2 ICMP Protocol

Some more and popular protocols in network layer of TCP/IP protocol suite are Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP). These protocols worked together with the IP datagram protocol for their own working purpose. Therefore we can say that IP Protocol or its header used as a carrier for ICMP and IGMP protocols communication (fig 2.11) [6].

Timestamp request and timestamp reply are the examples of ICMP which are similar to echo request and echo reply. Additionally it provides sender timestamp request and receiver timestamp reply and difference is known as Round Trip Time (RTT) which is in milliseconds.
Exploiting this protocol is important for hackers because by changing or modifying in field he/she can easily divert the network traffic.

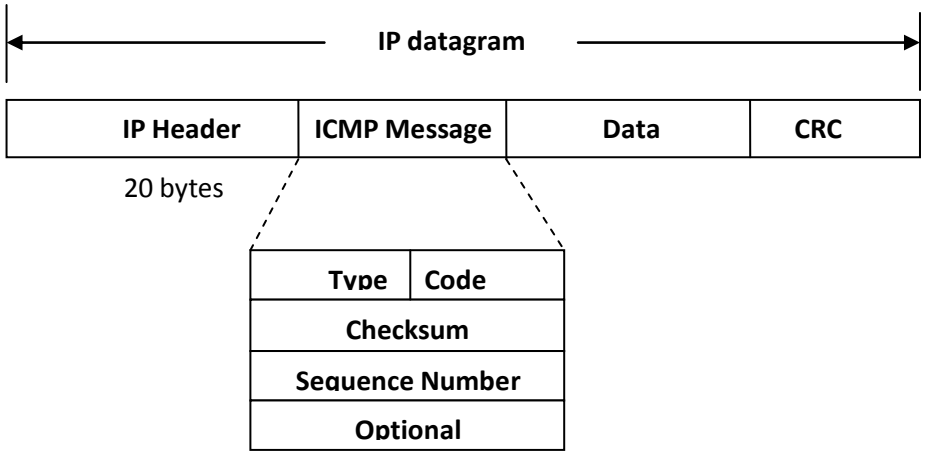

Fig 2.11: ICMP message encapsulation with IP datagram

Echo request and echo reply are the functions of ICMP. With the help of ping command we can judge that our destination host is alive or not alive in the network, administrators used this for analyze the traffic. Some other ICMP types are expressed in the table below (Table. II.I) [11].

TABLE II.I: ICMP Message Types

Type	***Code***	***Description***	***Query***	***Error***
0	*0*	Echo reply	*	
3		Destination unreachable:		*
	0	*Network unreachable*		*
	1	*Host unreachable*		*
	2	*Protocol unreachable*		*
	3	*Port unreachable*		*
	5	*Source route failed*		*
	6	*Destination network unknown*		*
	7	*Destination host unknown*		*
4	*0*	Source quench (elementary flow control)		*
5		Redirect		*
8	*0*	Echo request (ping request)	*	
11		Time exceeded:		
	0	*Time to live equals 0 during transit (traceroute)*		*
	1	*Time to live equals 0 during reassembly*		*
12		Parameter problem:		
	0	*IP header bad*		*
	1	*Required option is missing*		*
13	*0*	Timestamp request	*	
14	*0*	Timestamp reply	*	

2.3.2.3 IGMP Protocol:

Internet Group Management Protocol (IGMP) looks like internet Control Message Protocol. It exists in Internet layer in TCP/IP protocol suite. ICMP datagram also encapsulates with IP datagram for communication in a network. It supports multicasting concept between a group of hosts and between multicasting supported routers, in a physical network, which is against broadcasting. For the working of

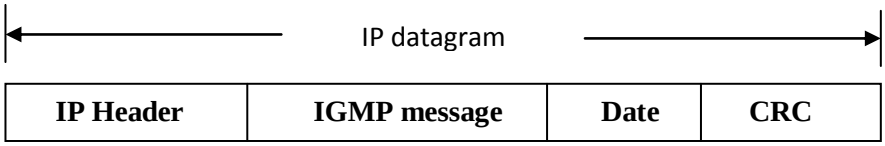

Fig 2.12: ICMP Message Encapsulation with IP Datagram

multicasting, it provides the familiarities, how a class D and IP address are mapped with the hardware or Ethernet address [11].

By using net state query with some of its parameters we can get multicasting report or routing tables of our own system which is associated with hardware interface like netstat –nr

Route Table
===
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 1a 73 c4 18 02 ..... Broadcom 802.11b/g WLAN - Packet Scheduler Miniport
0x3 ...00 1b 38 8d af bb ..... Intel(R) PRO/100 VE Network Connection - PacketScheduler Miniport
0x10005 ...00 15 83 16 c0 22 ..... Bluetooth Device (Personal Area Network) #2
===
===
Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	194.47.156.1	194.47.156.108	25
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
194.47.156.0	255.255.255.0	194.47.156.108	194.47.156.108	25
194.47.156.108	255.255.255.255	127.0.0.1	127.0.0.1	25
194.47.156.255	255.255.255.255	194.47.156.108	194.47.156.108	25
224.0.0.0	240.0.0.0	194.47.156.108	194.47.156.108	25
255.255.255.255	255.255.255.255	194.47.156.108	194.47.156.108	1
255.255.255.255	255.255.255.255	194.47.156.108	3	1
255.255.255.255	255.255.255.255	194.47.156.108	10005	1

Default Gateway: 194.47.156.1
===

naah08@sweet: netstat -nr
Kernel IP routing table

Destination	*Gateway*	*Genmask*	*Flags*	*MSS*	*Window*	*irtt*	*Iface*
194.47.153.0	*0.0.0.0*	*255.255.255.0*	*U*	*0*	*0*	*0*	*eth0*
0.0.0.0	*194.47.153.2*	*0.0.0.0*	*UG*	*0*	*0*	*0*	*eth0*

Microsoft Operating system is used in first output and in second Linux operating system is used. The output expression is little bit different.

Security Level Protocols

2.3.2.4 IPSec Protocol

IPSec is an internet layer protocol which provides security at internet layer. The key principle of IPSec on internet layer is that, it provides the security to individual users at transparent level. It provides the data access authentication as well as data encryption on the same level.
IPSec covers three areas of security level, data encryption, traffic authentication and key management [14].

2.3.2.4.1 Protocol Identifier

The IPSec protocol has classified into two sub-level protocols on the basis of their different working algorithms [11].

- Authentication Header (AH)
- Encapsulation Security Payload (ESP)

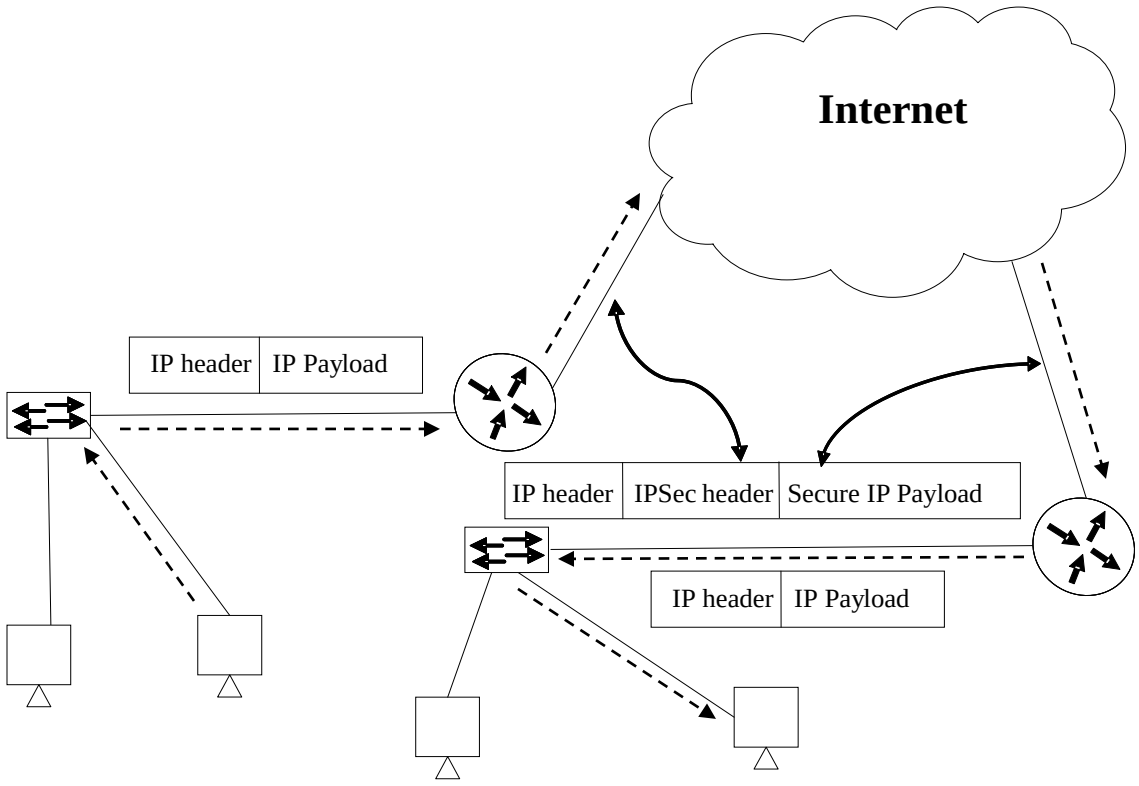

Fig 2.13: IPSec Packet flow Scenario

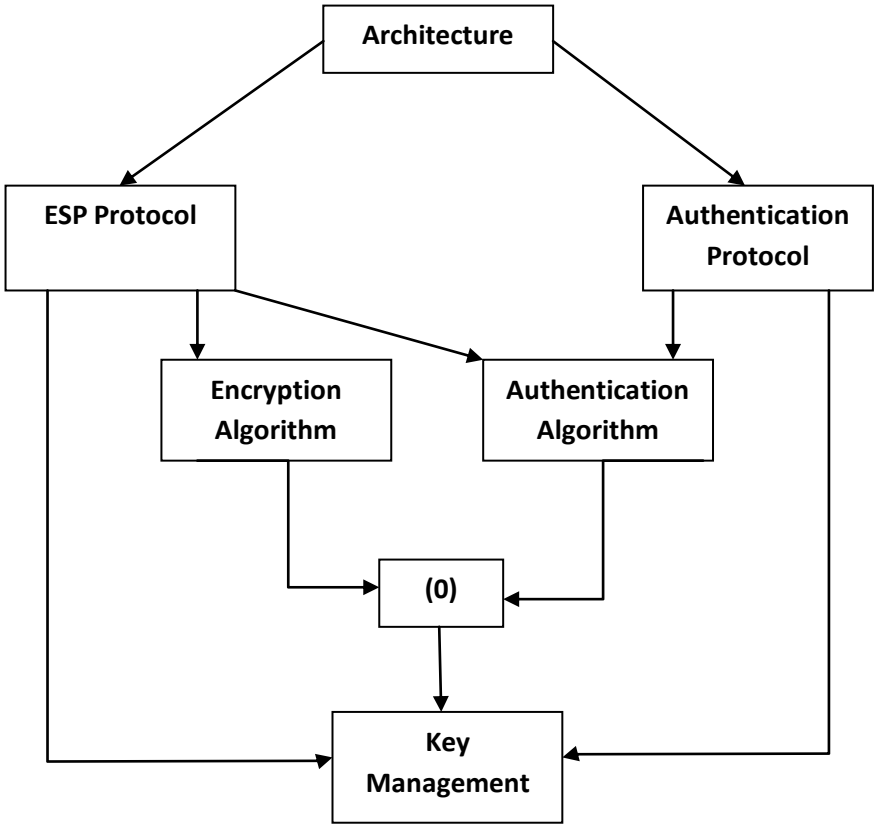

Fig 2.14: IPSec Architecture data flow

The authentication header has massage authentication block in its header field for authentication of massage, whereas encapsulation security payload has one more block of data encryption with massage authentication. Its mean that ESP protocol has one more feature of encrypt the data with authentication. However both of IPSec protocols are used in the IP level security. Above figure 2.14 shows the security level architecture model.

2.3.2.4.2 Mode of Operations

There are two modes used in IPSec for secure data transmission [15].

- Tunnel Mode
- Transfer Mode

In "*Transfer mode"* first it provides the protection of existing upper layer protocols (tcp/udp) then provides the protection of existing IP payload (data). That is why ESP in transfer mode only encrypts and authenticates the IP data but does not protect the current IP header. Same as for AH protocol which provides the IP data or IP payload authentication and some selected part of IP header. But in "*Tunnel mode"* first it provides the protection to the existing IP packet then entertain the AH or ESP field in the IP packet. So ESP encrypts and authenticates the existing IP packet and then IP header in tunnel mode, same as for AH protocol which authenticate IP packet and then selected portion of IP header in tunnel mode[14]. (See fig 2.15)

There is another view expressed that is clear in diagram (fig 2.16) [14]. The dark color shows the old condition whereas white shows the current operation on appropriate protocol level.

Before AH & ESP

Org. IP header	TCP/IP header	Data (IP Payload)

AH in Transport Mode

Org. IP header	AH	TCP/IP header	Data(IP Paylod)

(Payload)

AH in Tunnel Mode

New IP header	AH	Org. IP header	TCP/IP header	Data (Payload)

ESP in Transport Mode

Org. IP header	ESP header	TCP/IP header	Data	ESP trailer	ESP auth.

ESP in Tunnel Mode

New IP header	Org. IP header	ESP header	TCP/IP header	Data	ESP trailer	ESP auth

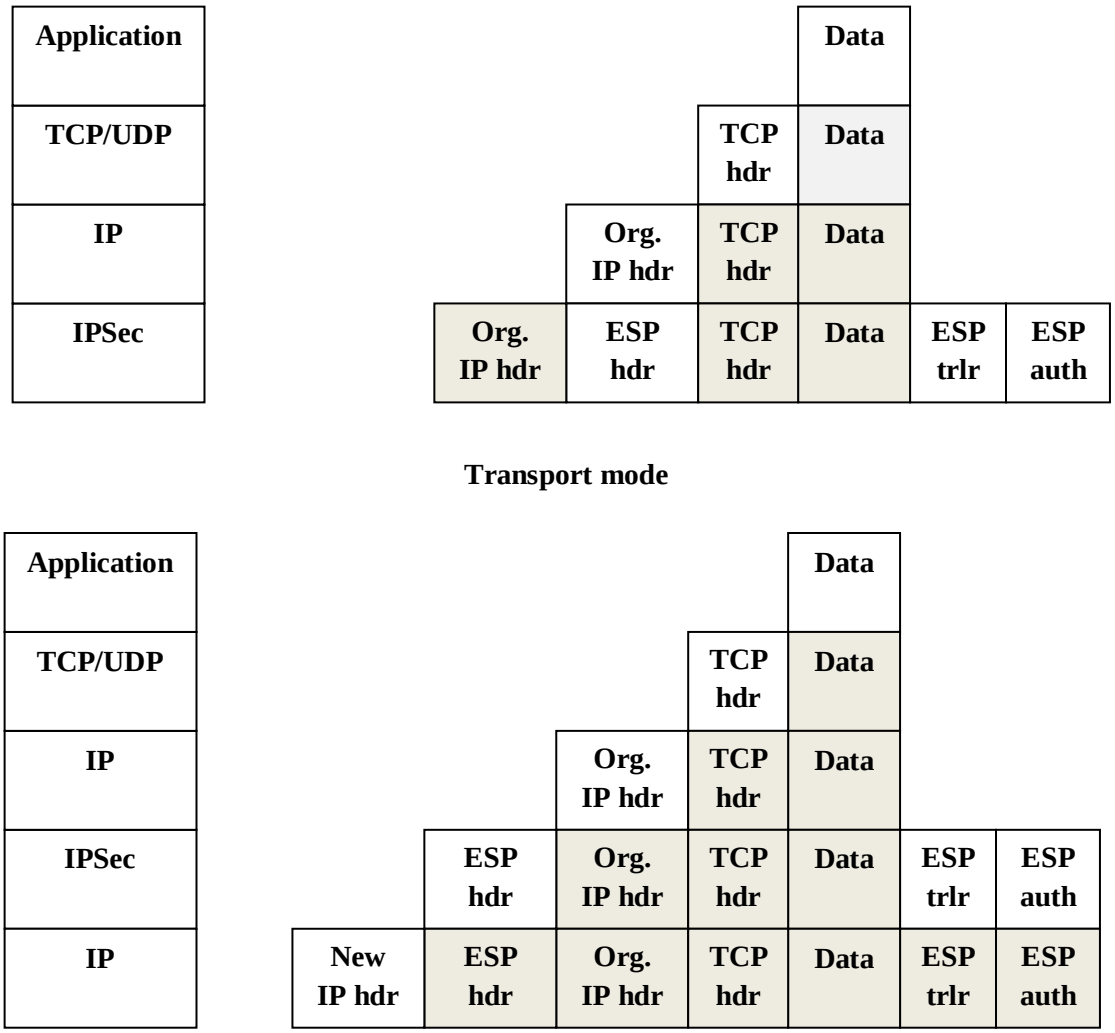

Fig 2.16: ESP Protocol Operation in Different Modes

2.3.3 Transport Layer Protocol

Transport layer is the third layer in TCP/IP protocol suite which consists of two protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Different functionalities of these protocols comes up with different architectural models or headers. The main feature of Transport layer protocol is, introducing a new protocol header that was not present in lower layer protocols, that is a port concept. Working with Internet Protocol features; IP address and port function from transport layer protocol, against a specific services or application run on server that we get “socket” concept [16].

2.3.3.1 TCP Protocol

The Transmission Control Protocol (TCP) removes the existing drawbacks in internet protocol (IP); TCP makes connection before sending the data to destination that is why known as connection oriented protocol. Connection oriented functionality provides the reliable data transmission in communication. Similarly TCP notifies and remove errors with the help of error detection function which detects the errors during transmission. Acknowledgement from receiver shows that packet is successfully delivered to the destination that is why we say that TCP is a reliable protocol. If sender receives acknowledgement with error packet then sender sends again error-less packet toward receiver. Below is the figure showing some more features of TCP Protocol (fig 2.17) [6].

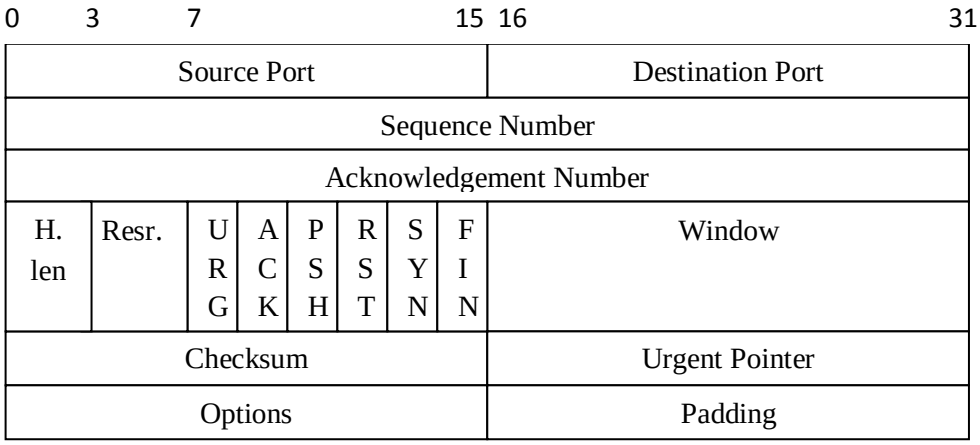

Fig 2.17: TCP Header

Source and Destination Port:

TCP protocol provides the source and destination services port. There are many applications, services and system processes that are associated with unique ports. By allocating specific ports with specific services on server end administrators can allow/deny system services to specific client or group of clients, i.e. web services.

Sequence and Acknowledgement Number:

The error detection is done by sequence number and acknowledgement number. The sequence number controls the sequence of sent packets, if sender receives any acknowledgment with error-packet then sender once again send error-less packet so that maintain the exact sequence number of the packet.

Code bits or flag indication:

There are six different flags indicator in TCP header which identifies different functions in TCP packet. Following are six flags [6].

1) URG Bit: This flag indicates the urgent data request; it assigns higher priority to urgent packets.

2) ACK Bit: This flag indicates that the datagram has an acknowledgement of previous packet or that the datagram contain some specific acknowledgement number value.

3) PSH Bit: This flag indicates push bit. It work against with URG bit.

4) RST Bit: RST bit indicates reset request for connection from sender to receiver.

5) SYN Bit: Synchronization of sequence numbers of TCP packet.

6) FIN Bit: It is a notification shows that sender wants to stop the data.

7) Checksum: The checksum field in TCP header provides error detection in TCP packets. In prospective of network security. The above fields in TCP header are very important for any hacker. They can use these flags to achieve their malicious goal.

2.3.3.2 UDP Protocol

Second protocol of transport layer is User Datagram Protocol (UDP). UDP is a connection less protocol i.e., it does not establish a connection between sender and receiver before sending the data. Many applications which does not require connection establishment before transmission uses UDP examples of applications are Mobile TV, VoIP etc.
As compared to TCP header UDP has very simple header as shown in Fig 2.18. UDP does not provide reliability of data [11] because of no acknowledgement flag. But infect UDP is faster than TCP and in some applications speed is more important than reliability like in VoIP Applications. However source port, destination port and checksum fields have same functionality as in TCP header which we have already described above.

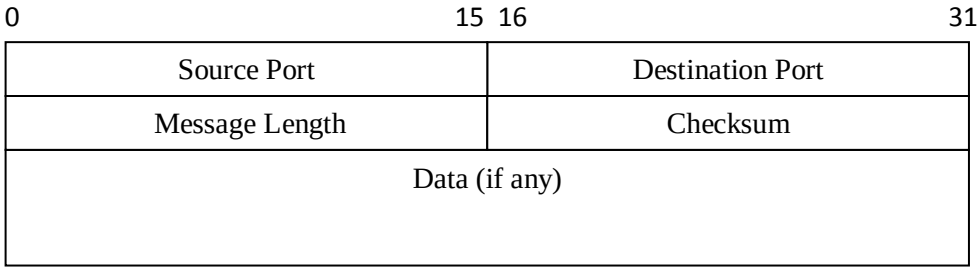

Fig 2.18: UDP Header

Security Level Protocols

There are some protocols which provide security at transport layer. Protocols are:

- Secure Socket Layer (SSL)
- Transport Layer Security (TLS)
- Secure Shell (SSH)

All above security protocols work on transport layer. Secure Shell (SSH) is a protocol that provides secure network communication channel at transport layer [14]. It is used in sever-client connection environment. Initially user authentication is done at both ends similar like in TCP communication where three-way handshake connection is establish before data transmission, then SSH makes a secure tunnel between server and client before communication starts. In SSH, the connection established on the base of SSH user and server authentication after this it provides a communication tunnel for data transmission (fig 2.19).

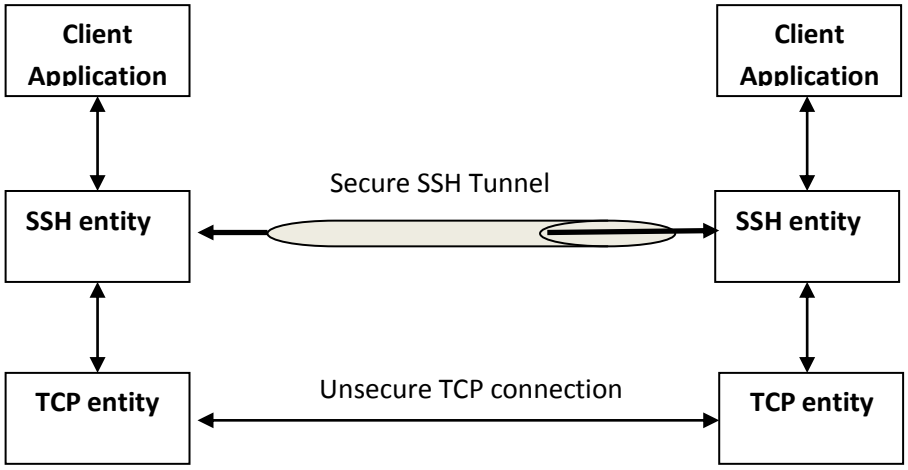

Fig 2.19: TCP Connection via SSH Tunnel

Similarly SSL and TLS provide security to web applications at transport level. (fig 2.20) [14].

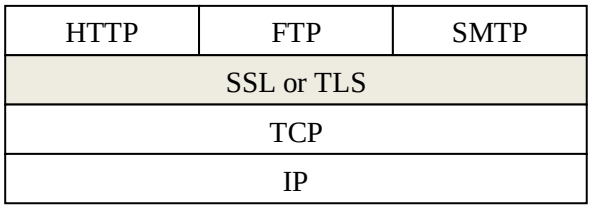

Fig 2.20: Transport Level Web Security

2.3.4 Application Layer Protocol

Application layer consist of applications and processes that works above the transport layer. These applications and processes do work by using the network or remaining lower layer protocols between two or more host in a network as an application-to-application or process-to-process communication level [17].
It is clear that all application level protocols communicate on network through transport and internet level protocols (see fig 2.5).

The applications on application layer which uses TCP protocols for communication in a network known as “Stream” applications on the other hand the application on application layer which uses UDP protocol known as “Message” applications and regarding these on transport layer “Segment” and “Packet” simultaneously.(fig 2.21)[18].

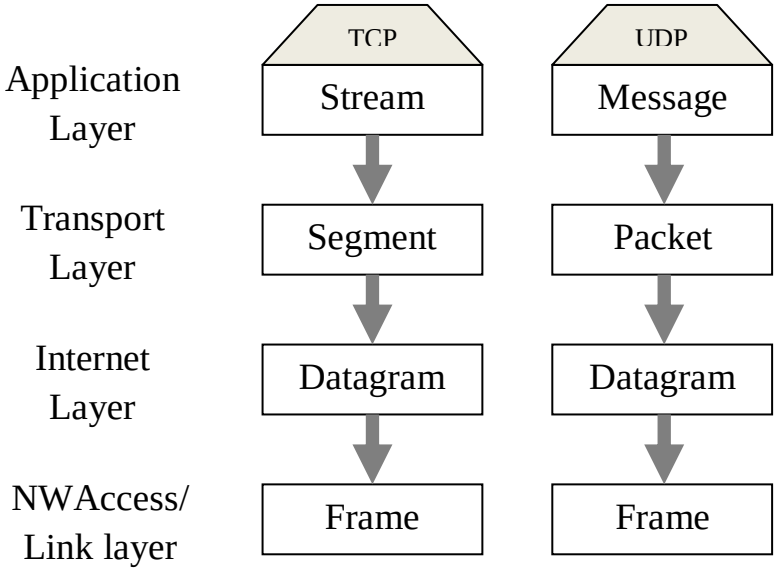

Fig 2.21: Data Format in Application Layer

There are number of protocols at application layer we will discuss some of them regarding our project prospective, detail of these protocols will explain in next chapters.

2.3.4.1 SMTP Protocol

Electronic mail (e-mail) used almost everywhere in the world for communication of data in simple readable text or in GUI mode worked on application layer. The protocol used for Email is Simple Mail Transport Protocol (SMTP). This application protocol is laying on TCP protocol. Figure 2.22 shows the architecture of SMTP [11].

Mail transfer agent is responsible for transferring the e-mail messages from one system to another system on a local area network, but if email is delivered on wide area network then this agent is known as relay mail transfer agent. Similarly a user agent is responsible to send and receive electronic mail from mail-server to mail-client, i.e. Microsoft outlook express, Windows live mail etc [19].

2.3.4.2 FTP Protocol:

The protocol which is used for transferring the file form source to destination is called File Transfer Protocol (FTP). FTP transfers the file securely from source to destination across the local area network or wide area network. Before sending the data FTP makes secure connection between server and client on the basis of user authentication. Another feature of FTP protocol is that, it establishes dual TCP

connections between server and client. One connection is for user authentication and second for data

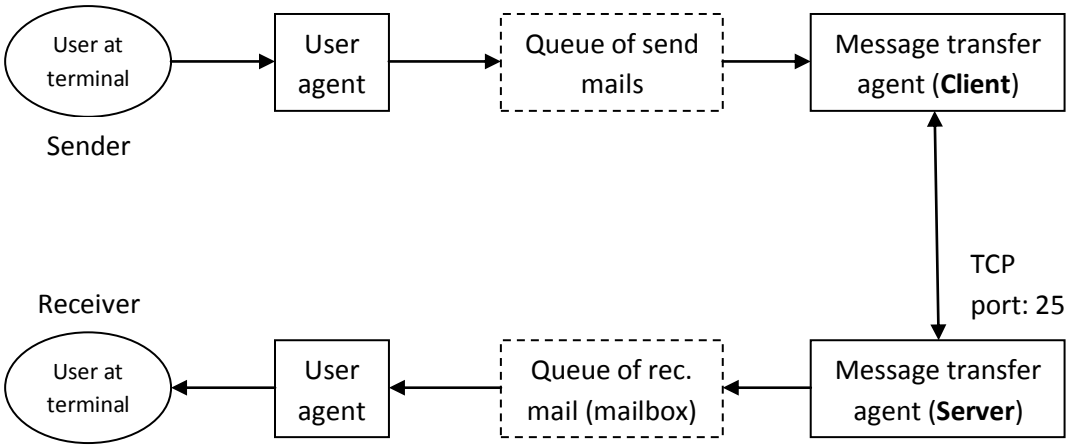

Fig 2.22: Flow Structure in Internet Electronic-Mail

transmission which provides reliable data transmission with authentication (See fig 2.23) [11].

Security Level Protocols

2.3.4.3 Telnet

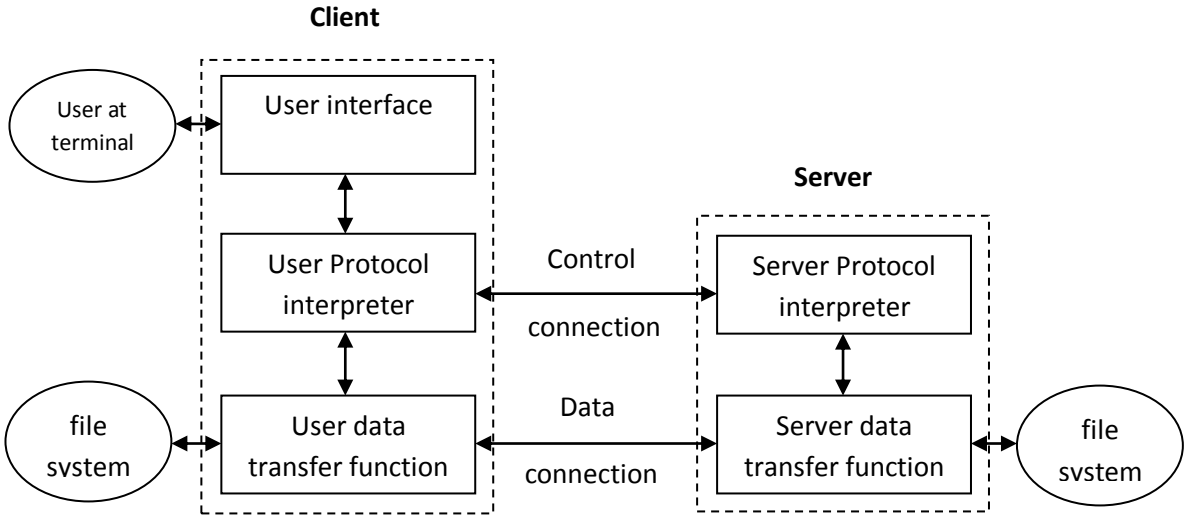

Fig 2.23: FTP Connection Process

Telnet is another famous application in prospective of network connection between two network hosts. Actually the telnet provides connection between a network host and any other network device. So we can say that it establishes a hardwired terminal connection from host to any other network device. Similarly in ftp connection it makes secure connection on the basis of host authentication on network

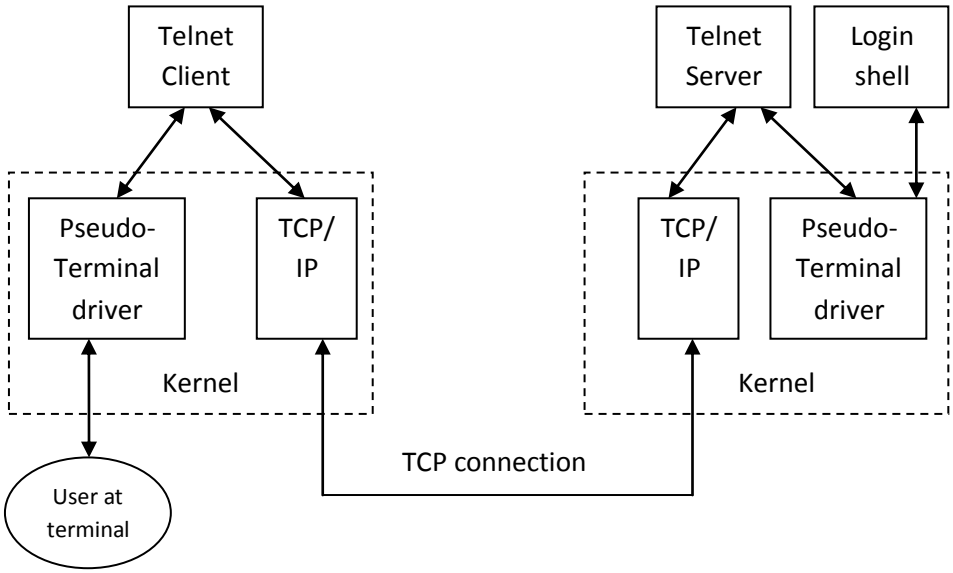

Fig 2.24: Telnet Connection Structure

device or any other different operating system [11] that is why we say that telnet is an application level security protocol.

Chapter 3

NETWORK SECURITY THREATS AND VULNERABILITIES

Network Security

When we talk about security, the first step is that how we define network security. If you ask from 10 different administrators about the definition of network security, you will probably get 10 different answers. However as its name suggest network security is the protection of networks, their applications or services against unauthorized access that prevents form modification, disclosure or destruction of data. It also assures that the network is performing correctly with no harmful side effects. [20] .This is admittedly, a very broad definition, but a general definition better prepares network administrators to deal with new types of attacks. Each organization defines its own security policy that describes the level of access, which is permitted or denied. So it is necessary for any organization to make such a security mechanism that is broad in scope and helps to deal with new types of attack

3.1 Security Threats

When talking about threat it can be any person or event that can cause the damage of data or network. Threats can also be natural for example wind, lightning, flooding or can be accidental, such as accidentally deletion of file.

3.2 Security Vulnerabilities

Vulnerabilities defined as the weakness in any network that can be exploited by a threat. Recently almost in all areas network technologies have been applied, such as banking, tax, E-Commerce. These applications are consist of different network devices and computers and it is very important to protect these applications and devices from malicious hackers so that chances to exploit the vulnerabilities may reduce. There are different hardware and software tools available in the market to protect against these attacks, such as firewalls, Intrusion Detection Systems (IDS), antivirus software and vulnerability scanning software. However the usage of these hardware and software cannot guarantee the network against attacks. “The only truly secure system is that which is powered off – and even then I have my doubts”, a quotation by a leading security expert [21]. According to the statistic from the reports of Computer Emergency Response Team/Coordination Center (CERT/CC), the number of exploited vulnerabilities increases dramatically [22], as shown in figure 3.1.

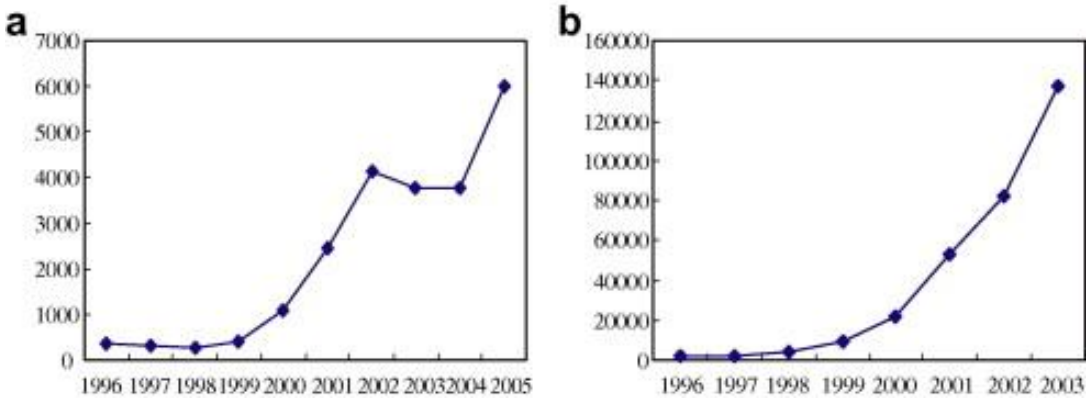

Fig.3.1. (A) The number of found vulnerabilities (B) the number of reported events.

The impact of these threats and vulnerabilities points to the problems that result in disclosure, modification or denial of service. Below are some common threats to a network.

3.3 Unauthorized Access

If you are trying to gain a casual access to an unsecured wireless network, you can be arrested on spot, even if you have no criminal intent (other than stealing their bandwidth, of course). In Canada it is called theft of telecommunication [23]. The main advantage of any network is resource sharing. As a part of network we share different types of services like file and printer sharing due to shared resources any one can try to gain illegal access which can cause unauthorized access in network.
Password sharing, guessing and capturing are three common methods to gain illegal access. Password sharing and guessing are not a new mean of illegal access, there are different techniques for guessing a password.

- Try default passwords.
- Try all dictionary words.
- Try all short words, usually 1 to 3 characters long.
- Try user's personal number, mobile or phone number, home address, etc.
- By collecting user's personal information like his/her birth day, family names.

Password capturing is a technique in which a hacker unknowingly steals user's ID and password. Trojan horse program designed for this purpose that can capture the password. Below is some basic information that can prevent from unauthorized access.

- Use strong passwords, contains at least 10 characters, contains at least one alpha, one numeric and one special character and use passwords that cannot contain dictionary words.
- Use hardware and software firewall.
- Use protection software against trojan, spyware, viruses and other malwares.
- Carefully handle emails, usually viruses, spyware and other malware are distributed through emails that have an e-mail attachment.

3.4 Inappropriate Access of resources

Unauthorized access occurs when a user try to access a resource that is not permitted for it. This may occur because administrators not properly assigned the resources. It may also occur when privileges are not enough for a user. Company which have different departments and users, some users have inappropriate access to any network resources, mostly because the users are not from the same department or may be such users who are from outside the company. For example access to the accounts department data is inappropriate by the administrators for the users which belong to some other department. In this case administrators need to grant more access rights than a user needed.

3.5 Disclosure of Data

In any organization, some information which is either stored in a computer in the network or transmitted may require some level of confidentiality. Illegal access occurs when some one who is not authorized for that tries to read the data. It mostly happen because our information is not encrypted. There are different encryption schemes that are used today; we will discuss them in detail in next chapters.

3.6 Unauthorized Modification

Unauthorized modification of data is attack on data integrity. Any changing in data or software can create big problems; possibly can corrupt databases, spreadsheets or some other important applications. Any miner unauthorized change in software can damage the whole operating system or all applications which are related to that software and perhaps need to reinstall the software with all related applications.
This can be made by unauthorized as well as authorized users. Any change in the data or in application can divert the information to some other destinations. This information can be used by any outsider or hacker who can make some changes and again send to the destination.

Some reasons that can cause the unauthorized modification are [24].

- Lack of encryption of data
- The user which only requires read permission granted write permissions also.
- Access control mechanism that allow unnecessary write permission.
- Lack of protection tools.

3.7 Disclosure of Network Traffic

When we talk about the data security we see that there are two different types of data, first type of data which is in system or computers and the second one which is transferring from machine to machine or share among the network users. These two types of data falls under two types of security, computer security and network security. The tools that are designed to protect the first type of data fall in computer security while the protection of data during transmission called network security. However we cannot distinguish a clear difference between these two types of security. As we discuss earlier that users know which type data is confidential it is also important to maintain the confidentiality of that data during its transmission. The data which can be compromised consist of passwords, e-mail messages, user names or any other useful information that could be used in future for negative purpose. Even e-mails and passwords which are stored in encrypted format in system, they can also be captured during transmission as a plaintext.

3.8 Spoofing of Network Traffic

During the transmission of data two things are important that assure the integrity of data, one is that, data is coming from a trusted host and second is that data contents are not altered or changed. Spoofing occurs when some one tries to pretend a trusted host. IP spoofing, Email spoofing and Web spoofing etc, are some types of spoofing. Messages transmitted over any network are consist of some address information, sender address and receiver address. An intruder or any hacker initially finds the IP address of a trusted host after compromising the host intruder can modify the message (packet header) so that it appears that the message is coming from that trusted host, as shown in figure 3.2. Same thing is in email spoofing that email looks like it came from Bob, but in reality, Bob did not send any email. Someone who was pretending to be Bon send the email. In web spoofing attacker create a web page like bank's site or any email like hotmail web page but this web page is basically under the control of attacker so when you put the information it goes directly to the attacker. Several reasons are behind spoofing for example transmitting the network traffic in plaintext; do not use any message authentication code technique etc.

3.9 Disruption of Network Function

Basic function of any network is to share the resources and information. A disruption occurs when network did not provide the needed functionality on time. Interruption in network can affect on one type of functionality or on different functionalities.
Several reasons may lay behind the disruption on network

- Network has no ability to detect the traffic, some time network goes down because of the useless traffic.
- Network with single point of failure.
- Hardware failure.
- Improper maintenance of network equipment.
- Unauthorized access to network components may cause the changing in the

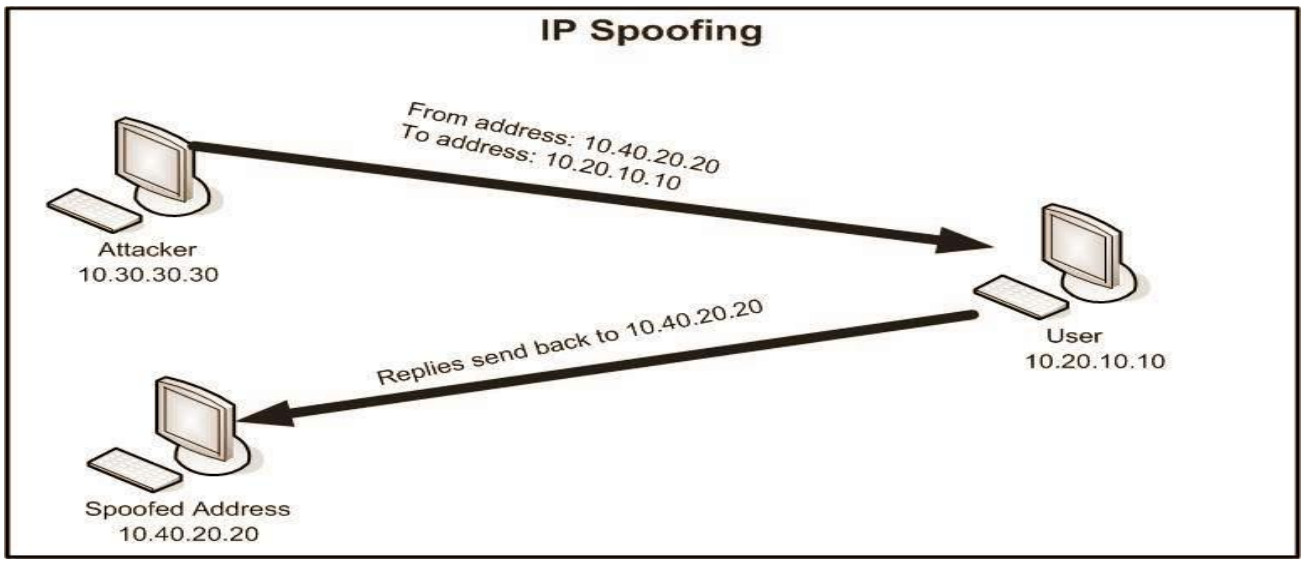

Figure 3.2 IP Spoofing

configuration of the components which also disrupt the network function.

3.10 Common Threats

Security is a continuous process and continuous war between attacker and defender. There is no security mechanism that exists which gives the complete protection. Several types of attacks can be eliminated but others will take their place. Implementation of a security mechanism some time cost too much therefore some administrators simply tolerate the expected losses and find it most cost effective solution.
Below we discuss some threats and associated losses with their expected growth. The list is not comprehensive some threats may have some common elements to other areas [25].

3.10.1 Errors and Omissions

There are lots of human unintentional errors which contribute in security problems. These can occur anywhere in the system. Sometime a small data entry error can cause the system crash, some of the error occurs during maintenance or installation which can also be a threat for security. Errors are an important threat to the integrity of data. These can produce unintentionally by data entry operators, system operators and developers. People mostly assume that the information coming from a computer system is more accurate. In past few years improvement in software quality reduces this threat.

3.10.2 Fraud and Theft

Integrity of data and confidentiality of information are the key features of any system. As information technology is increasing the threat of fraud and theft is also increasing. Attackers use daily new methods to exploit a system, these frauds involve in small amount money to large number of financial accounts. Financial systems are not only the target of hackers, systems which have any resources or controls are under attack by intruders, For Example University grading system, inventory system, human resource attendance system etc.
Threat of fraud and theft is both from insider or outsider. Majority of frauds are done by the insiders, because they are authorized users and they know the vulnerabilities in the system and they are in better position to commit a crime. Former employees of any organization may also a threat for company if administrators have not terminated their accounts properly and on time.

3.10.3 Disgruntled Employees

Disgruntled employees know better the flaws in network and they know which actions can cause the most damage. Downsizing in any organization can create a group of these people which have enough information and access to damage the system. Some examples of common sabotage are

- Editing in data.
- Modify the data incorrectly.
- Deleting the data.
- Copy the data and further use it for wrong purpose.
- Spoil the hardware.

Administrators or system managers can decrease this threat by deleting the disgruntled employee's accounts in a timely manner.

Figure 3.3 Destruction of infrastructure due to earthquake

3.10.4 Physical and Infrastructure

Some time nature shows its power. It is also a reality that the loss occurs by the cause of natural disasters is more dangerous than viruses. Flood, fire, strikes, thunder storm, earthquakes, volcano eruptions, under water explosions, loss of communication are some of the examples, which sometime can cause the damage of whole physical and network infrastructure. We cannot forget the World Trade Center and Tsunami. Some time these disasters results in an unexpected way. For example in winter storm, even your whole computer network is fully functional but people cannot go to office due to the loss of infrastructure.

Fig 3.3.Shows the loss of infrastructure due to earthquake

3.10.5 Malicious Hackers

Any one who tries to gain illegal access to computer systems for the purpose of stealing or corrupting the data called hacker.
Hackers are real and most dangerous threat for the organizations which have big computer system network. They can be from inside the organization, outside the organization or form some other continent. They break the security of the systems, compromise the system and steal the data before any illegal access detected. Hacking can be of two types, ethical hacking and non ethical hacking. Non ethical hackers are those who are harmful for any organization. “It takes a thief to catch a thief”, a general phenomenon. If you want to repel a hacker attack first you have to know that how they think. Nowadays organizations are hiring hackers to find vulnerabilities in their network security mechanism. This type of hacking is called ethical hacking and such hackers are called ethical hackers. Time is changing now emerging trends in IT is leading us to a brighter day when computers can do even more for us than they are doing now. Theses changes may leave more vulnerability to exploit for the next generation of hackers.

3.10.6 Malicious Application Terms

Malicious programs are hard to detect. They may be installed personally on a machine or build widely as commercial software package. Viruses and other type of malicious programs have the ability to replicate themselves on several systems.

In the next chapter we will discuss about different types of network attacks, their weaknesses and different malicious programs.

Chapter 4

NETWORK SECURITY ATTACKS

4.1 General Categories of Security Attacks

To compromise between opening a system and lock it down so that no one can use it, is called security and any action that compromises the security is called a security attack. A system which is providing the services required by the user accurately and preventing the illegal use of system resources is called a secure system.
Attacks can be categorized into following basic categories [27].

- Interruption: For using the data or resources it is necessary that they are available 24/7 for the authorized parties, when and where they need it. Attack on the availability of data is called interruption. Availability can be affected by intentional or un-intentional acts. Examples of un-intentional acts are, accidentally system crash, deletion and overwriting of data and some time due to non human factors like flood, fires and earthquakes. Whereas destruction of infrastructure due to wars, strikes and some attacks by hackers that crashes the system, such as denial of service *(DOS)* and distributed denial of service *(DDOS)* attacks are the examples of intentional acts. Protection against availability attacks includes backup and restoration.

- Interception: The core concept is that the data should be hiding from unauthorized users. If some one who is unauthorized to see private data, can see or copy the data that can further be used in intensive active attack. Such an attack is known as attack on confidentiality. Data integrity can be accomplished by strong authentication and strict access controls, because some time authorized users may also a threat for confidentiality of data. They can obtain another person's credentials.

- Modification: Integrity of data deals with prevention of intentional or unintentional modification of data. Attack on integrity of data called modification. Different algorithms used for validation of data that can resist in alteration of data. Protection of data from modification is foremost concern than detection. Integrity of data could maintain at many layers of OSI system model.

- Fabrication: Attack on authenticity called fabrication. Authenticity means that message is coming form the apparent source. It assures that you are who you say you are. User name and password is the most common way to achieve authentication, some other techniques are like smart cards and digital certificates.

Above mentioned attacks are shown in figure 4.1

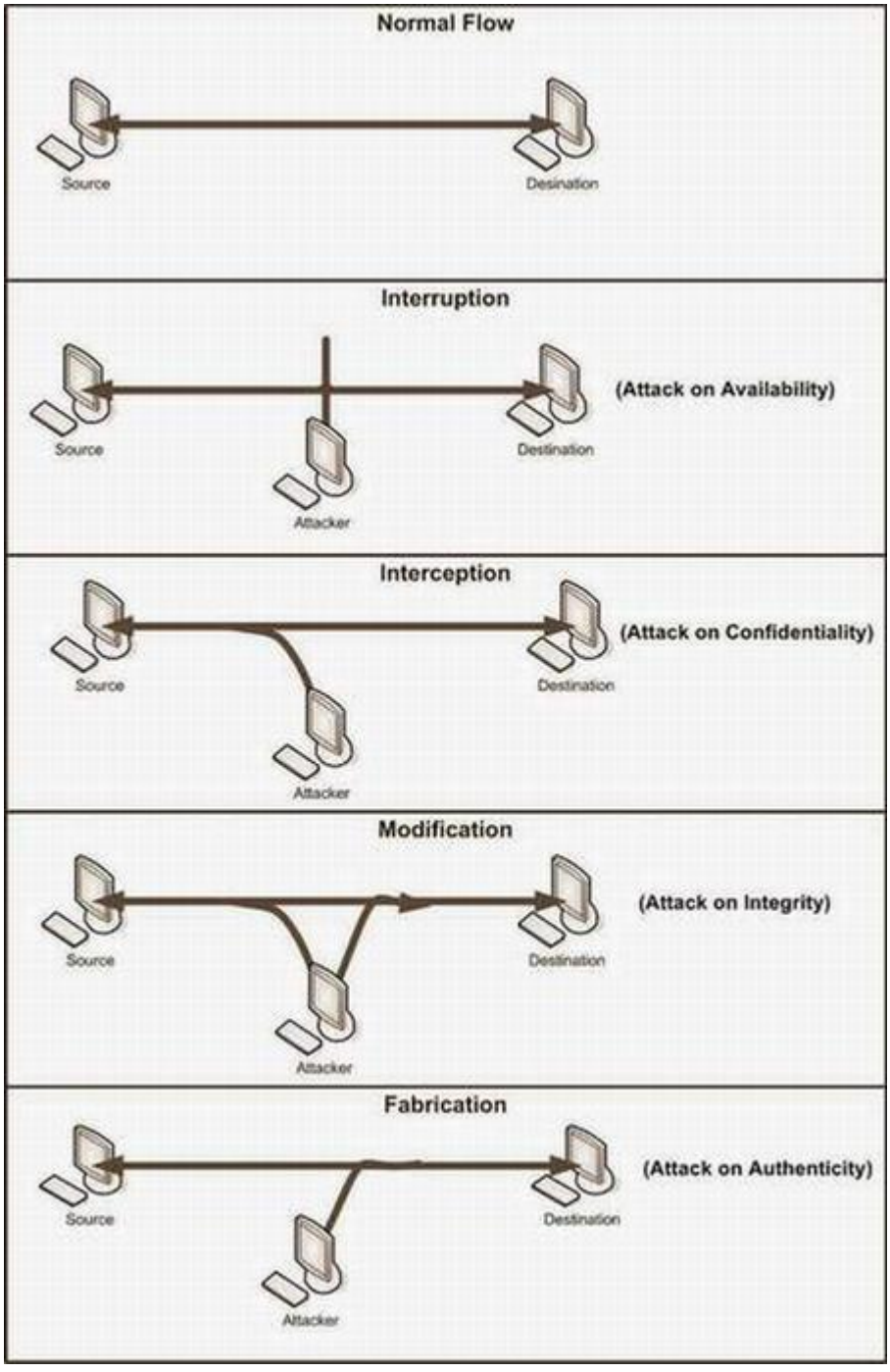

Fig.4.1. Basic types of Security Attacks

On the basis of these four attacks we can further classify security attacks as *passive attacks* and *active attacks*. Passive attacks are only involved in monitoring of the information (interception). The goal of this attack is to obtain transmitted information. Two types of passive attacks are "*release of message content"* and *"traffic analysis"***.** Passive attacks are

hard to detect because they do not involve in any alteration. Different encryption schemes are used to prevent against these attacks.

Active attacks are involved in modification of data (interception, modification, fabrication) or creation of false data. These attacks are further subdivided into four categories, "*masquerade", "replay", "modification of data"* and *"denial of service"*. When an unauthorized user tries to pretend as an authorized user is called masquerade attack. Replay attacks involved in capturing the message between two communication parties and replay it to one or more parties. Bring the network down to its knees by flooding the useless traffic in network is called denial of service attack.

Figure 4.2 and 4.3 are showing passive and active attacks.

Attacks are either active or passive. Information which hackers obtained from a passive attack is used in more aggressive active attack. We will discuss in detail some common types of network attacks.

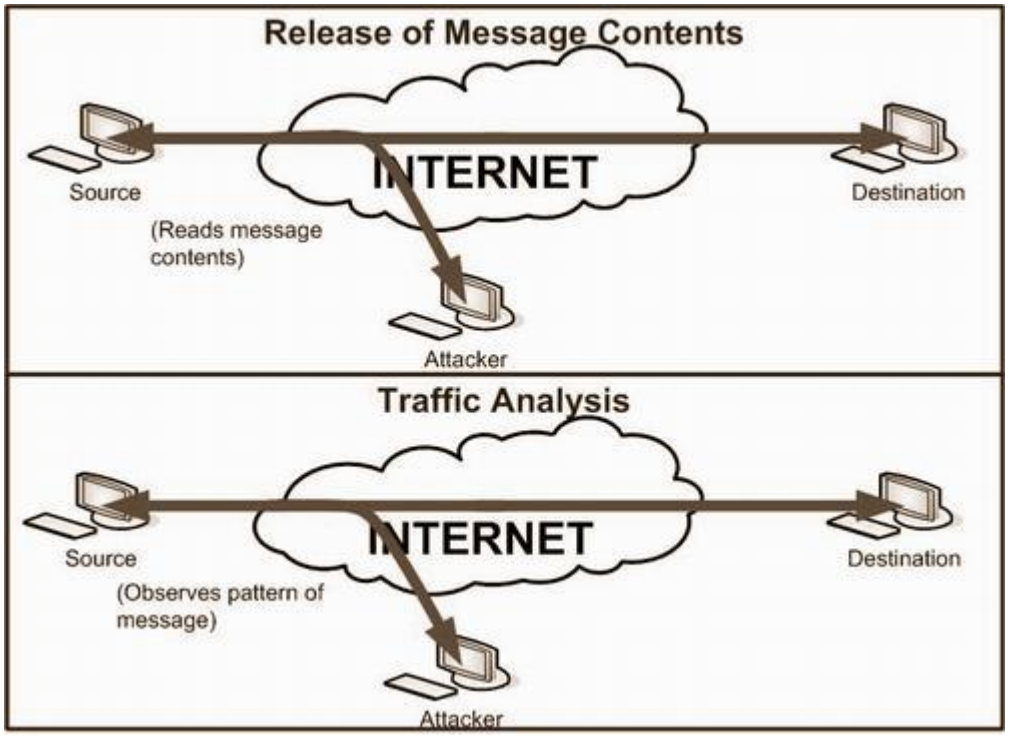

Figure 4.2 Passive Attacks

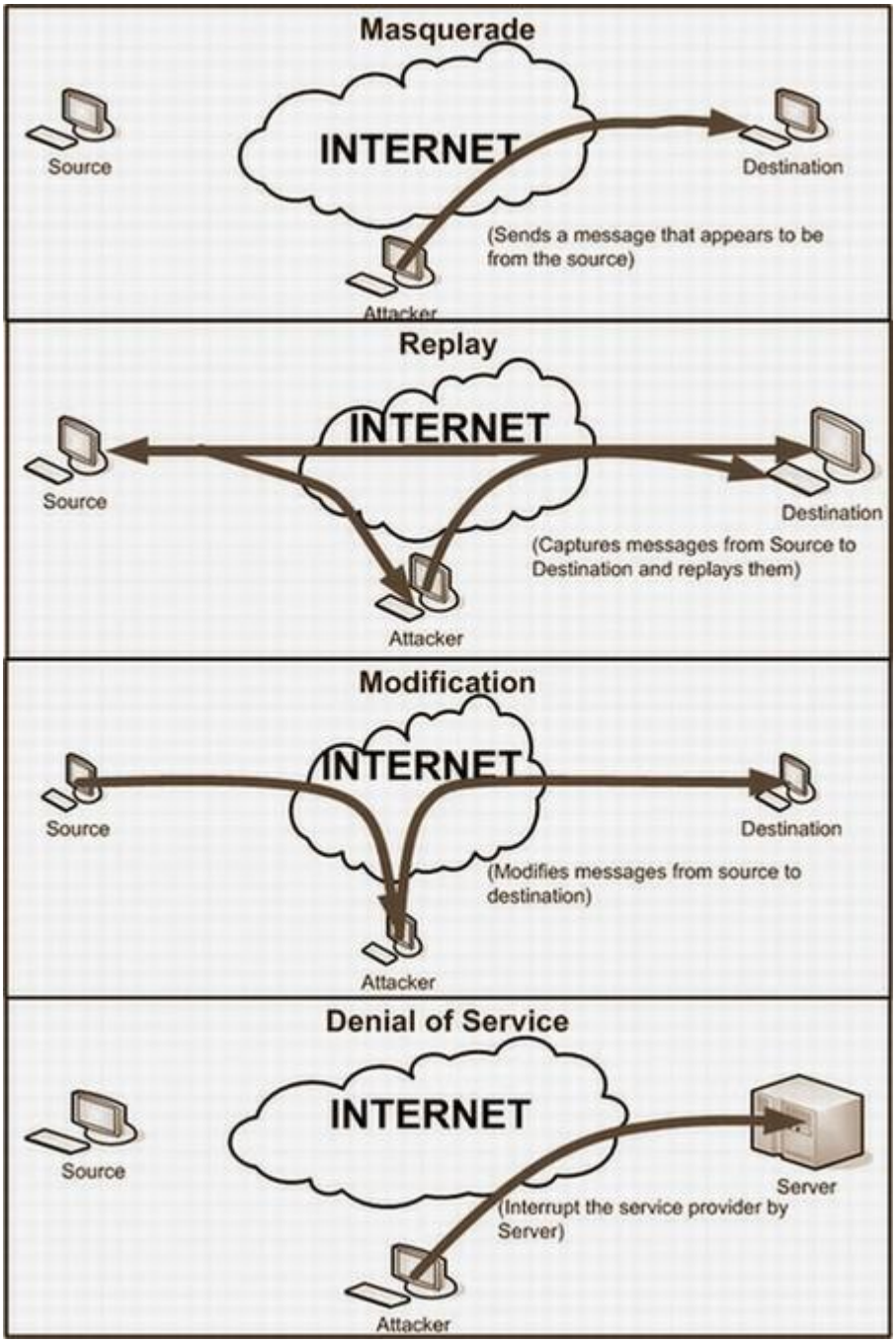

Figure 4.3 Active Attacks

4.1.1 Reconnaissance Attacks

Gathering information against a targeted host or network is called reconnaissance attack. Attacker analyze the target host and try to discover the details like alive IP addresses, open ports of the network, failour of operating system, and types of services and protocols running

on the network. Reconnaissance attacks are common they are not so much dangerous because they are not involved in any kind of alteration or destruction of data but on the other hand they show the vulnerabilities in the network. They allow hackers to see which ways are open to access the system and provide enough information to them which they can further use in denial of service (DOS) attacks.

Some basic reconnaissance attacks are:

- Packet Sniffers
- Port scan and ping sweep
- Internet information queries

4.1.1.1 Packet Sniffers

As we discussed earlier that data which is traveling across a network is not in a continuous stream of data in fact it is in the form of packets. As we know that we cannot see the atom through naked eye we need a device like electronic microscope same is in the case of analyzing the data packet. Packet sniffer is a tool or device that can be used for capturing the packet at data link layer. Packet sniffer is not only a hacker's tool but it can be used both by the hacker for eavesdropping and by the administrators for network monitoring and troubleshooting. *Tcpdump, windump, wireshark (ethereal)* and *Dsiniff* are examples of different sniffing tools.

Sniffing can be of two types depending on the network.

- Passive Sniffing
- Active Sniffing

4.1.1.1.1 Passive Sniffing

Passive sniffing is used in hubbed networks. The drawback of using the hub in network was that, the hub broadcast a packet to each and every machine on the network. There is a filter on each machine which decides whether to accept or discard the packet. If a packet addresses to a specific machine then filter decide to accept it otherwise discard the packet. Sniffer disables this filter so that network traffic can be analyzed. This stage is called "promiscuous mode" [28]. Hence if 'Bob' on computer A sends a message to 'John' on computer B, a sniffer on computer C can easily capture the contents of that message even without knowing Bob and John. Passive sniffing is hard to detect because it generates no traffic on network. This type of sniffing worked well when hubs were used. To avoid passive sniffing most of the networks nowadays are using switches instead of hubs.
Figure 4.4 is showing passive sniffing.

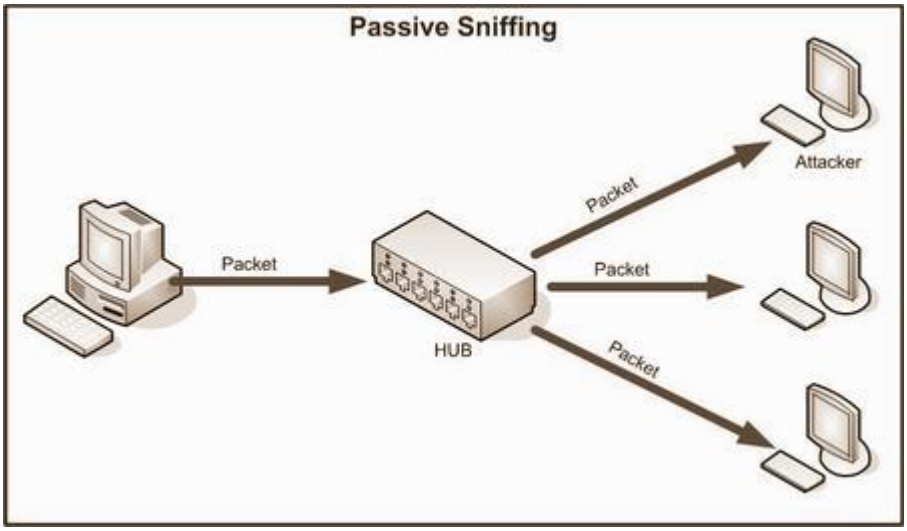

Figure 4.4 Passive Sniffing

4.1.1.1.2 Active Sniffing

Active sniffing is performed on switched network. A switch limits the sniffer to see the broadcast packets. Switch worked as a central entity, rather then broadcasting it simply get message from source machine and send it directly to the addressed machine. So if computer C is in promiscuous mode it cannot see the message form Bob to John.
It does not mean that sniffing is not possible in switched networks. Media Access Control (MAC) flooding and poisoning of the Address Resolution Protocol table (ARP) are the ways to hack a switched network.

- MAC Flooding
- Spoofed ARP Messages

Switches worked on the basis of MAC addresses. They maintain an address resolution protocol (ARP) table in a special type of memory called Content Addressable Memory (CAM). ARP table has all the information that which IP address is mapped to which MAC address.
The act of overloading the CAM is known as MAC flooding. Low memory in older or cheaper switches can cause MAC flooding. Flooding of too many MAC addresses can fill up the memory so that switch cannot hold more entries. At this stage switch goes to a *failopen* mode [29] and cannot perform IP to MAC mappings, starts behaving like a hub and starts transmitting the data to all machines. In MAC flooding attacker inject large amount of traffic which may draw attention towards hacker. This traffic can be detected by any sniffer detecting software.
The other technique to hack a switch network is called ARP poisoning. A review of ARP is that it is almost similar to Domain Name Server (DNS). DNS resolves domain names to IP addresses while ARP resolves IP addresses to MAC addresses. Hacker fools the switch and tries to pretend the destination machine.

He tries to convince the switch that the IP address of another trusted host belongs to him. A very interesting thing is that it is also up to the attacker that which IP address he wants to redirect to his system, spoofing thsystem, spoofing the default gateways will redirect all host messages towards the attacker. However for this, attacker has to poison host ARP table. The other way is to poison the ARP cache of a central entity of the network, hacker express that the IP address of switch (or router) is mapped with his MAC address. Through this way all the traffic first goes towards the attacker then the router [30]. Active sniffing is shown below in figure 4.5

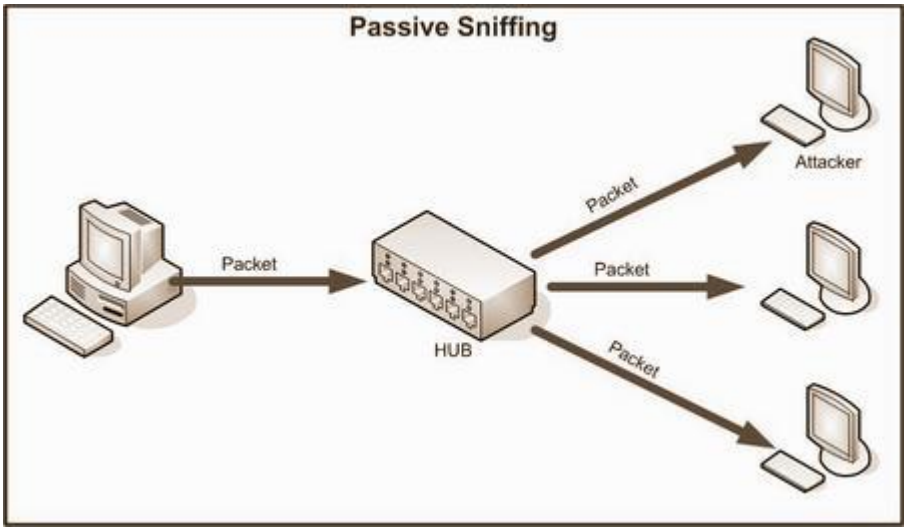

Figure 4.5 Active Sniffing

4.1.1.2 Port Scan and Ping Sweep

Port scan and ping sweep are two common network probes typically used to run various test against a host or device to find vulnerable services. They are helpful to examine the IP address and the services which are running on a device or host. In port scanning hacker sends a packet to each target port and reply message indicates that either the port is open or closed which is further helpful to launch an attack against a specific service. For example if hacker finds that port 143 (IMAP port) is open then on next step he/she tries to find out that which version of IMAP is running if that version is vulnerable then hacker can access the machine as a super user using an "*exploit*" program (program that automatically break the security hole) [31]. The most popular probing tool is Nmap (Network Mapper).

Different types of Nmap scans are

- ***TCP Connect Scan***: It makes a complete TCP connection that's why is easy to detect.
- ***TCP SYN Scan***: Attacker sends a SYN to each target port, if target port is open target sends SYN-ACK. The attacker then sends a RESET packet and aborts the connection. This type of scan is also called half-open because attacker connects to the port and breaks the connection just before full connection. These types of scans are hard to detect.

- ***FIN Scan***: attacker sends a fin packet which is able to pass by firewalls without modification; open ports ignore the packet while close ports sent back a RESET packet.
- ***ACK Scan***: ACK scan is good in network where firewalls are running. It did not classify the port as open or closed, if reset comes back from the target it classify the port as "*unfiltered*" otherwise "*filtered*".

The method of finding that which IP addresses are alive is called ping sweep. Attacker sends an ICMP packet to each machine (with in a range) to a targeted network. The aim is to find out the machines which are alive and which are not alive. These ICMP replies from different machines are logged into a file for future reference. Network administrators may also use ping sweep to figure out which systems are alive and which are not for diagnostic reasons.
Fping is a tool used for performing ping sweep. Working on round robin function, takes a list of IP addresses, sends a ping packet to an IP address and immediately proceed toward next IP address. To detect ping sweep there are different tools available. Example is ***Ippl*** a protocol logger that have the ability to log ICMP, TCP and UDP packets.

4.1.1.3 Internet Information Queries

DNS queries provide the particular information of domain and the addresses associated with that particular domain. IP queries display the range of IP addresses and for which domain that addresses are associated. Ping sweep presents a clear picture of a particular environment. After these queries port scan start by the hacker which leads him to find out which ports are open and which services are running on these ports. Finally the whole information can be helpful when hacker tries to compromise any system through these services.

4.1.2 Access Attack

We discussed earlier that there are vulnerabilities in services which are running on a system like web services, FTP services and any authentication services that authenticates the user and hacker can exploit these vulnerabilities. Access attacks occur when a malicious hacker exploit these vulnerabilities and succeed to access the confidential information of any organization.
Different types of network attacks are

- Password Attacks
- Trust Exploitation
- Port Redirection
- Man-in-the-middle attack

4.1.2.1 Password Attack

Several methods can be used for password attack. Trojan horse, IP spoofing and packet sniffers can show the detail of the user like user name and password. We may refer password attack as, repeated attempts to find the user information (user name or password). Once an intruder succeeds then he/she has the same access right which compromised account has.
Most common weaknesses in an organization are

- Weak passwords.
- Default Passwords (most of the devices and applications have set on their default password which we forgot to change).
- Password are stored as plain-text.

We can mitigate password attacks by using strong and encrypted passwords; by change the password after some specific time and by selecting the property that after certain wrong login attempts the account should be locked.
However, password cracking is also helpful to build and maintain a more secure system like;

- To sense the security of the password.
- Password cracking can be used to recover forgotten password.
- To migrate users.
- To maintain check and balance system [32].

4.1.2.1.1 Types of Password Attack.

Strong, long and encrypted passwords does not mean that they are unbreakable; it's just a matter of time. Few years earlier the time to break a password was may be 100 days but now it's just a matter of two or three weeks.

Different types of password cracking attacks are:

- Dictionary Attack
- Brute force attack
- Hybrid Attack

	Dictionary Attack	Brute force Attack	Hybrid Attack
Speed of the Attack	Fast	Slow	Medium
Passwords Cracked	Finds only words	Finds every password(A-Z, 0-9, special characters)	Finds only the password that have a dictionary word as the base

Table lV.l Types of password Attacks

Different password cracking programs are available like L0phtcrack, NTSweep, NTCrack, Crack, John he Ripper etc.

4.1.2.2 Trust Exploitation

When a hacker attacks on a computer which is outside a firewall and that computer has a trust relationship with another computer which is inside the firewall, the hacker can exploit this trust relationship. We can mitigate this type of attack by using private VLANs between switches or by limiting the trust relationship between systems which are

inside and outside the firewall. We can also reduce this by eliminating useless trust relations between different servers. For example if our AAA (Authentication, Authorization, and Accounting) server is inside the DMZ (Demilitarized Zone), there is no need to have a relation of AAA server with the file server. Figure 4.6 explaining trust exploitation phenomena.

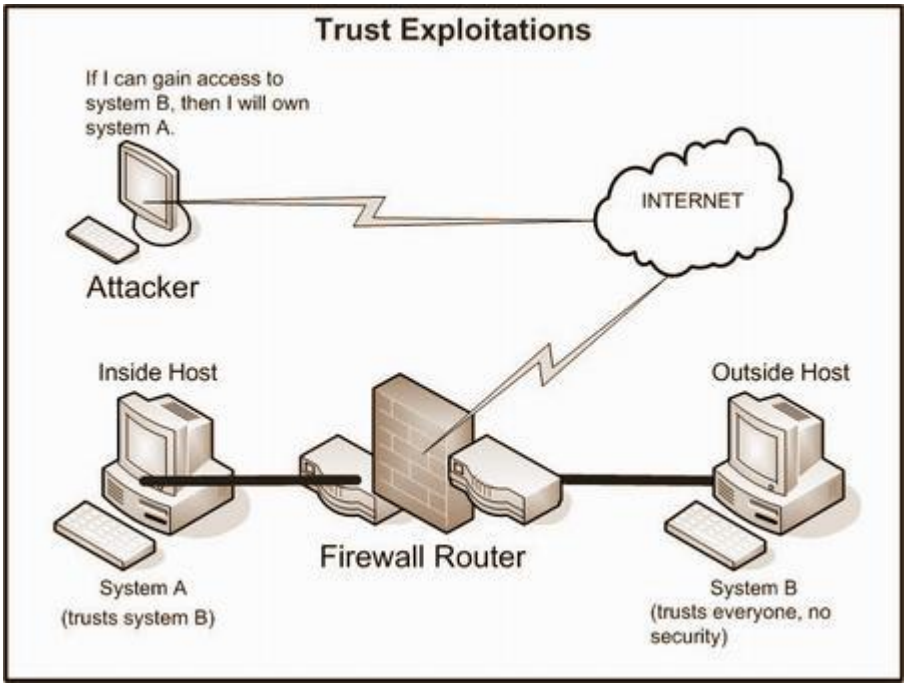

Figure 4.6 Trust Exploitation Attack

4.1.2.3 Port Redirection

It is another type of trust exploitation attack in which a hacker bypasses the security mechanism. Consider the below network in which hacker on the outside have the ability to access the public computer but not the computers which are in DMZ or which are inside the firewall. If public computer compromised by the hacker then hacker installs a software that can redirect the traffic towards the hacker, directly to the inside computers. In this way hacker makes a tunnel for communication and bypasses the security firewall. See figure 4.7 for port redirection attack.

4.1.2.4 Man-in-the-Middle Attack

When hackers succeed to intrude himself between two communication parties this type of attack is called MITM (Man-in-the-Middle) attack. In this way hacker can intercept data between source and destination host, can modify data and retransmit it to the destination host and can also inject any type of false data. MITM attacks can affect on availability, confidentiality, integrity and authenticity of data. Strong cryptography can mitigate this type of attack. SSL, SSH and use of IPSec also gives end to end security (entire connection is encrypted).

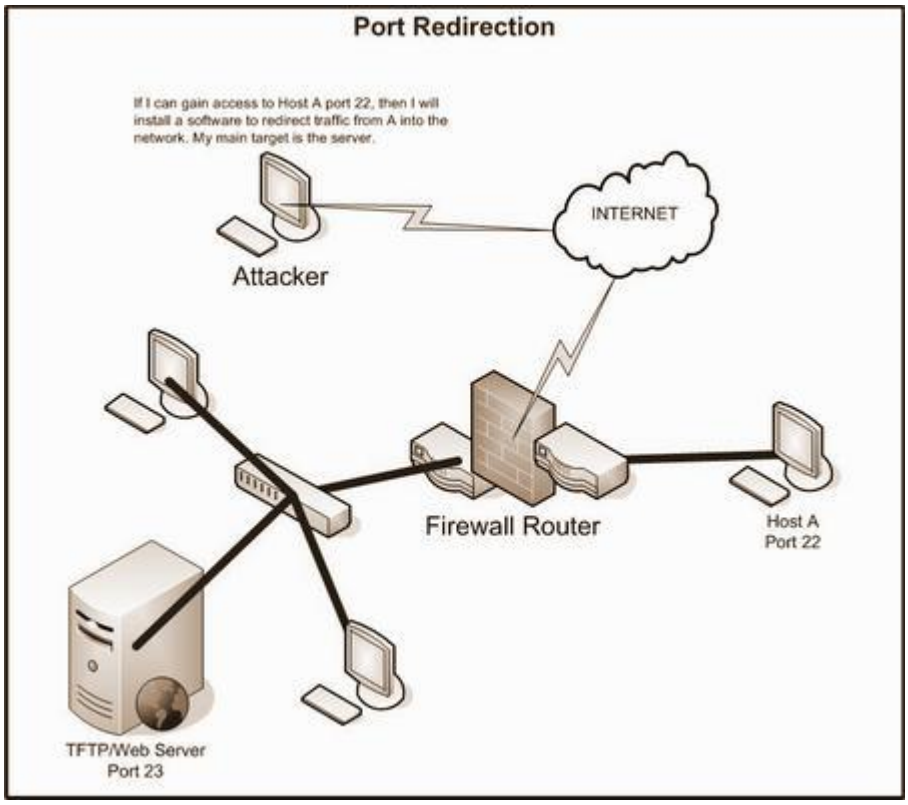

Figure 4.7 Port Redirection Attack

4.1.3 DOS Attacks

Types of attack that bring the network down in such a way that recourses are not available even for authenticated users are known as DOS attacks. Malicious hacker saturated the target machine with useless traffic so that it cannot respond or too slow to respond and some times unavailable. Attacker may target a single machine to make it impossible for outgoing connections on the network or may attack on the whole network to make it impossible for incoming and outgoing traffic. For example attack on web site of any organization. *Ping of death, SSPing, Land, Win Nuke and SYN flood* are some of the examples of DOS attacks. In SYN flood attack hacker sends a SYN packet to target host which then respond with SYN acknowledgement, at the end attacker does not send any ACK packet to the target host that causes the connection to remain in half open state. TCP connection does not remove this connection from its table and wait to expire this session, attacker take the advantage of this and continue sending new SYN packets until TCP SYN queue filled and cannot accept new connections [33]. The common method for blocking DOS attack is to place a filter which examines the pattern of data; if same pattern of data came frequently then filter can block that message.

4.1.3.1 Distributed Denial of Service (DDOS)

In DDOS attacks several compromised systems are used to launch an attack against a targeted host or network. For targeting a host attacker first compromise some other hosts on network and

install some software for controlling them usually these compromised hosts are called agents or zombies. Using these agents attacker launch overwhelm attack against the target. Compromised

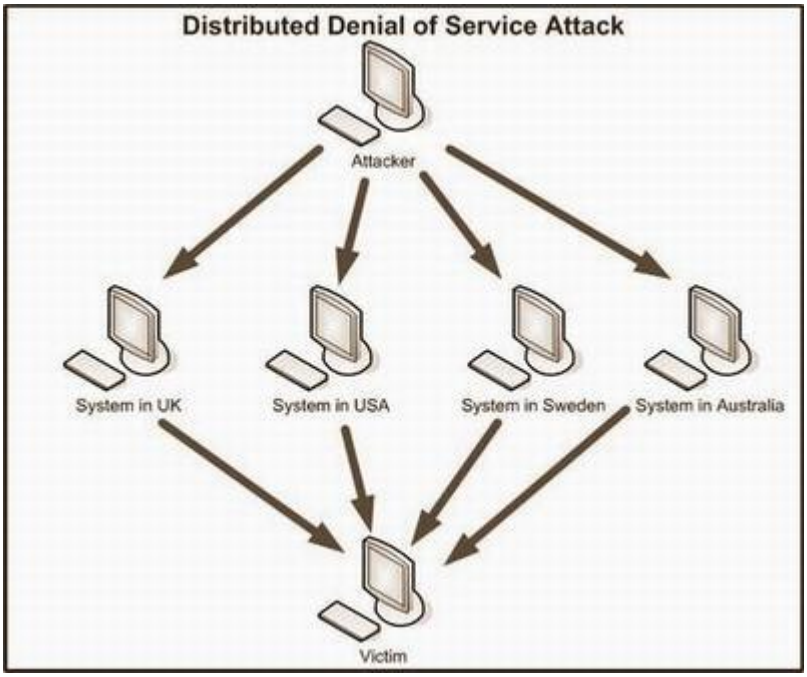

Figure 4.8 Distributed Denial of Service Attack

systems control with different software like *Trino and Shaft*. Example of DDOS attacks are *SMURF, MYDoom and TFN*. DDOS attacks are very hard to defend. To trace out the intruder is also very difficult as they are on back side and using other hosts against the victim. Figure 4.8 is describing distributed denial of service attack.

4.1.3.2 Buffer Overflow

We can define buffer overflow as when a hacker tries to store too much data in buffer which it cannot hold. Take an example of glass which can hold 5 ounces of water if we put 8 ounces what will happen? Obviously water overflows from the edges. Buffer overflow is similar to this example;

where glass corresponds to buffer and water corresponds to data. The overall goal of this attack is to weaken the function of victim's program so that hacker can easily take control of that program. Buffer overflow is the best known attack on security which can cause attack against availability, integrity and confidentiality of data. Examples are *NetMeeting Buffer overflow, Linux Buffer Overflow, Outlook Buffer Overflow.*

4.1.4 Viruses and Other Malicious Program

Viruses and other malicious program have the ability to make duplicate copies of them on an ever increasing number of computers. A "*Virus"* is just like a computer program that spread by copying itself into other programs. Another malicious program *"Worm"* is spread through the network. Without the network it cannot spread and can eliminate only when whole network or system is shutdown. Examples of popular worms are *Code Red, Slammer, Storm Bot.* A malicious

program that resides in system and execute on an event like date or time is called **"***Logic Bomb", "Trojan Horse"* is another type of malicious program that hackers use to steal useful information like user name, password and bank account codes.

Chapter 5

SECURITY COUNTERMEASURE TECHNIQUES AND TOOLS

5.1 Security Countermeasure Techniques

The security countermeasure techniques are directly related to such parameters that survive in the form of network bugs or vulnerabilities and their effects in a communication network. After analyzing the effect of these parameters, we can select some key security countermeasure techniques for a network.

The selection and implementation of these countermeasure techniques in network environment depends on the network administration team. It depends upon their updated knowledge and awareness about network, standard network architecture, traffic parameters in the form of application behavior (OSI and TCP/IP layer network protocols knowledge and working role), network hardware performance, security threats and existing weak points in network. A rough or out of date knowledge can become a cause of network bugs and vulnerabilities.

By considering the above measurements many research organization have assigned some most essential key security countermeasure techniques for a standard level network infrastructure [34].

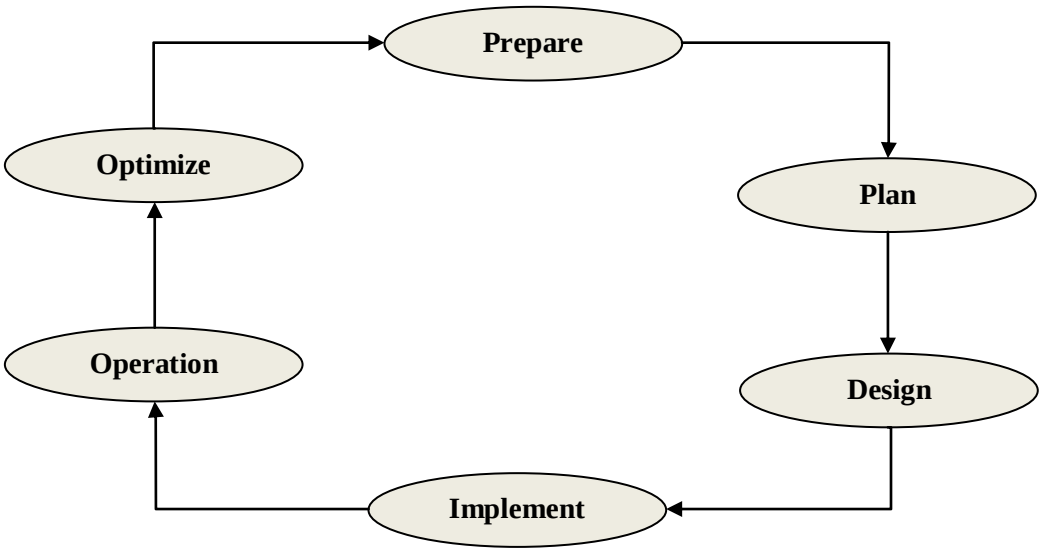

Fig 5.1: Network Lifestyle Phases or Services Approaches [35]

5.1.1 Security Policies

A strong security policy performs an efficient role in a network. If policy develops after analyzing the network and behavior of its components then it results a much secure and smooth network.

5.1.2 Authority of resources

The authorization of systems or network resources has an important role in security countermeasure. After a fair survey of network we may assign a proper level of authority for accessing the system resources. The policies of antivirus or the access control list of router or firewall can define an authority for accessing network resources in a proper manner.

5.1.3 Detect malicious activities

The presence of intrusion detection system has an important role in security countermeasure. The study and analyzing the log files against malicious activities in network can save a system. It provides a futuristic safety approach against many other malicious aims.

5.1.4 Mitigate possible attacks

The symptoms of a malicious attack give us an idea about which type of protection is required for a system against that attack. We can re-adjust or re-configure our security system parameters by generate a strong resistive block against the attack.

5.1.5 Fixed core problems

By fixing basic problems in a system or network we can save the system or network. These basic but core problems are basically a hidden spot which exists in any common network or system, like improper updating of system applications, out of date applications and updates virus patches (not on proper time) these all can create a security flaw in any network.

5.2 Security Countermeasures Tools

We will now discuss tools to defend against the attacks, we have discussed earlier.

5.2.1 Cryptography

Cryptography is used to protect data from interception. We have to be sure that our confidential data cannot be understood by an unintended user. Cryptography is the study of methods to send data in unrecognizable form so that only the intended user can recognize and read the message. There are two basic cryptographic terms, *Plain Text*, the text or data which we want to encrypt, and *Cipher Text*, the encrypted form of plain text.

5.2.1.1 Overview

Cryptography concerns with two things, Data is coming from the apparent or trusted source and contents of data are not altered. Goals which we want to achieve from cryptography are:

- *Confidentiality: T*o keep the data between authorized user.

- *Data Integrity:* Assuring data integrity, we must have the ability to detect manipulation of data by unauthorized users.
- *Authentication:* Identification of sender and receiver is called authentication. When exchanging the data two communication parties must identify each other.
- *Non-repudiation:* In some situations when one entity denies previous commitments, there must be a solution (usually a third party) to resolve this situation is called non-repudiation. For Example [36].

We can classify cryptography into these three independent dimensions:

1. Types of operation used to change the plain text into cipher text. Major focus is on "no information loss". Two general rules used in all types of encryption algorithms; *Substitution*, in which all units of plain text are replaced by some other units and *Transposition*, in which all units are rearranged.

2. Communication depends on the number of keys used. If single key is shared between sender and receiver, this type of encryption is called *symmetric* encryption also called conventional encryption and the shared key is called secret key. If two different keys are used between sender and receiver, this referred to as *asymmetric encryption* also called as public-key encryption or two-key encryption.

3. The procedure in which the plain text is processed. The way in which input blocks of elements produce an output block against each input block is called *block cipher* while the way in which input elements process continuously and produce out put of one element at a time is called *stream cipher* [37].

5.2.2 Conventional or Symmetric Encryption

It was the only encryption scheme available before the public-key encryption. One secret key is shared among the sender and the receiver. Whole procedure of conventional encryption consists of five stages:

1. *Plain Text:* The original message or data which we want to be encrypted.
2. *Encryption Algorithm:* Encryption algorithm performs different transformations on the data.
3. *Secret Key:* Secret key is the input to the encryption algorithm. Different transformations performed by the encryption algorithms depend on the secret key.
4. *Cipher Text:* This is the out put of scrambled message.
5. *Decryption Algorithm:* Reverse of the encryption algorithm, it produces the plain text with the help of same secret key and the cipher text.

5.2.2.1 Principle

The following figure 5.2 describes the conventional encryption. The encryption process consists of an encryption algorithm and a secret key. The value of key does not depend on the plain text. If we change the value of key the algorithm will produce a different output or cipher text. When cipher text is produced we can fetch the plain text back by using the decryption algorithm with the help of same secret key.

In the above figure the encryption algorithm produces cipher text Y with the help of original message X and secret key K as an input

$Y=E_K(X)$

And at the end intended user reverse the transformation.

$X=D_K(Y)$

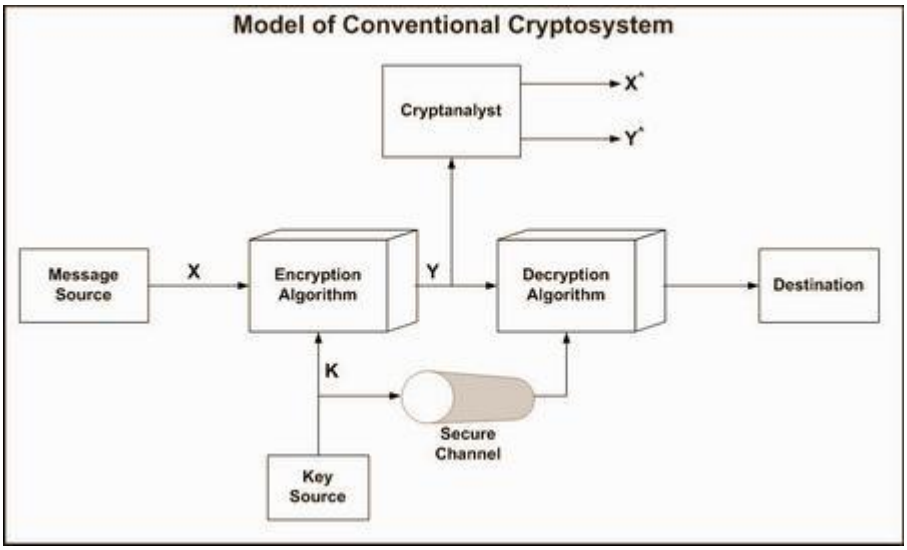

Figure 5.2 Model of Conventional Encryption

One important thing is that the security of the conventional encryption depends on the secret key not on the algorithms. Even if we know the cipher text and algorithms, it is practically impossible that a message can be decrypted with the help of cipher text and encryption/decryption algorithm.

5.2.2.2 Symmetric Algorithms

Symmetric and public key symmetric, are two general types of algorithms. In most symmetric algorithms two communication parties use the same key for encryption and decryption that is why it is also called secret-key, single-key or one-key algorithm. For safe communication key must remain secret. Symmetric algorithms can be divided in two categories on the basis of their operations on plain text. *Stream Ciphers* which operate plain text as single bit or byte. For example if we shifted alphabets three places up.

Plain Text	H	E	L	L	O
Key	+3	+3	+3	+3	+3
Cipher Text	K	H	O	O	R

We can create a more complex key, for example instead of shifting each character by three, we increment with a key "123"

Plain Text	H	E	L	L	O
Key	+1	+2	+3	+1	+2
Cipher Text	I	G	O	M	Q

While Block Cipher operates on plain text as a group of bits, these groups of bits are called blocks. For example if we generate a key which switched every two alphabets with each other.

Plain Text	H	E	L	L	O
Cipher Text	E	H	L	L	O

There are different symmetric algorithms. Such as Data Encryption Standard (DES), Triple Data Encryption Algorithm (TDEA) and International Data Encryption Algorithm (IDEA).
DES is the most widely used encryption scheme. Following are the properties of DES:

- Widely used encryption scheme.
- Algorithm referred to as Data Encryption Algorithm (DEA).
- Is a block cipher.
- The block of the plain text is 64-bit long.
- The secret key is of 56-bit long [38].

Using of 56 bit key means that there are 2^{56} ($7.2*10^{16}$) possible keys, so if a brute force attack occurs the approximate time to break the cipher will be more than thousand years.
Another example of symmetric algorithm is TDEA also known as ***3DES***. This algorithm uses three executions of DES algorithms encryption-decryption-encryption. Using of three executions make it more secure (Fig 5.3).Key length of 3DES is 168 bits.

$C=E_{K3}[D_{K2}[E_{K1}[P]]]$
Where C= Cipher Text
P= Plain Text

Whereas decryption has the same procedure with keys reversed.
$P=D_{K1}[E_{K2}[D_{K3}[C]]]$

IDEA, Blowfish and RC5 are examples of some other symmetric block ciphers.

5.2.2.3 Key Distribution

As we have discussed earlier that for secure communication between two parties there must be a same key. It is also necessary to change the key frequently so that attacker could not compromise the key. So the strength of any cryptographic system depends on the key distribution process. There are several ways to distribute the keys between two parties A and B. [39]

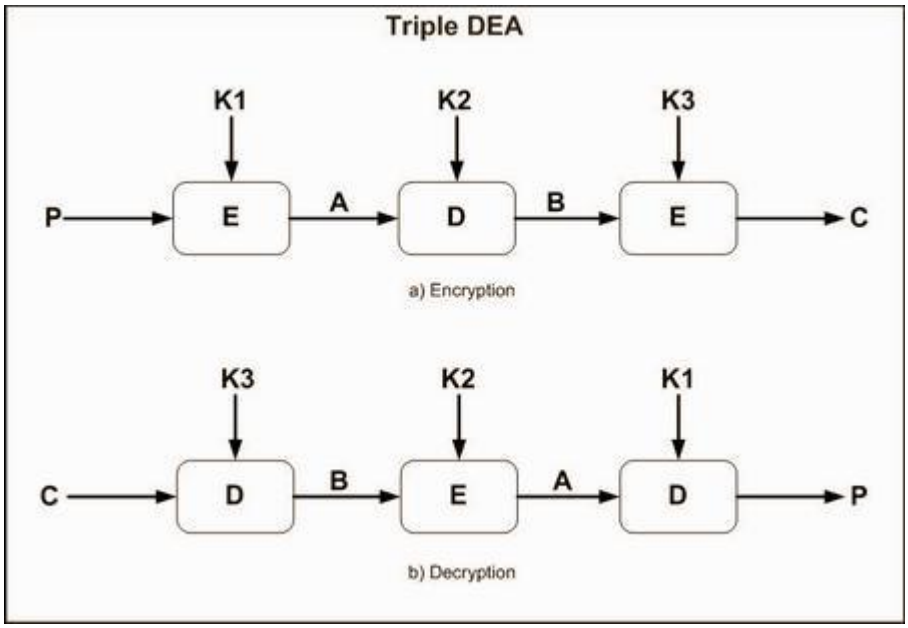

Figure 5.3 Triple DEA

- Key could be selected by party A and physically delivered to party B.
- Any third party could select a key and physically deliver it to A and B.
- If A & B have previously used recent key, one party could transmit the new key to other, which is encrypted by the old key.
- In case of encrypted connection of A & B to a third party C, third party C could deliver the key to A & B on encrypted links [39].

5.2.3 Public-Key or Asymmetric Encryption

Instead of using one key which is used in conventional encryption, asymmetric uses two separate keys. The use of two keys makes the communication more secure and authenticated. Asymmetric scheme has six ingredients:

1. *Plain Text*: The original message or data.
2. *Encryption Algorithms*: Encryption algorithm performs different transformations on the data.
3. *Public and Private Key*. The transformation by the encryption algorithm totally depends on these keys. These keys are selected in such a way that if one is use for encryption, the other is used for decryption.
4. *Cipher Text*: This is the out put scrambled message.
5. *Decryption Algorithm*: Reverse of the encryption algorithm.

5.2.3.1 Principle

Public and private keys are used in public-key encryption, as name suggests that public key is used publicly while private key is only used by its owner.

The following steps are followed in public-key encryption (See figure 5.4).

1. Each and every user in a network generate a pair of keys, one is used for encrypting the message while other is for decrypting the message.
2. From those two keys each user places one key in a public register, so that every other user can access that key. In this way each user has a collection of public keys of all the users in network.

3. If user A wants to send a message to user B, A encrypts a message with B's public key.

4. When user B receives the message he/she decrypts it by using his/her private key. No one else can decrypt this message

So in this approach private keys are generated locally only for user itself and could not be shared, while every participant has a collection of public keys. Securing the private key means secure communication.

Public key encryption could be used in another way (as illustrated in figure 5.5). Some time we are more interested in data integrity and data authenticity than eavesdropping.
For example if user A wants to send a message to user B, Instead of data confidentiality user B only want to assure that the data is coming from user A.

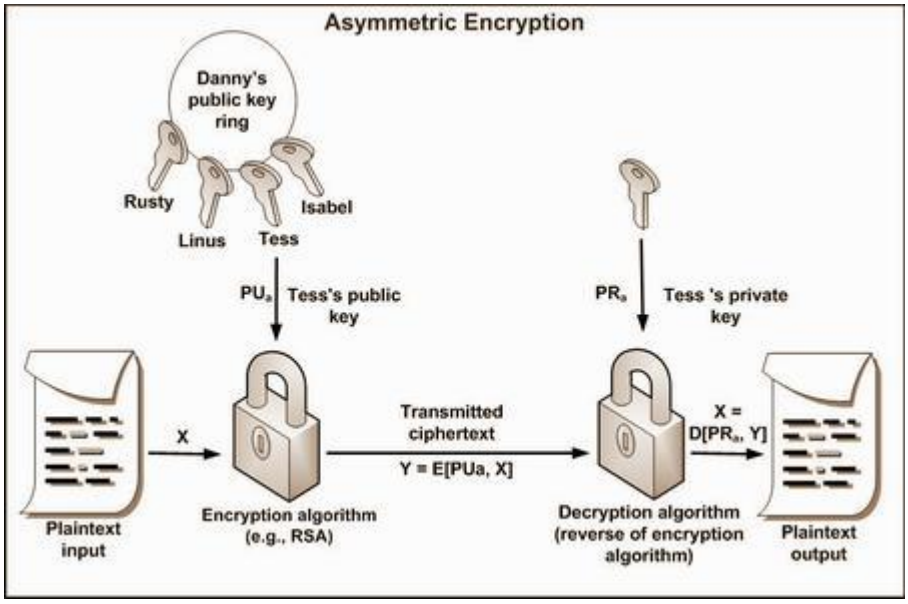

Figure 5.4 Asymmetric Key Encryption

In this case A uses his own private key to encrypt the data, when B receives the cipher text; he/she can decrypt the data with A's public key which proves that message has been encrypted by A.

Encrypting the message Using recipient's public key provides confidentiality while encrypting the message using sender's private key provides authenticity, the term used

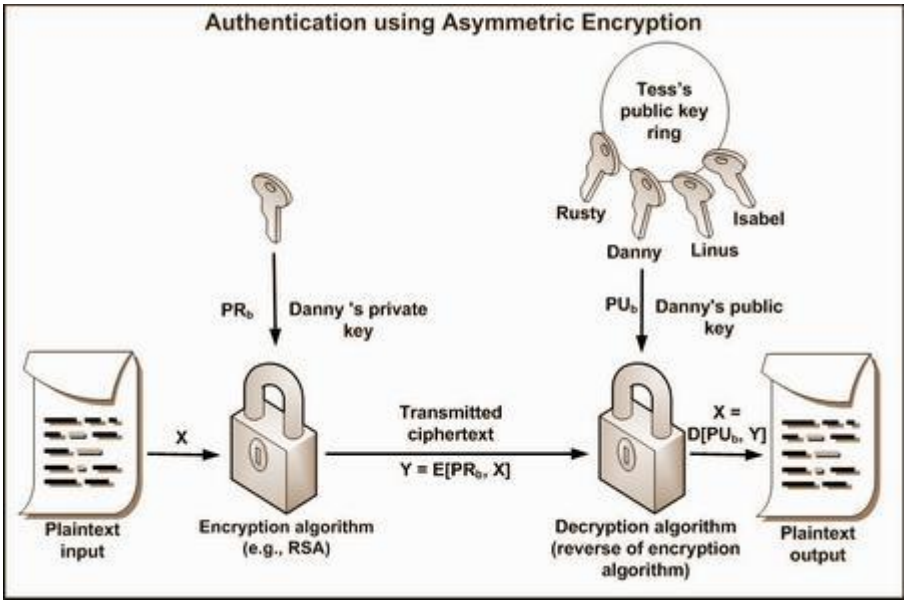

Figure 5.5 Authentications Using Asymmetric Encryption

for this phenomenon is called "*Digital Signature"***.** In digital signatures sender signed the message with its private key which can be verified by any user who has the sender's public key (figure 5.6).
Digital signatures can be used to authenticate the message source. For example when any government publishes its electronic copy of budget or its public or private laws, or when universities publish their student's transcripts they publish it with their digital signatures.

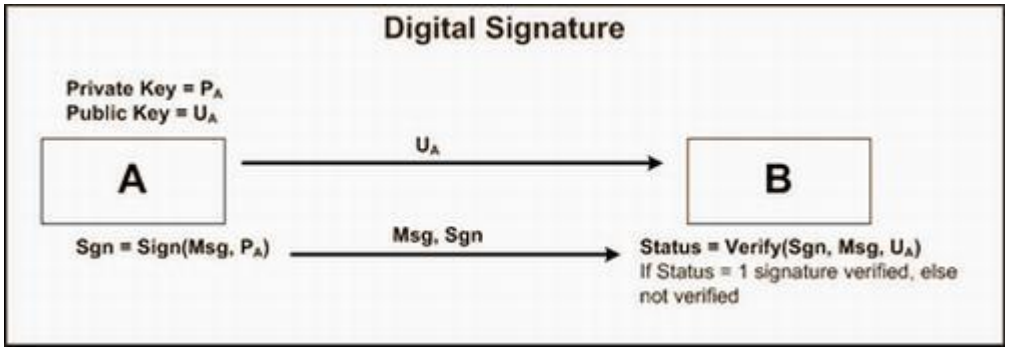

Figure 5.6 Digital Signature

5.2.3.2 Asymmetric Algorithms

Asymmetric cryptography depends on the cryptographic algorithms based on two keys. There are some conditions which every algorithm must fulfill:

- It must be easy for any party to generate public and private key
- It must be easy for sender A to encrypt the message by using public key to produce the cipher text.
- It must be easy for recipient B to decrypt that message with private key to recover the original text.
- Determining the private key is not possible for any party even if they know the public keys.
- It should not possible for any opponent to recover the original message by using the public key and cipher text.
- Any one can use any key for encryption whiles other for decryption [40].

RSA and Diffie-Hellman are the two most widely used algorithms for public-key cryptography. RSA is a block cipher and used for encryption as well as signature. Encryption is similar to signature in RSA except that the private key is used for singing while public key is used for verification. Some other algorithms are Digital Signature Standards (DSS) and Elliptic-Curve cryptography (ECC).

5.2.3.3 Key Management

The major weakness in public-key encryption is that public key is public. Thus, anyone can forge such type of public announcement. An intruder could pretend to be user A and can send its public key to any other participant or even can broadcast his public key. The solution is to use public-key certificate; issued by a third party which is called *Certificate Authority* (CA). This authority is trusted by the user community it can be any governmental organization that issues a certificate which consists of public key, user ID of the key owner and at the end whole block is signed by the CA. *X.509* is a standard scheme used in most network security applications for certification.

Chapter 6

SECURITY SOLUTIONS

In this chapter we will discuss different security tools and applications which are widely used nowadays.

6.1 Application Level Solutions

Security solutions at application level further divided for different applications, discussed one by one.

6.1.1 Authentication Level

The verification of any identity called authentication which also verify the integrity of data. If an individual request generated for an operation, without knowledge of that individual it is often difficult to decide that either this operation is allowed or not. Traditional authentication methods are not suitable for computer networks having sensitive data. We will discuss little bit about most important authentication specifications which are currently in use.

6.1.1.1 Kerberos

In traditional networks a user types a password to verify its identity during login phase, this process is called authentication. Password based authentication is not a good solution because passwords sent across the network and any intruder can intercept these password. A strong authentication based cryptography required so that intruder could not gain information that will helpful to impersonate him. The most common example of this type of authentication is *Kerberos*, which is based on conventional encryption. It is a distributed authentication service in which server verifies a user without sending information on network. Developed in mid 80's, currently having two versions V4 and V5. V4 is still running at many sites but V5 is considered as standard. One drawback of Kerberos is that they are not good against the Trojan horse programs and password guessing attack. We will not discuss the procedure that how Kerberos works because it is beyond our scope [41].

6.1.1.2 X.509

It is another authentication protocol based on public-key certificate. The authentication protocols defined in X.509 are widely used, for example in S/MIME, IP Security and in SET. We will discuss theses terms later. As we discussed in previous chapter that there might be a chance that intruder can generate false public keys in public-key infrastructure to avoid this threat we trust on a third party which generate certificates. The Certificate consists of public key of the user, signed by the private key of that trusted party and that party is called Certificate Authority (CA).

6.1.2 Email Level

The most widely used and growing network application across all platforms is electronic mail. We will discuss two schemes that used most for authentication and confidentiality of email.

6.1.2.1 Pretty Good Privacy

PGP is the remarkable effort of a single man Philip R. Zimmermann which Provides confidentiality and authentication service for email and file storage applications. We discussed a lot about conventional encryption which is fast, based on a single key and used for both encryption and decryption. The secrecy of this key is very important and the main problem in conventional encryption is in the distribution of the secret key. This problem was solved by public-key cryptography; we use two keys *public key* for encryption and corresponding *private key* for decryption. Any one can encrypt the data with public key which is published to every one but nobody can decrypt that data except the person who has corresponding private key. It is also not possible to deduce the private key with the help of public key. But infect the problem in dual key encryption is that every one may have a copy of public key. PGP combines the best features of both cryptographic schemes. When a user encrypts a message with PGP it first compresses the message then creates a one time secret key for data encryption, this key is called session-key. Firstly the data is encrypted with this one time session key then session key also encrypt by the recipient's public key. This encrypted session key and cipher text then transmit to the recipient. On recipient's side PGP recovers that session key with the help of private key and this recovered session key then use to decrypt the cipher text. Public key encryption is almost 1000 times faster than public-key encryption. Combination of these two cryptographic schemes makes use of public-key encryption with speed of conventional encryption. The operation of PGP consists of five steps:

1. *Authentication:* when sender creates a message a 160-bit hash code of the message is generated with the help of Secure Hash Algorithm -1 (SHA-1) which is a cryptographic hash function. By using sender's private key this hash code is encrypted with RSA. The receiver then recovers the hash code by decrypting it with the sender's public key. At the end receiver generates a new hash code for the message to compare it with the recovered hash code if both hash codes are same then the message is said to be authentic message.
2. *Confidentiality:* PGP provides the confidentiality by encrypting the message. CAST-128, IDEA and 3DES algorithms are used for encryption. Initially sender generates a message with a 128-bit session key; which is randomly generated only for one time. After this the message is encrypted with IDEA, 3DES or CAST-128 algorithms. Session key is encrypted with RSA using recipient's public key. At the end user recover the session key with its private key and use it to decrypt the message.
3. *Compression:* PGP by default compresses the message after applying the signature but before encryption. The reason for compress the message before encryption is that it is more difficult to get the information from a compressed message. For compression *ZIP* algorithms is used.
4. *E-mail Compatibility:* When PGP used the partial or all resulting block consists of 8-bit octets while many email systems only allow ASCII text. To avoid this PGP uses radix-64 conversion, which expand the message by 33%.
5. *Segmentation and Reassembly:* Emails with maximum message length are restricted. To avoid this restriction PGP break the message that is too large and at the receiver end reassemble the block again [42].

Different reasons of widely used PGP are:

- Available free on variety of platforms.
- Based on well known cryptographic algorithms.
- Developed by a single person that's why not governed by any standard organization.

6.1.2.2 Secure/Multipurpose Internet Mail Extension (S/MIME)

We already have discussed SNMP in detail in chapter 2 that it is a simple mail transfer protocol which sends messages in 7-bit ASCII format. MIME was defined to accommodate the non-ASCII data. In fact MIME is not a mail transfer protocol it is only an extension of SMTP and a supplementary protocol that allows non-ASCII data to be sent through SMTP. Any email message consists of two parts, header and the body. Header has the information that helps in message transmission while body format is normally unstructured. MIME permits emails to attach sound, picture and enhanced text hence MIME defines that how the body part of message can be structured. MIME itself has no security services. S/MIME provides security for MIME data by sign the data and by use of public-key encryption. It provides authentication of data by using digital signature and integrity of data by encryption. Both PGP and S/MIME are on IETF standard but S/MIME emerges as an industrial standard.

6.1.3 IP Level

Applying security on IP level can ensure the secure communication for the applications that has security mechanism also for the security ignorant applications.

6.1.3.1 Internet Protocol Security (IPSec)

IPSec is not a single protocol. It is a general framework by using a set of algorithms it allows different entities to communicate securely with each other. It provides encryption and authentication to all traffic at IP level with the help of strong cryptography. Authentication and encapsulation are two basics of IPSec. Two protocols that provide authentication and encapsulation are Authentication Header (AH) and Encapsulation Security Payload (ESP). These two protocols used in combination or alone to provide a desired set of security services for the IP layer. Figure 6.1 shows the document overview of IPSec.

- *Architecture:* It covers the general security requirements and the processes defined in IPSec.
- *ESP*: It covers the packet format and issues related with the use of ESP for packet encryption and optionally authentication.
- *AH:* It covers the packet format and issues that how the AH use for packet authentication.
- *Encryption Algorithm:* It covers that how the set of encryption algorithms used for ESP.
- *Authentication Algorithm:* It covers that how the set of authentication algorithms used for AH and optionally for ESP authentication.
- *Domain of Interpretation (DOI):* The values which are required for the other documents to relate with each other are covered by DOI.
- *Key Management:* It describes the key management schemes. Oaklay and ISAKMP is an example of two schemes.

Another fundamental part of IPSec is *Security Association (SA).* It is a one way relationship between sender and receiver that is responsible for security services and to the data carried on it.

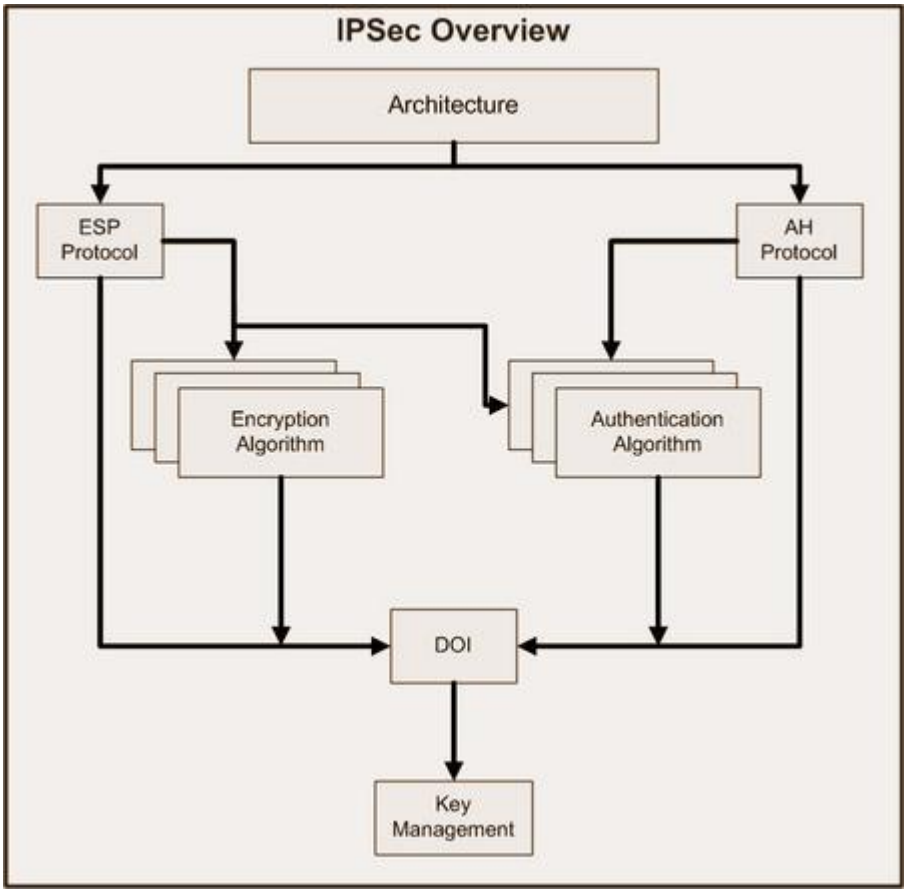

Figure 6.1 IPSec Document Overview

It make by the use of either ESP or AH. If we want to apply both AH and ESP protection on a traffic stream then we need two SAs. *Transport mode* and *Tunnel mode* are two types of SAs which provides different types of protection to data. In transport mode protection provides to only upper-level protocols like TCP, UDP or ICMP while entire IP packet is protected in tunnel mode. (described below in table 6.1).

IPSec provides secure communication across entire internet, LAN and across public and private WAN. Remote access over internet, connectivity of branch offices over internet and enhancement of electronic commerce security are some of the examples of IPSec. Thus we can say that the principal feature of IPSec is to provide security of all distributed applications like data transfer, remote login, web access and email.

6.1.4 Web Level

Web is visible for everyone, most of the users are not aware of the risks. Browser side risks, wrong configuration in web servers are some types of risk that helps intruders to unauthorized remote access and interception of data which sent form client/server to browser and browser to

	Transport Mode SA	Tunnel Mode SA
AH	Authentication provide to IP Payload and selected portion of IP header and IPv6 Extension header	Authenticate the entire inner IP Packet plus selected portion of outer IP header
ESP	Encrypt IP Payload and any IPv6 extension header	Encrypt inner IP packet.
ESP with authentication	Encrypt IP Payload and any IPv6 extension header. Authenticate IP payload but no IP header.	Encrypt and authenticate inner IP packet

Table VI.I

client/server. We will discuss two standardized schemes Secure Socket Layer (SSL)/Transport Layer Security (TLS) and Secure Electronic Transaction (SET) that are used for web security.

6.1.4.1 SSL/TLS

Various approaches are used for web security and they have different scope of applicability with corresponding location in TCP/IP protocol suite. One way is to provide web security at IP layer level which we already discussed earlier. One advantage of using IPSec is that it is transparent to end users and we can filter the traffic. Another solution is that to provide security just above TCP (see figure 6.2). SSL is one of the most commonly used security mechanism available on Internet. Like other security protocols SSL is also based on cryptography. After SSLv3, Internet Engineering Task Force (IETF) renamed it as TLS which now considered as standard. TLS is almost same like SSLv3. SSL/TLS encrypt the data at transport layer. Instead of HTTP normal port 80, SSL comes up with a special URL identity "HTTPS" which uses port 443 to establish a secure SSL session. SSL supported browsers are used mostly for sensitive data like credit card information. TLS provides end to end authentication and then secure communication using cryptography. SSL protocol runs above TCP/IP and follow these steps:

1. With the help of public-key cryptography, clients check the server certificate that it is issued by a trusted Certificate Authority? (CA).
2. Same technique repeated for server it check the client's certificate and public ID that it is issued by a trusted Certificate Authority.? For example if banks send information to you it will also check your identity.
3. Using public-key cryptographic technique an SSL encrypted connection established between server and client.

SSL protocol further consists of two sub protocols. *SSL Record Protocol and SSL Handshake Protocol* (Figure 6.3 describe SSL protocol stack). SSL record protocol describes the format used to transmit data. The most complex part of SSL is handshake protocol that allows server and client to authenticate each other and by using SSL record protocol transfer the data between SSL enabled server and client.
TLS/SSL authenticates to both communication parties (servers and clients) and provide data integrity, that's why can helpful against replay attack, man-in-the middle attack and masquerade attacks.

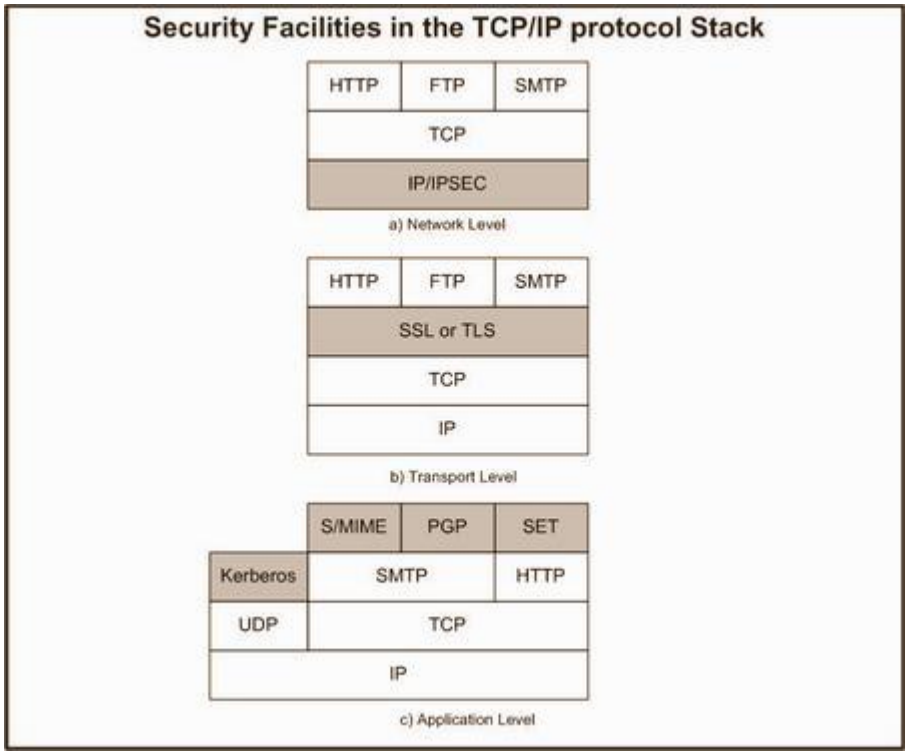

Figure 6.2

6.1.4.2 Secure Electronic Transaction

As the name suggest Secure Electronic Transaction (SET) is a security protocol designed for protecting credit cards transactions over internet. Developed by VISA and MasterCard and some other big companies involve are IBM, Microsoft etc. The goal of SET is to authenticate buyer and merchant identity and then confidential transaction. Figure 6.4 shows the SET participants.

SET uses different technologies for authentication and encryption. For confidentiality of information and integrity of data DES and RSA used with SHA-1 hash codes, X.509v3 certificate used for authentication of card holder account and merchant account. Privacy achieve through dual signatures. The reason of using dual signature is that in SET transaction there are two recipients involve one is merchant and other is bank. Customer sends order information to merchant and payment information to the bank for these two signatures are used, one signature is for merchant and one is for bank. The key features of SET are

1. Using DES algorithm it provides confidentiality of data even prevent merchant to learn the cardholder's detail.
2. RSA digital signatures with the use of SHA-1 hash codes provides integrity of data which secure the payment information, personal data and order information that send from cardholder to merchant.

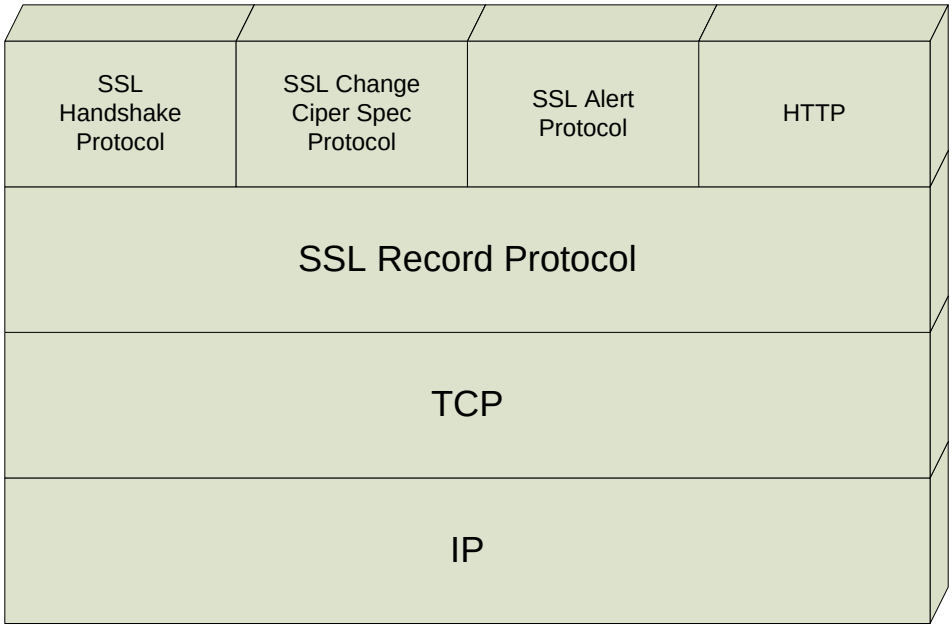

Figure 6.3 SSL Protocol Stack

3. Using X.509 certificates it authenticates cardholder account and merchant account.

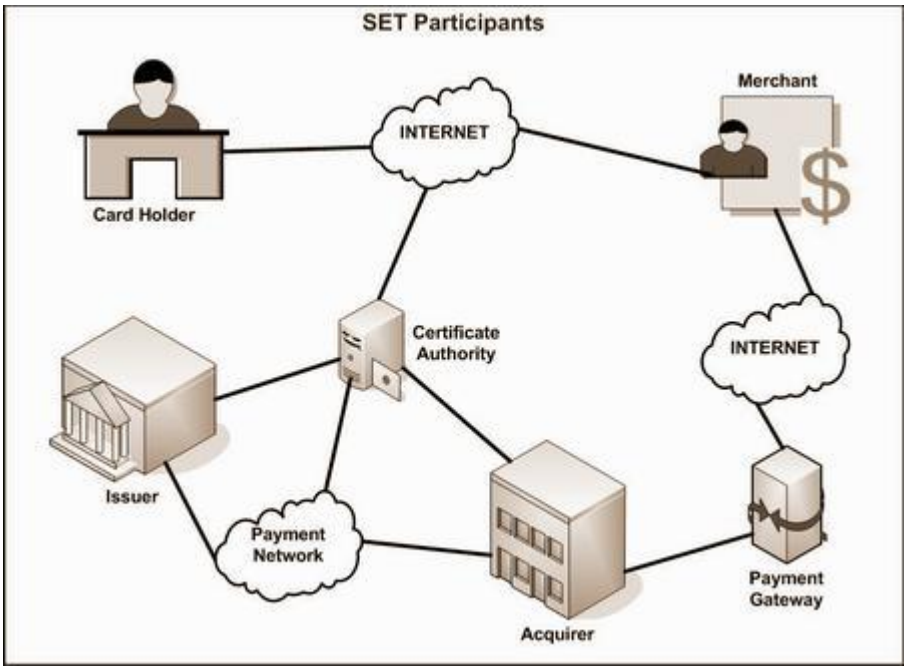

Figure 6.4 SET Participants

6.2 System Level Solutions

On the basis of the security countermeasure techniques and tools, we proposed different security solutions. These security solutions are further dived into two main categories, application level security solutions and system level security solutions. Due to differentiation of user base and software base trespasses, system level security solutions are further divided into IDS, IPS, antivirus applications and firewalls.

6.2.1 Intrusion Detection System (IDS)

The IDS is the system which detects any unauthorized access or intrusion in a system or network. It is a security solution which has a passive position in a system or network against these intrusions. In a network deployment the function of the IDS is to monitor the traffic or network activity without impacting the traffic [43]. It means that an IDS in a network only detects or identifies any changes in network but does not perform a resistive action against such changes.

These customize rule based IDS are fixed by network/system administrator on the basis of previous behavior of the network.
The IDS system uses two approaches for notification of intrusion in a network [44].

- **Statistical detection**
  It depends on the statistical behavior of the network; the statistical detection approach has further division into two sub categories.

  - *Threshold detection*
    In threshold detection, the IDS can monitor the number of established connections in a specific time or the number of new user requests for a specific application that runs on a network.

  - *Profile based detection*
    In profile based detection, the IDS system monitors the behavior of a user at different time slots. It monitors the user login/logoff session times on the network also counts the number of password failure attempts by user in short time intervals.

- **Rule based detection**

  Rule based intrusion detection system performs the activity, if any change is found in the rules of proper network flow. It is also important because it works on customized settings of the network assigned by the network/system administrators.

Classifications:

The IDS security solutions are further classified into three main categories [45].

1) Network based intrusion detection system (NIDS)
2) Host based intrusion detection system (HIDS)
3) Distributed intrusion detection system (DIDS)

Network based intrusion detection system (NIDS)

Network based intrusion detection system works in a network. It monitors all the network traffic especially at hardware layer based traffic. The communication and working functionality of hardware layers in TCP/IP suite are already discussed in chapter two, like in link layer,

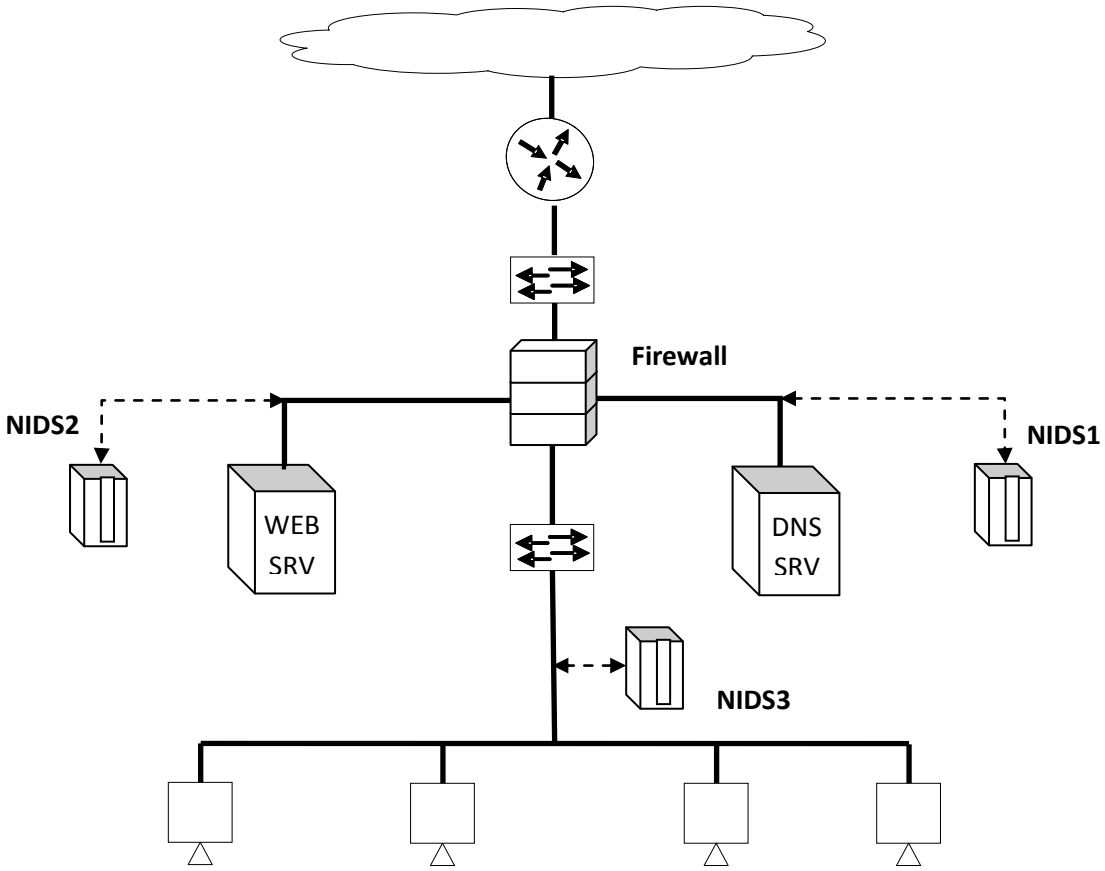

Fig 6.1: NIDS Based Network

hardware interface card can communicate with another system via communication medium through hardware address (MAC address).

Consider the working functionality of NIC is that first it generates an ICMP request for acquiring a physical address (IP address). This request is broadcast on network. Some time NIC gets bulk of ICMP requests which can create a chance of network congestion situation. NIDS monitors all the same types of intrusions with appropriate NICs and creates a log file. Similarly NIDS has a feature to monitor all the network switches communication, if it observes any network intrusion through these switches then it makes a report. NIDS connects to network via any port of network switch. (See fig 6.1) [45].

Host Based Intrusion detection system (HIDS)

The role and placement of Host based IDS is slightly different from NIDS. Host-based intrusion detection system is deployed only on a local machine or system. It is responsible to monitor local system based activities or intrusions i.e. CPU performance, file sharing resources and functionality of system applications like web-server application and mail-service. (see fig 6.2) [45]

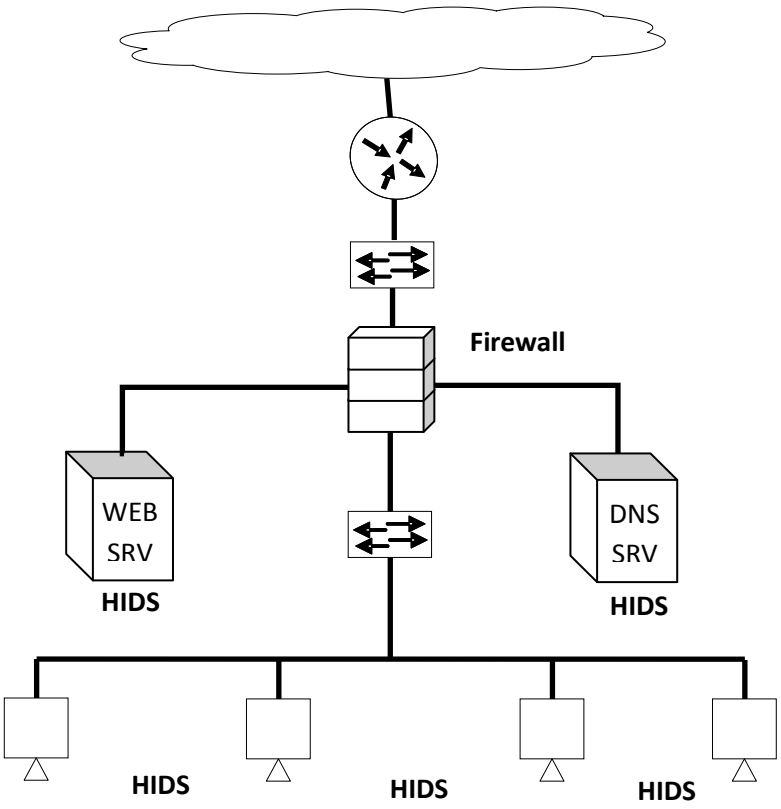

Fig 6.2: HIDS Based Network

Distributed intrusion detection system (DIDS)

In DIDS there is one central control machine that performs a role of administrator or manager and all remaining IDS systems behave like clients. These IDS client machines normally called IDS-sensors. All these IDS sensors can detect the intrusions in the network or system and send a report to the main IDS manager.

These IDS-sensors are in the form of NIDS, HIDS or both. So we can say that the DIDS is a combination of both NIDS and HIDS systems. The one main feature of DIDS system is that all IDS sensors send their reports of network and local system based intrusions to the IDS manager and an IDS manager is responsible to update its IDS sensor patches or signature database against new bugs and intrusions that occurs in the network. (See fig 6.3)[45]

6.2.2 Intrusion Prevention System (IPS)

The intrusion Prevention System performs a role of protection against intrusions that occurs in a network or local system. It works on the basis of output of IDS system log files. Due to this reason we can say that the IPS system is an extension of the IDS system.
But there are some differences between IDS and IPS. IDS system works in a passive mode, i.e. it only has the ability to detect any intrusion in the network, whereas an IPS works in an active mode. An IPS performs action when it founds any packet dropping or unauthorized connection. [46][47]

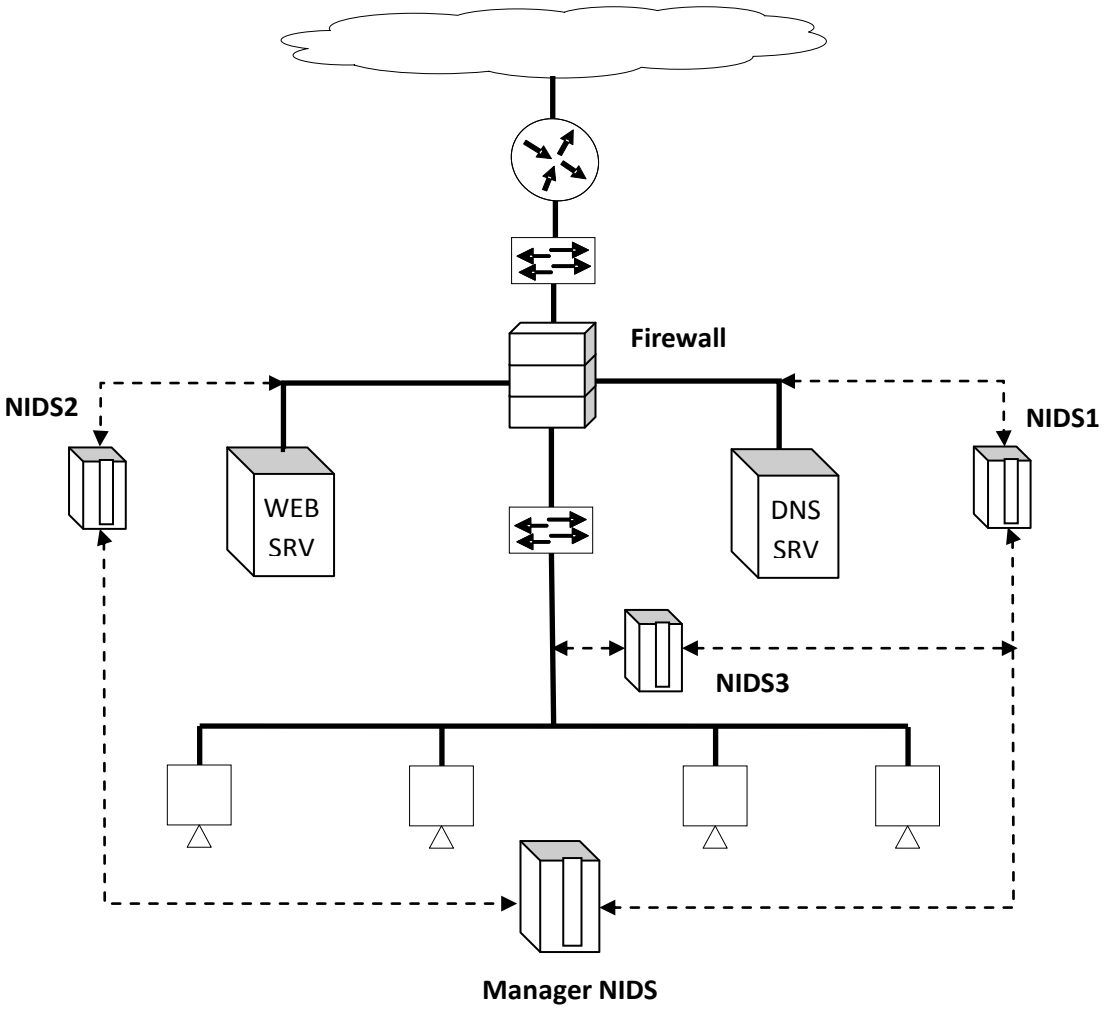

Fig 6.3: DIDS Based Network

Functions of an IPS system are same as of an IDS system. It may work as a standalone machine or system known as Network Based Intrusion Protection System (NIPS) that have the ability to block or deny any unauthorized interruption that occurs in the network. Or it may perform a role with an existing system or operating system known as Host Based Intrusion Protection System (HIPS). HIPS protect and deny local unauthorized activities, like high utilization of CPU from any type of service and movement of local system files within the system or to another system.

As per functionality of an IPS system, we can say that a router access control list or firewall rules might be consider a basic IPS system [46] and similarly the combination of blocking capability of a firewall and deep packet inspection through an IDS system is known as an intrusion prevention system. [48].

6.2.3 Antivirus Techniques

Antivirus techniques are already explained in chapter 5, there are number of malicious applications/softwares which perform harmful activities within a local system or on network.

These applications can be in the form of different "viruses" which may infect or modify the system files or applications, or can be in the form of "worms" that may create their own replicas in a system and utilize the vacant space in system.
Some of these applications perform their role only on local system or some of them travel from one machine to other machine through network resources or other medium like usb's and floppies.

For protection from these types of malicious applications we use antivirus techniques on our network or system known as antivirus applications.

The functional architecture of an antivirus technique can be followed up in the given below sequence of operations [44].

Detection
The first step of an antivirus application is that it has the ability to detect the occurrence of a virus or other malicious program in system application or in data file.

Identification
After detection function the second step of an antivirus is that it has the ability to identify the type of virus with its malicious aims.

Removal
The virus removal is the last step of an antivirus application.

Antivirus Functional Techniques

There are many functional techniques used by antivirus applications for detection, identification and finally removal of viruses from a system or a network. Some of these important techniques are: [44] [48].

Generic Decryption (GD)

The generic decryption is an antivirus technique designed for the polymorphic type of viruses. The architecture of polymorphic virus is described in chapter 5. Polymorphic virus contains total encryption architecture. It contains an encrypted virus signature as well as an encrypted key in its internal body; whereas it has an outer body cover which is also encrypted. The outer cover decrypt by its internal key. So it is very complicated to detect the virus signature through a simple antivirus.

The generic decryption antivirus technique has the ability to detect and clean the type of viruses which have polymorphic architecture. It followed some steps described below [44]

- ✓ Generic decryption technique first generates a virtual machine into a real machine. This virtual machine has complete hardware and applications same like in actual machine.

- ✓ In the process of scanning or diagnosing, system and data files are placed in virtual machine one by one.

- ✓ If the polymorphic virus exists in any placed file, then polymorphic virus performs act to this filefirst it decrypt is outer cover body by its own internal key.

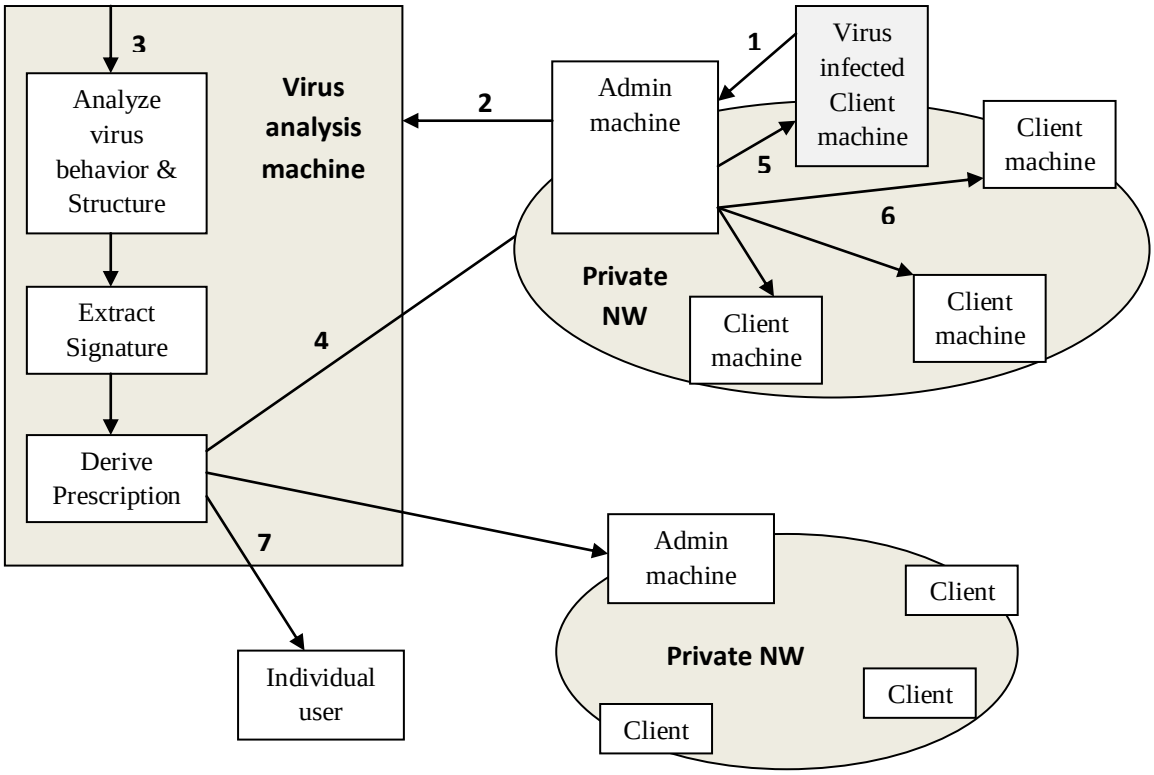

Fig 6.4: Digital Immune System

- ✓ As it decrypt its own outer body. It has opened its internal structure, specially its virus signature, in front of any generic decryption antivirus, And then generic decryption antivirus can easily removed this virus from this file.

This process occurs only in virtual machine that is created by generic decryption antivirus; this virtual machine is also totally isolated to actual machine and its applications. In this way polymorphic virus does not have an effect on the actual machine at the time of its operation.

Digital Immune System

A digital immune system or digital immune antivirus is a technique that provides a protection against those types of viruses which have the characteristics to spreading from one computer to other computer through a network. Normally "*worm*" is considered such type of virus.
Digital immune system has its own scanner elements on every client machine in a network; these scanner elements first detect such type of viruses on local client machine, then the scanner client machine sends this information to the main administrator machine, which is also a part of the same network. Administrator machine collect the information and send it to virus analysis machine.

The virus analysis machine may exist on same network or may be on wide area network. The virus analysis machine has some working blocks in its architecture.

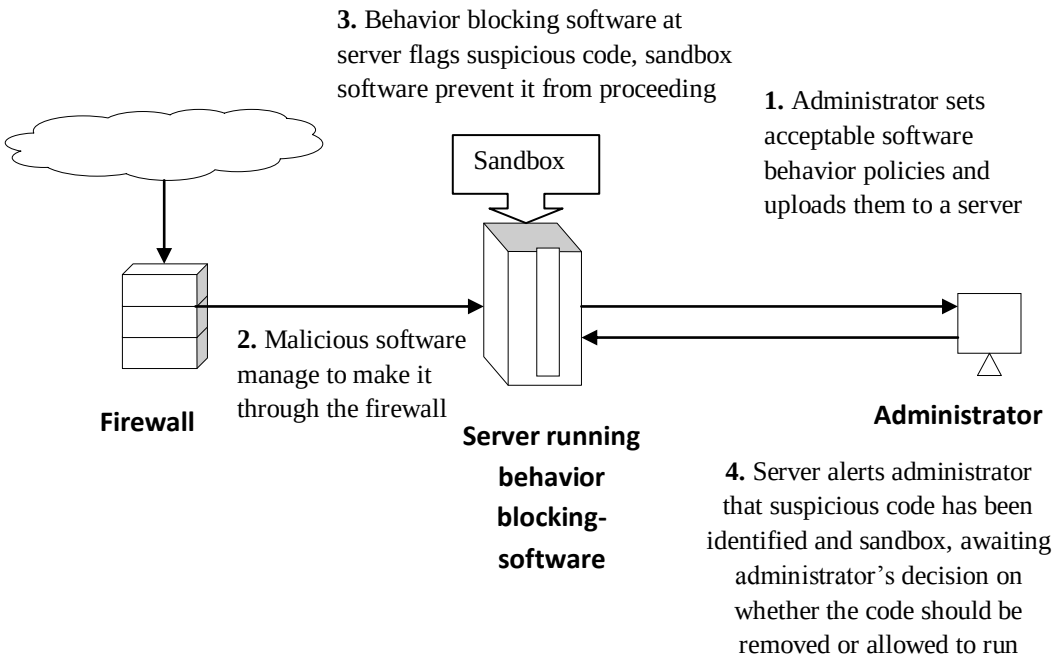

Fig 6.5: Behavior Blocking Software Operation

- *1st block; this block is isolated with other blocks. It is used to detect the virus and read out its structure, i.e. virus type.*
- *2nd block; it detects virus signature.*
- *3rd block; this is the last block of virus analysis machine, it removes the viruses form the infected files.*

After removing viruses from that file, virus analysis machine sends this information to the whole network clients. All network clients update this virus signature information in their databases. A digital immune system is very efficient to detect and remove such type of viruses which spread over the network. (Fig 6.4) [44]

Behavior Blocking Software

The behavior blocking antivirus software integrates with the operating system of a host computer and monitors program's *behavior* in real time [50]. This application runs on both, server and clients but the main protection is done by the server side.

The behavior blocking system can monitor the system files with operating system's behavior. So if any changes occur in system files it detects and send a report to the administrator and wait for an action from the administrator. Updating the main server is the responsibility of administrator. (See fig 6.5)[44].

6.2.4 Firewalls

A firewall is a barrier which performs isolation between two different networks or systems. It decides that which kind of traffic can pass through a network and in which direction. Firewalls

provides an additional level of defense system providing the capabilities to add much tighter and more complex rules of communication between different network segments or zones [43].

A firewall may contain only one system or it may consist of more than one system. The role of firewall is to provide protection of one network from other network. The connection architecture of a firewall in a network is that it creates a barrier between two networks. For this it must have at least two network interfaces one for the network which is intended to protect and other for the network that is exposed to [51]. Simply a firewall protects the internal network from external network.

Considering the connection architecture of a firewall there are some important points to discuss.

- ✓ Physically firewall is connected with two or more than two networks through its interfaces, so that all incoming and outgoing traffic has a single point for communication. Therefore all traffic must pass through firewall for communication purpose from one direction to another direction.

- ✓ The second point is that only authorized traffic is passed through firewall, either traffic is coming in to the network or going out from the network. All incoming or outgoing traffic must fulfill the security measures that define in a firewall as rules.

Characteristics Parameters:

A firewall follows below parameters [44].

- *Service control*

A firewall controls those services that want to pass through the firewall. It also controls the communication services which have some additional functional parameters, like source/destination IP addresses with their specific ports and type of protocols.

- *Direction control*

A firewall controls those services, which has rights of communication. Means firewall can restrict incoming traffic to come inside the network and can restrict the outgoing traffic to go outside the network or may be allowed to both type of traffic.

- *User control*

It can assign that which user can access to which services. These users can be either from the local network or from the outer world.

- *Behavior control*

With the help of a firewall administrators can control the working behavior of a service and a user. They can assign that a user either have full access rights on a service or on a system, or partial access rights to that particular service or system. At the same time firewall can decide that the same user is not allowed to access other parts of that particular service or system.

Types of firewall:

There are many types of firewalls. Administrators have to decide that which type of firewall is right for a given control architecture [43]. However firewalls can be divided into four categories [44][52].

1) Packet filter firewall
2) Application gateway
3) Circuit level gateway
4) Stateful filter firewall

Packet Filter Firewall

A packet filter firewall monitors all incoming and outgoing network based packets. It allows or denies packet to pass through one network to another network. It checks the packet parameters and compares them with its own tables that contains packet parameters after that a packet filter firewall decides to allow or deny the packet.
The packet parameter field normally contains, source/destination IP address, source/destination services ports, types of packets (either TCP or UDP) and information flags that notify the purpose of packet.

Due to its packet filtering functionality, it may allow specific packets form specific interfaces for communication. This rule can be implemented for both inside and outside traffic. Packet filter firewall is easy to implement and does not require a high level of configuration in a standard network. It is also known as first generation level firewall [52].
A packet filter can remove the bug which exists in TCP (three way handshake) communication, which a hacker can as a SNY flood attack.

For detection and protection against a SYN flood attack we can use a packet filter firewall in a TCP interception mode (See fig 6.6) [53].In TCP interception mode a packet filter firewall catches the TCP request "*SYN"* flag packet from outside the network, which is coming toward a targeted server for establishing a TCP (three way handshakes) connection from an unidentified user. Firewalls do not allow this packet before identification of user. So firewall sends a "*SYN-ACK*" flag packet to the user. If there is a valid user then it sends an "*ACK*" flag packet to the firewall. This confirms the validity of user so now packet filter firewall sends request to server to establish a TCP connection otherwise discards the first "*SYN"* flag packet request.

Application Level Gateway

An application level firewall provides more shelter and reliability than a typical packet filter firewall. Application level firewall works on application level and they can better analyze the traffic at application layer. It provides a client-server network environment. All hosts that want to communicate with outside the world use the firewall as a gateway, hosts are considered as client while the application level firewall performs as a server. So we can say that an application level firewall is also an application level gateway.
Since all traffic must pass through the firewall so it has full command on authentication and authorization of data traffic. It filters the traffic at very high level that's why it provides a high level of security.

Stateful Inspection Firewall

A stateful inspection firewall is a combination of multiple firewalls, especially with packet filter firewall and application level gateway. It scans the packets at network level and read packet content at application level. It provides more security and is called 3rd generation level firewall [52].

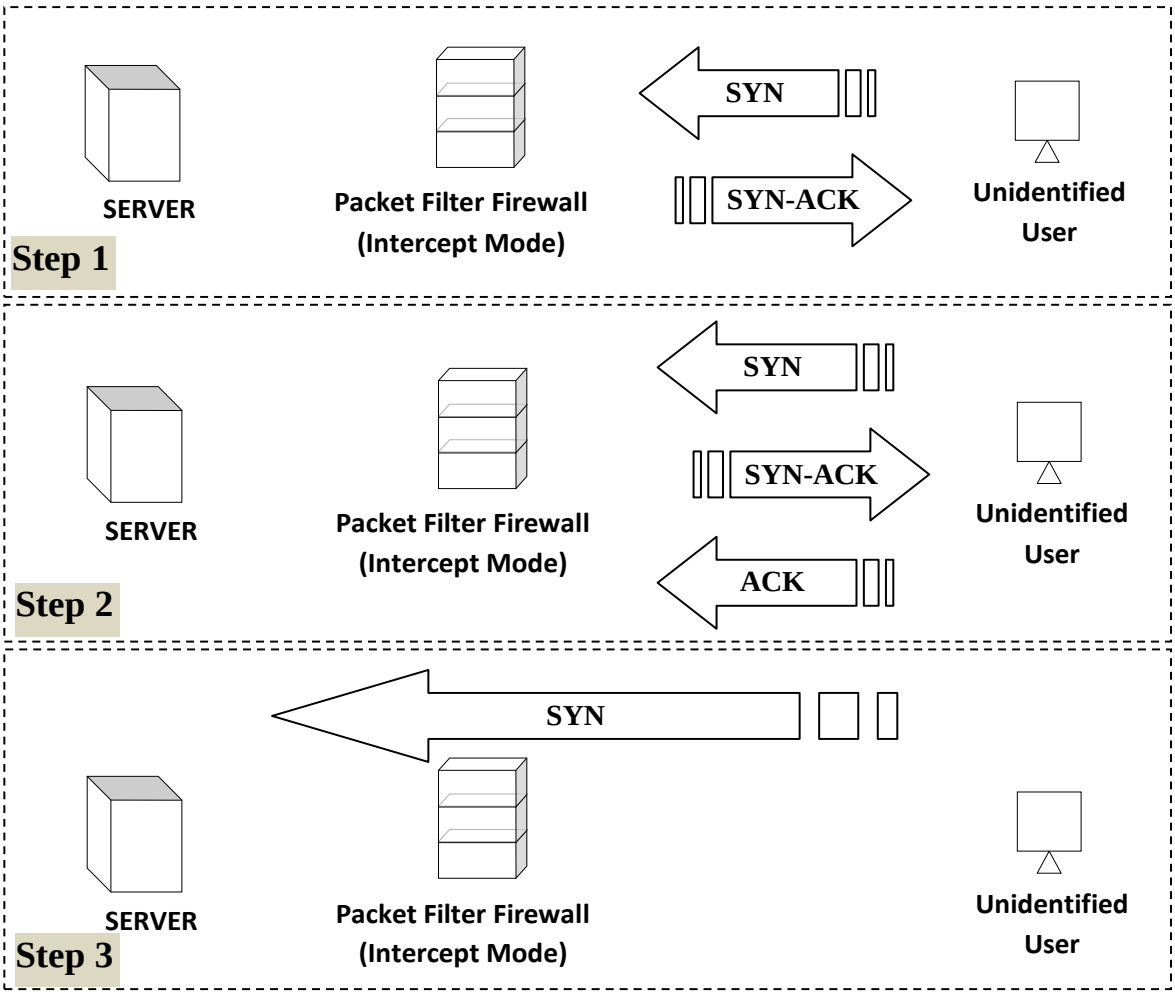

Fig 6.6: Packet Filter Firewall in TCP Intercept Mode

Chapter 7

SIMULATION / TESTING RESULTS

OPNET Modeler

OPNET provides several modules which contain the behavioral response of network protocols, it also have the characteristics of network hardware elements. These given simulator modules in OPNET, are helpful to generate and establish a real-life time network environment within a lab. The configuration and results outcomes of the network element behavior are very close to a real network environment. GUI based test configuration scenarios and their graphical outcome results are the bonus features, which are acquired by an OPNET simulator [55], [56].

7.1 Overview

As detail study of the network elements "*hardware & Protocols*", we can find out the existence network vulnerabilities, which can be examined by design and implementation of a real network in a lab through OPNET Modeler 14.5.

7.2 Goal

The objective of our simulation is, to analyze and differentiate the level of security, by deployed divergent user's level authorities against specific applications and/or resources, through different mind approaches network/system admins. We will also analyze the background effects after deployment of security in a network environment.

7.3 Scenario

Simulation consists of three scenarios, these test scenarios, depend on exhaustively functional and strong working awareness about network parameters and its modules "*hardware and protocol"*. These are following.

1- **General Network Scenario;** use *"default mode"* setting of network parameters.
2- **Firewall Network Scenario;** use a *"well approached"*, deployed security through existence hardware based security module. But after deploying security, it loses some specific client→Server connection against particular application.
3- **VPN-with-Firewall Network Scenario;** an "*intelligent approach"* mind network admin, use the given network parameters in proper way and establish a customized network solution which can provide the specific network resources availability to a specific & authorized client in proper way, which is a secure and smooth flow network requirement.
   It may fulfill the security of network and provide the availability of resources in required manner.

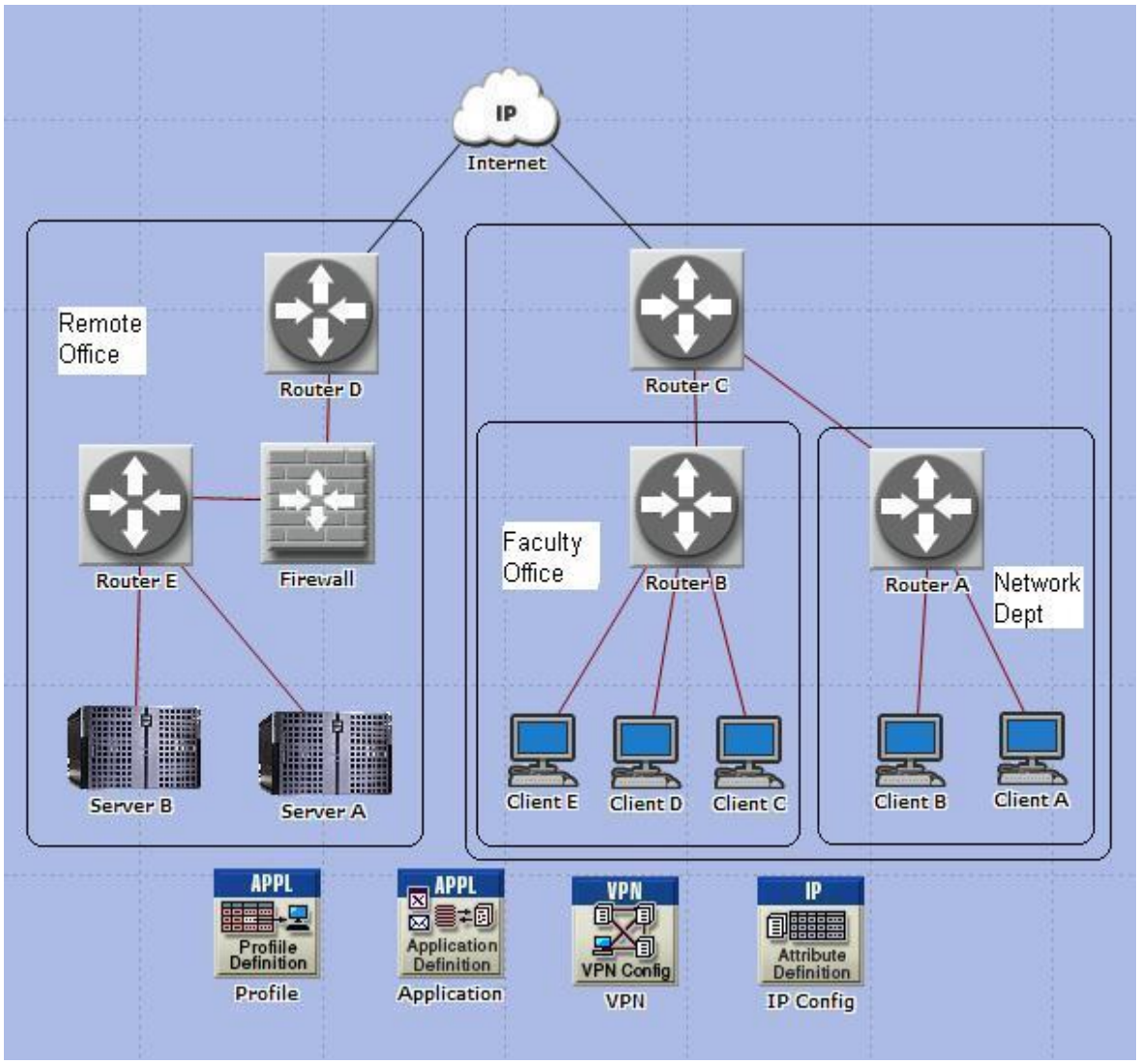

Fig 7.1 Network Scenario

7.4 Object Modules

The objective modules that are used in our simulation model are given, in table 7.1.

TABLE 7.1: Object Modules

S/No	Object Name	Object Model	Qty	Object Module Description
1	Application	Application Config		Default Support (Database Access, Email, File Transfer FTP, File Print, File Transfer FTP, Video Conferencing, VOIP, Web Browsing HTTP)
2	Profile	Profile Config		Sample Profile (Engineer, Researcher, E-commerce customer, Sales Person, Multimedia Users) Engineer (Web Browsing HTTP, Email, File Transfer FTP, File Transfer FTP)
3	VPN	IP VPN Config	01	Support VPN tunneling establishment between specific end routers
4	IP Config	IP Attributes Config	01	
5	Internet	IP32_cloud	01	Internet Cloud
6	Router (A,B,C,D,E)	Ethernet4_slip8_gtwy	05	IP based Gateway Router, support VPN connection.
7	Firewall	Ethernet2_slip8_firewall	01	Packet filter Firewall, allow and deny specific application through firewall across the two different network
8	Client (A,B,C,D,E)	Ethernet_wrkstan	05	Simple client machines
9	Server (A,B)	Linux_Server	02	Linux based server machines
10	Link	PPP_DS3		PPP connection (44Mbps)
11	Link	100BaseT		Ethernet connection (100Mbps)

7.5 Applications/Services

- In Client HTTP: Traffic Received (bytes/sec)
- In Client FTP: Traffic Sent (bytes/sec)

7.6 Task Assignments

The task assignment through simulation is described in table 7.2.

TABLE 7.2: Task Assignment

S/ No	Client Title	Section/ Deptt.	Job Description	Authorization Permission; Access/Deny Level
1	Client A	Network	Network/System Administrator	• Permit: (HTTP traffic) *Download/Access http traffic form server* • Permit: (FTP Connection) *Upload/Established FTP connection to sever*
2	Client B	Network	Network Assistant	• Permit: (HTTP traffic) *Download/Access http traffic form server* • Deny:(FTP connection) *Upload/Established FTP connection to sever*
3	Client C	Faculty	Faculty Member A	• Permit: (HTTP traffic) *Download/Access http traffic form server* • Deny: (FTP Connection) *Upload/Established FTP connection to sever*
4	Client D	Faculty	Faculty Member B	• Permit: (HTTP traffic) *Download/Access http traffic form server* • Deny: (FTP Connection) *Upload/Established FTP connection to sever*
5	Client E	Faculty	Faculty Member C	• Permit: (HTTP traffic) *Download/Access http traffic form server* • Deny: (FTP Connection) *Upload/Established FTP connection to sever*

7.7 Object Modeling

Set the object parameters as per given task assignment. i.e. in *"Application config",* object attributes has *default* supported; (Database Access, Email, File Transfer FTP, File Print, File Transfer FTP, Video Conferencing, VOIP, Web Browsing HTTP) applications. Similarly in *"Profile Config"* object attribute has *Sample Profile* (Engineer, Researcher, E-commerce customer, Sales Person, Multimedia Users) and furthermore in "*Engineer"* profile supported; (Web Browsing HTTP, Email, File Transfer FTP, File Transfer FTP), which will fulfills our experiment requirements. On the other hand we set the attributes of all clients machine, application servers attributes, router and firewall attributes as per our requirements. The object attribute are fixed according to table 7.1 descriptions, which are also explained in fig 7.2.

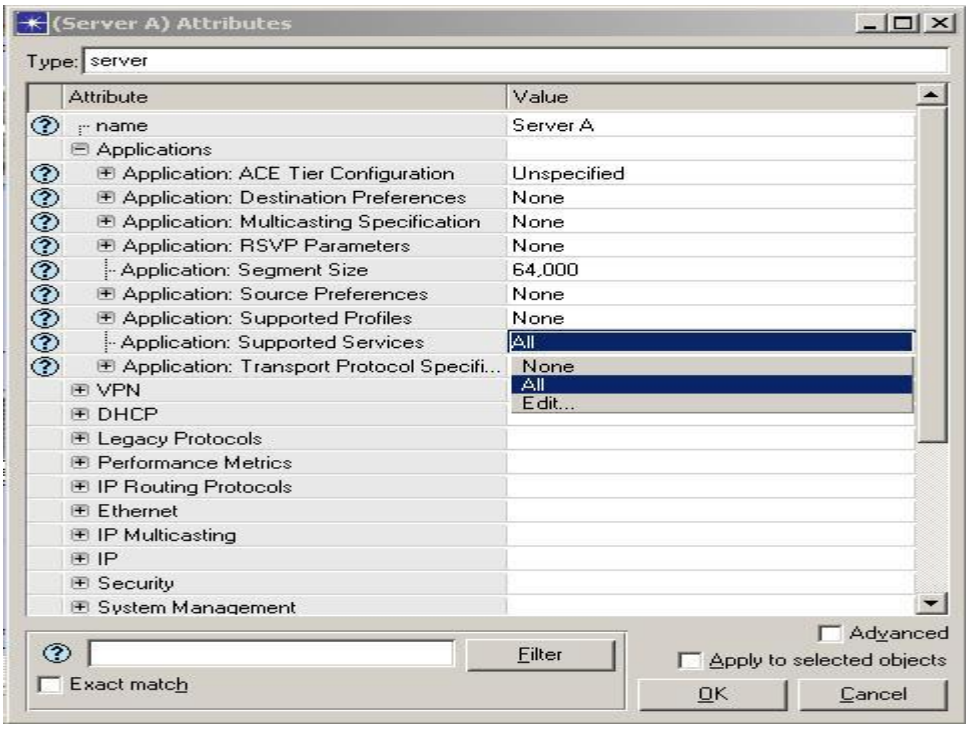

Fig 7.2 Server Attributes

7.8 Results

Results obtained from the simulation scenarios are explained as under.

7.8.1 General Network

(Use *"default mode"* configuration in network parameters)

Here all network clients, Client A; *"Network/System Admin"* Client B; *"Network Assistant"* Clients (C,D,E); *"Faculty Members"* can access HTTP traffic from server as shown in fig 7.5. In *"default mode"* configuration, they have the same access right to establish a FTP connection with the server for uploading any record/data to the server, or update server database through any client as shown in fig 7.3, 7.4. It is a big drawback or weakness in existing network (in default mode); resources availability of unauthorized user. Because it makes vulnerable attack in the form of any Client (B.C.D & E.). It is clear by simulation results in Fig 7.3, 7.4, 7.5.

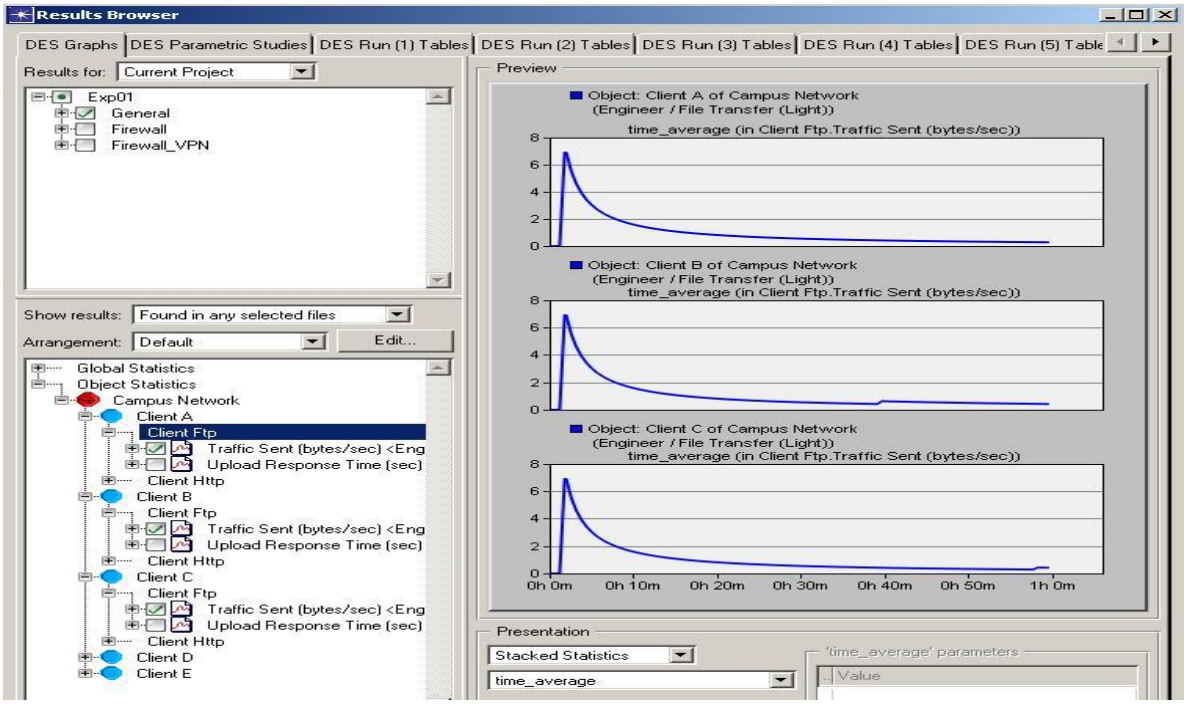

Fig 7.3: General Network (Default Mode)

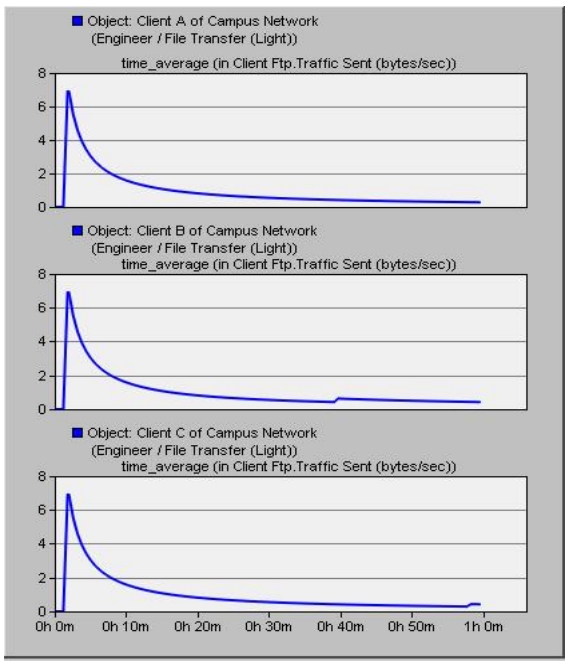

Fig 7.4: General Network *(ftp traffic)*

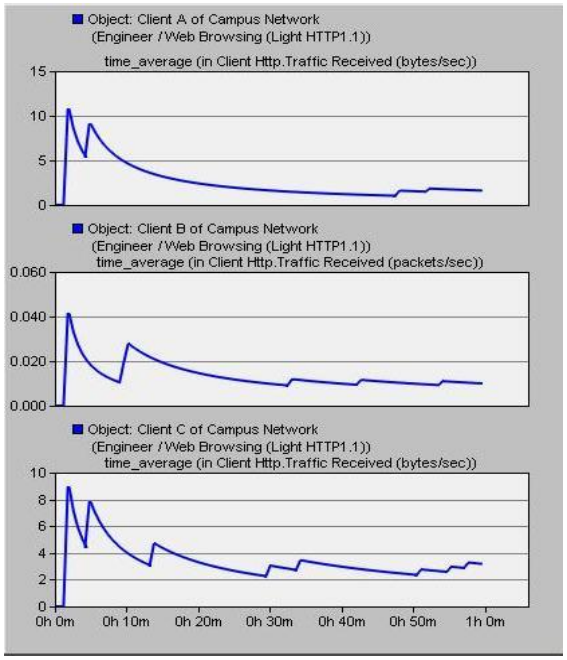

Fig 7.5: General Network *(http traffic)*

7.8.2 Firewall Based Network

(Use existing security module "Firewall", block specific application services)
Deny "FTP-connection" through firewall across two different networks.

Here all network clients, Client A; *"Network/System Admin"* Client B; *"Network Assistant"* Clients (C,D,E); *"Faculty Members"* can access HTTP traffic from server. At the same time they all lose access right to establish FTP connection with the server. This is a good thing which fulfills our one requirement, but as per network requirement, we also want access rights to establish a FTP connection with server for uploading any record/data to server, or update server database through only one specific Client A; "*Network/System Admin*". But after implementation above states network policy, we also lose the right of Client A. It is clear by simulation results in fig 7.6, 7.7.

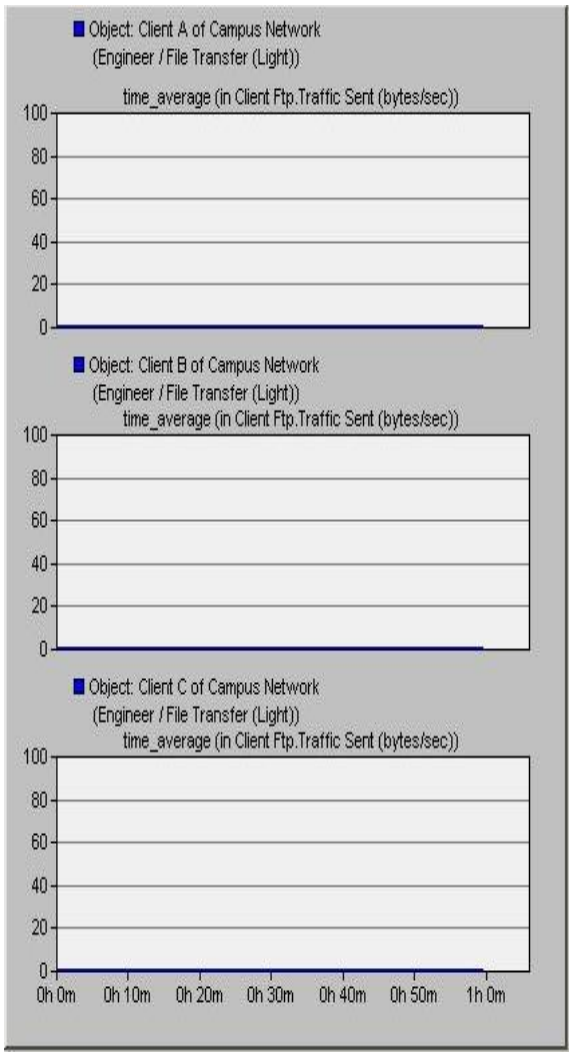

Fig 7.6: Firewall Based Network *(ftp traffic)*

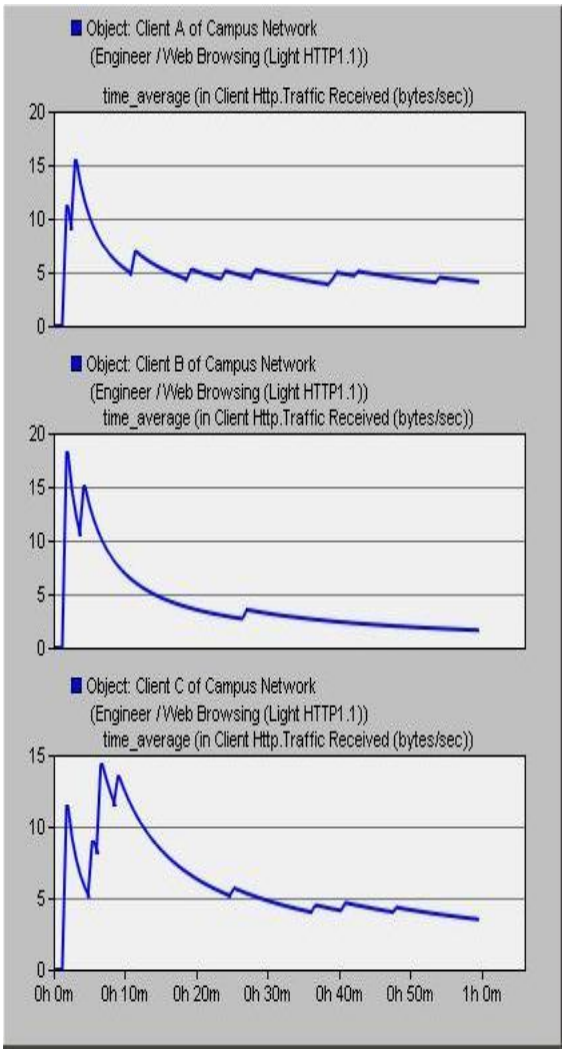

Fig 7.7 Firewall Based Network *(http traffic)*

7.8.3 VPN-with-Firewall

(Use exhaustively hardware functional and an expert network awareness approach)
Configure network parameters as per customized working requirement

Here all network clients, Client A; *"Network/System Admin"* Client B; *"Network Assistant"* Clients (C,D,E) *"Faculty Members"* can access HTTP traffic from server, but they all restricted to have any access rights to establish FTP connection with server, excluding Client A; *"Network/System Admin"*. It is a highly good approach which fulfills our all requirements that were required in task assignment table 7.2. It is shown by simulator results in fig 7.8, 7.9.

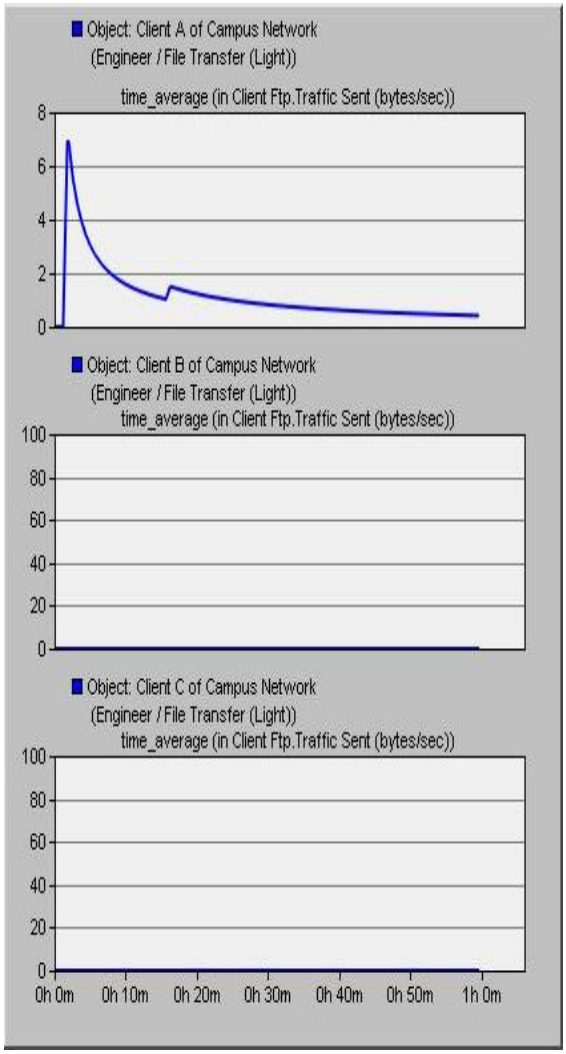

Fig 7.8: VPN Network with FW *(ftp traffic)*

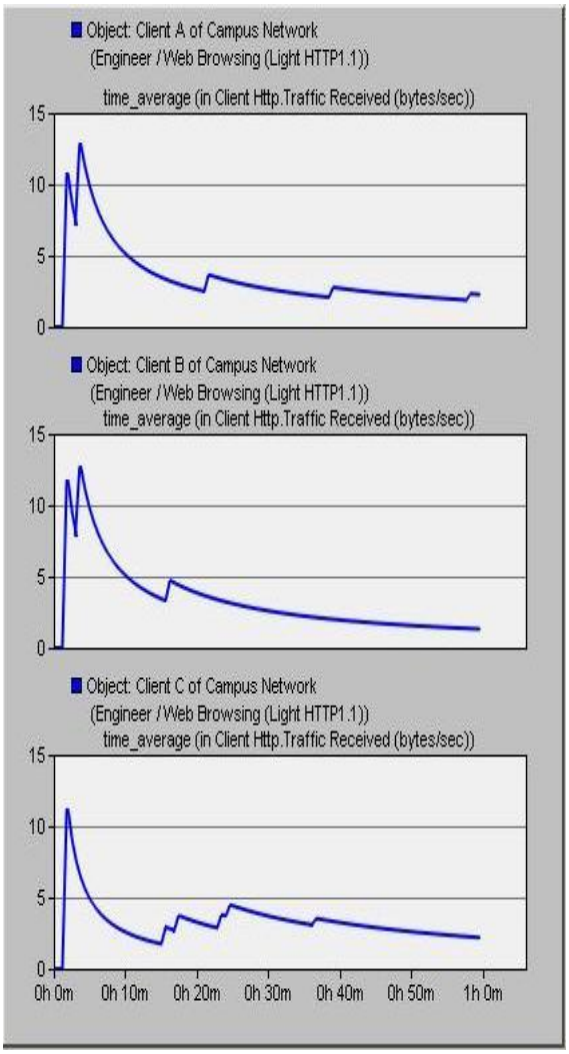

Fig 7.9: VPN Network with FW *(http traffic)*

7.8.4 Bandwidth Utilization

Here we have analyzed the affect of security deployment in a simple network, over the bandwidth utilization of the network. It has an importance in network performance. After implementation security in an unsecure network or enhance security in existence network, it provides a secure and reliable network. Consequently, we get some background outcome which effect on the network performance, i.e. effect on network QoS, increase or decrease communication delay factor, change the bandwidth utilization etc.

It is explained in simulated results presented in fig 7.11, 7.12, where at times to establish a IPSec in the form VPN tunnel, implement and analysis both mode of operations (*Transfer mode and Tunnel mode*). It is observed that, based on working functionality there is very little difference in

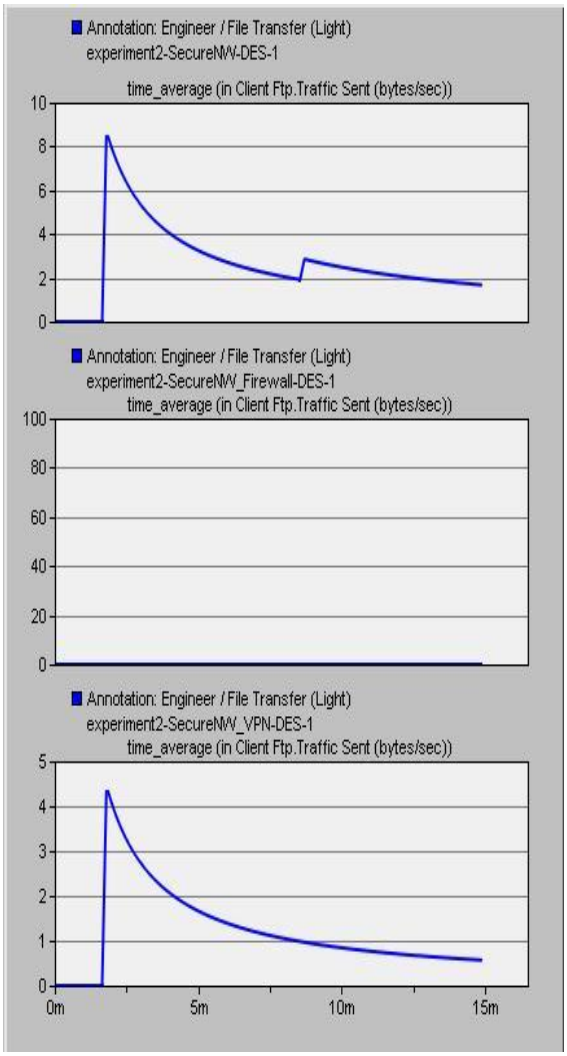

Fig 7.11: In Tunnel Mode

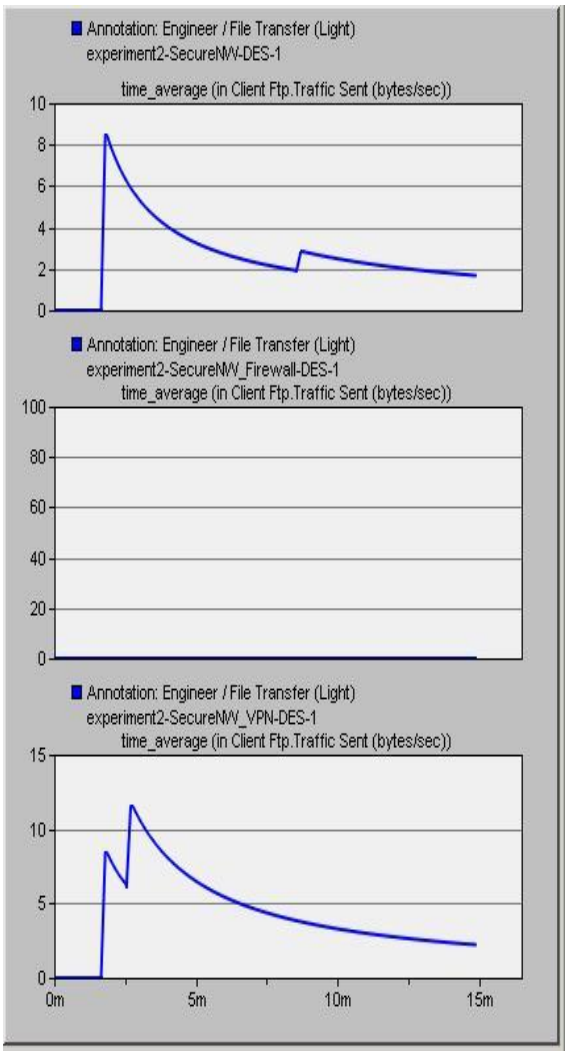

Fig 7.12: In Transfer Mode

both modes of operations. In "*Transfer mode"* first it provides the protection of existing upper layer protocols then after it provides the protection of existing IP payload, But in "*Tunnel mode"*

it first provides the protection to existing IP packet then entertain the AH or ESP field in the IP packet [14], (see fig 2.15).

Both VPN *Transfer and Tunnel* approaches provides or enhance level of security during communication, but after analyzing we got some results which shows that; at "*Tunnel mode"* it used or occupied approximately half of data bandwidth by apply security (fig 7.13).

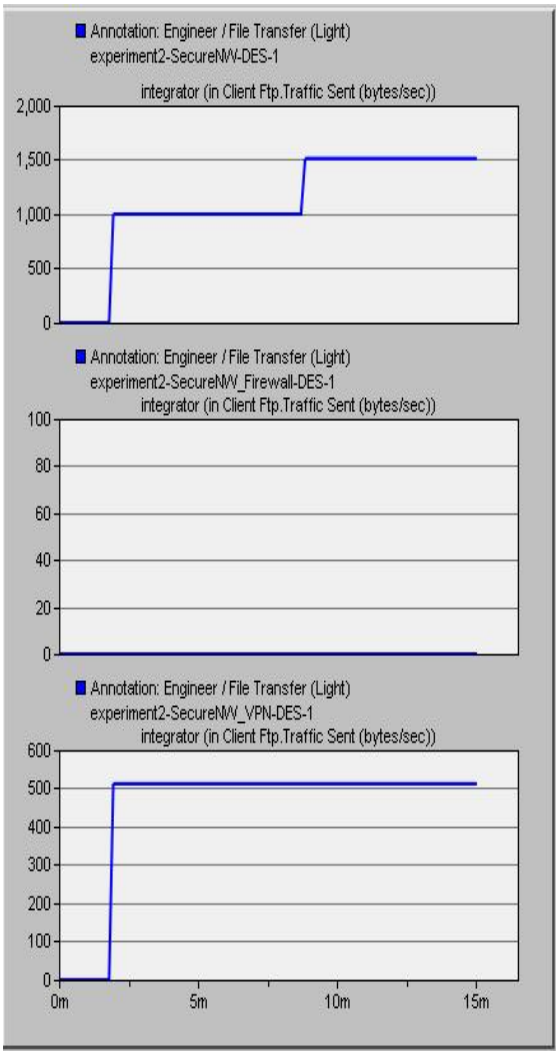

Fig 7.13: In Tunnel Mode

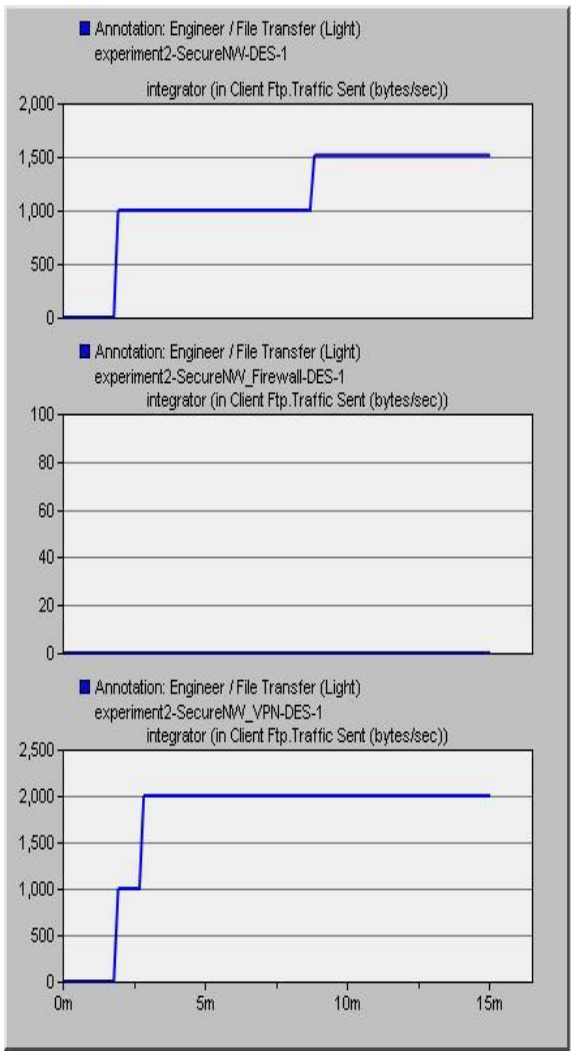

Fig 7.14 In Transfer Mode

On the other hand, when we deployed *Transfer mode*, we got results which showed that; it used or occupied double of data bandwidth by applying security or by comparing them *Tunnel mode* (see fig 7.14). As a result it is very important, what effects can occur after deployment security in a network.

Chapter 8

CONCLUSION AND FUTURE WORK

8.1 Conclusion

The aim of this thesis was to explore the network vulnerabilities and in-depth analysis of different security attacks and security solutions. Security is not about a specific firewall, product, brand and operating system. Properly configured firewalls, strong passwords that changed on regular basis, antivirus update on regular basis etc all these elements used collectively to good security practices. Deficiencies in bad products can defeat with good practice, whereas bad process can be diluted otherwise excellent products. It is better to have no security devices instead of incorrectly configured security devices. As we observed in first scenario of simulation, in which configuring the network parameters on default mode will allow resources even to use by unauthorized users. Similarly in second scenario setting the network on deny everyone will cause to stop working even network administrators. Some time deployment of security can affect the QoS of network as we observed in third scenario that tunnel mode utilizes half of the network bandwidth which decreases QoS and introduces delay factor. The bottom line is that a network cannot 100 percent secure. However we can guarantee better security by analysis our network. This analysis will helpful to find out the vulnerabilities in network. For example before introducing a firewall in network first analyze it that, does it integrate with the network, will it fulfills your future demands, will it reliable, scalable and maintainable, is it possible to upgrade it and compatible with new products and new softwares. This analysis will use as a baseline for designing a better security plan.

"The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable." [57]

8.2 Future Work

Experts agree that today's major challenge is not the security technology itself but how to make appropriate procedures and controls for achieving IT security. Hackers will still remain in the market and even their numbers seem to be growing. Emerging trends in IT arena will leading the world to a point where computers will do even more for us than they are doing now. Technology development never stands stills. Attacking tools will continue to advance, as will security solutions. If someone tries to stay up-to-date with every new threat soon he/she will be stress. It is better to look for the major vulnerabilities and try to eliminate them using with existing resources.

References:

[1] William Stallings, *Network Security Essentials Applications and Standards,* 2nd ed., New Jersey: Pearson Education, 2003, pp. 6

[2] http://www.brainwavecc.com/TechDocs/Security.html

[3] http://www.queencitynews.com/modules.php?op=modload&name=News&file=article&sid=1666

[4] Network Model, http://www.tcpipguide.com/free/t_TheBenefitsofNetworkingModels.htm

[5] JOHN D. DAY AND HUBERT ZIMMERMANN, "The OS1 Reference Model" *in proc*. THE IEFJ2, VOL. 71, NO. 12, Dec. 1983

[6] Gilbert Held, *TCP/IP Professional Reference Guide*

[4] Data Link Layer, http://en.wikipedia.org/wiki/Data_Link_Layer

[5] William Stallings, *Wireless Communication*

[6] Charles M. Kozierok, *The TCP/IP Guide: a comprehensive, illustrated internet protocols reference*

[7] The TCP/IP Protocol Suite, http://www.fujitsu.com/downloads/TEL/fnc/pdfservices/TCPIPTutorial.pdf

[8] W. Richard Stevens ,*TCP/IP Illustrated, The Protocols,* volume 1

[9] Peter Losin, *TCP/IP Clearly explained*

[10] TCP dump, http://www.usenix.org/publications/login/1998-8/tcpdump.html

[11] William Stallings, *Network Security Essential, Applications and Standards*

[12] Uyless Black, *Internet Security Protocols, Protecting IP Traffic*

[13] The Java Tutorial, http://java.sun.com/docs/books/tutorial/networking/sockets/definition.html

[14] Application Layer in TCP/IP suite, http://en.wikipedia.org/wiki/Application_Layer

[15] Craig Hunt, *TCP/IP network administration*

[16] Mail Transfer Agent, http://en.wikipedia.org/wiki/Message_transfer_agent

[20] "Glossary of Internet Security Terms", http://www.auditmypc.com/glossary-of-internet-security-terms.asp

[21] "Introduction to Computers/System Software-Wikiversity"

http://en.wikiversity.org/wiki/Introduction_to_Computers/System_software

[22] Yeu-Pong Lai and Po-Lun Hsia, "Using the vulnerability information of computer systems to improve the network security", *Journal of Computer Communications*, vol. 30, Issue. 9, pp. 2032-2047, 30 June 2007

[23] "Unauthorized Network access becomes a felony",

http://www.dba-oracle.com/t_unauthorized_access_computer_network_crime.htm

[24] "Guideline for the analysis of LAN Security", http://www.itl.nist.gov/fipspubs/fip191.htm

[25] "Computer System Laboratory Bulletin",

http://csrc.nist.gov/publications/nistbul/csl94-03.txt

[26] "What is Hacker?" http://www.webopedia.com/TERM/H/hacker.html

[27] Clemmer, L. (2010, 05). Information Security Concepts: Authenticity. Retrieved from Computing: Bright Hub: http://www.brighthub.com/computing/smb-security/articles/31234.aspx

[28] "What is a packet sniffer", http://www.wisegeek.com/what-is-a-packet-sniffer.htm

[29] "Sniffing", http://www.hackerscenter.com/index.php?/HSC-Guides/Ethical-Hacker/Sniffing.html

[30] Michael Gregg, George Mays, Chris Ries, Ron Bandes, and Branden Franklin. *Hack The Stack*, Rockland, MA: Syngress Publishing, 2006. [E-book] Available: Google e-book

[31] "Network Probes Explained", http://www.linuxjournal.com/article/4234

[32] Eric Cole. *Hackers Beware*, First ed. USA: New Riders Publishing, 2002

[33] Raman Sud, Ken Edelman. *Secur Exam Cram 2*, USA: Que Publishing, 2004

[34] Idaho National Laboratory; *"Control System Cyber Security; Defence in Depeth Strategies*", external report # INL/EXT-06-11478, May 2006

[35] Cisco Security IntelliShield Alert Manager Service, URL:

http://www.cisco.com/en/US/services/ps2827/ps6834/services_overview0900aecd803e85ee.pdf

[36] E-Thesis http://ethesis.nitrkl.ac.in/77/1/Yellapu.pdf

[37] Dr. K.Duraiswamy and Mrs. R.Uma Rani "*Security Through Obscurity*"

http://www.rootsecure.net/content/downloads/pdf/security_through_obscurity.pdf

[38] William Stallings, *Network Security Essentials Applications and Standards*, 2nd ed., New Jersey: Pearson Education, 2003, pp. 34-42

[39] "Network Security", www.sanog.org/sanog1/networksecurity1.ppt

[40] William Stallings, *Network Security Essentials Applications and Standards*, 2nd ed., New Jersey: Pearson Education, 2003, pp. 68-72

[41] B Clifford Neuman and Theodore Ts'o " Kerberos: An Authentication Service for Computer Networks", *Journal of IEEE Communications Magazine*, vol. 32, Issue. 9, pp. 33-38, Sep 1994.

[42] William Stallings, *Network Security Essentials Applications and Standards*, 2nd ed., New Jersey: Pearson Education, 2003, pp. 123-128

[43] Idaho National Laboratory; *"Control System Cyber Security; Defence in Depeth Strategies*", external report # INL/EXT-06-11478, May 2006

[44] William Stallings, "*Network Security Essential; Applications and Standards"*, ISBN-13: 978-0-13-706792-3

[45] Jay Beale, Andrew R. Baker, Joel Esler, Toby Kohlenberg & Stephen Northcutt, "*Snort: IDS and IPS toolkit*" ISBN-13: 978-1-59749-009-3

[46] Ted Holland, *"Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth",* GSEC Practical v1.4b, Option 1, February 23, 2004

[47] Intrusion Protection System; URL**:**http://en.wikipedia.org/wiki/Intrusion_prevention_system

[48] Desai, Neil. "*Intrusion Prevention Systems: the Next Step in the evolution of IDS.*" Security Focus. 27 February 2003. URL: http://www.securityfocus.com/infocus/1670

[49] M. A. R. Ghonaimy, Mahmoud T. El-Hadidi, Heba K. Aslan, "*Security in the information society: visions and perspectives*"

[50] Behavior Blocking Antivirus Protection; http://www.symantec.com/connect/articles/behavior-blocking-next-step-anti-virus-protection

[51] Firewall; http://www.vicomsoft.com/knowledge/reference/firewalls1.html

[52] Type of Firewalls; shttp://en.wikipedia.org/wiki/Firewall_%28computing%29

[53] Chris Bryant, CCIE #12933, "*CCNA Security And CCNP ISCW Tutorial: "SYN Flooding Attacks" and TCP Intercept"* URL: http://www.thebryantadvantage.com/CCNASecurityCCNPISCWTCPIntercept.htm

[54] Man Young Rhee, *Internet Security Cryptographic Principles, Algorithms and Protocols,* First ed. England: John Wiley & Sons, 2003, pp. 243-271

[55] K.Salah and A.Alkhoraidly "An OPNET-based simulation approach for deploying VoIP" International Journal Of Network Management Int. J. Network Mgmt 2006; 16: 159–183.

[56] Marcos Portnoi, Joberto S.B.Martins "TARVOS – an Event-Based Simulator for Performance Analysis, Supporting MPLS, RSVP-TE, and Fast Recovery"

[57] http://www.cs.iit.edu/~cs549/lectures/CNS-1.pdf