“Shielding Data in Transit: Secure Protocols and Encryption for Network Protection”

BY

MD SAZZAD HOSSAIN BHUIYAN
ID: 232-25-038

This Report Presented in Partial Fulfillment of the Requirements for
The Degree of Masters of Science in Computer Science and Engineering

Supervised By

Mr. Narayan Ranjan Chakraborty
Associate Professor and Associate Head
Department of CSE
Daffodil International University

Co-Supervised By

Mr. Abdus Sattar
Assistant Professor & Coordinator M.Sc
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JANUARY 2025

APPROVAL

This Project/Thesis titled **"Shielding Data in Transit: Secure Protocols and Encryption for Network Protection"**, submitted by Md Sazzad Hossain Bhuiyan, ID No:232-25-038 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on **11-01-2025**.

BOARD OF EXAMINERS

Chairman

Dr. Sheak Rashed Haider Noori, PhD
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Dr. Md. Zahid Hasan, PhD
Associate Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Dr. Arif Mahmud, PhD
Associate Professor & Director MIS
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

External Examiner

Dr. Mohammed Nasir Uddin, PhD
Professor
Department of Computer Science and Engineering
Jagannath University

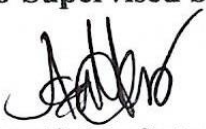
DECLARATION

I hereby declare that this research has been done by me under the supervision of Mr. Narayan Ranjan Chakraborty, Associate Professor and Associate Head, Department of CSE, Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

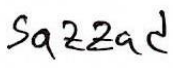
Mr. Narayan Ranjan Chakraborty
Associate Professor and Associate Head
Department of CSE
Daffodil International University

Co-Supervised by:



Mr. Abdus Sattar
Assistant Professor & Coordinator M.Sc
Department of CSE
Daffodil International University

Submitted by:



Md Sazzad Hossain Bhuiyan
ID: 232-25-038
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First I express my heartiest thanks and gratefulness to Almighty Allah for His divine blessing which makes it possible to complete the final year Thesis/internship successfully.

I am really grateful and wish my profound indebtedness to Mr. Narayan Ranjan Chakraborty, Associate Professor and Associate Head, Department of CSE, Daffodil International University, Dhaka, deep knowledge & keen interest of my supervisor in the field of Network Security to carry out this thesis. His endless patience, scholarly guidance continual encouragement, constant and energetic supervision constructive criticism, valuable advice reading many inferior drafts and correcting them at all stages have made it possible to complete this thesis.

I would like to express my heartiest gratitude to **Dr. Sheak Rashed Haider Noori**, **Head,** Department of CSE, for his kind help to finish my thesis and also to other faculty members and the staff of CSE department of Daffodil International University.

Finally, I must acknowledge with due respect the constant support and patients of my parents.

ABSTRACT

Given that the amount and the nature of transferred data are increasing day after day, the protection of information during its transmission is crucial. "Shielding Data in Transit:" Secure Protocols and Encryption for Network Protection," discusses key measures which should be taken so as to protect data while in transit in the given communication paths. This paper seeks to look at the most frequently used Secure Communication Protocols like the TLS 1.4, SASE (Secure Access Service Edge) and MACsec (Media Access Control Security) in terms of their advantages, limitations and how best to implement them on the network. Further, the paper examines complex encryption forms such as E2EE or quantum-resistant algorithms and the best practices to counteract novel dangers. Focuses are made based on how it can help protect daily applications such as, web traffic, email communications, IoT, and cloud applications. The paper also analyses changing threat posed in recent years; MitM attacks, eavesdropping and data leakage as well as providing the understanding of how the modern cryptographic tools and secure protocols are protecting data during the transmission. This work presents an overview of commonly used methods and technologies to assist the network engineers, security specialists and other involved organizations for developing effective and secure communication networks for exchange of information in turbulent and competitive world.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.1 Introduction

With the growth of digital society and with ever more networks being developed transferring information through networks has never been more significance. Everything from money transfers and medical histories, correspondence, and patents, to personal messages and corporate information is transferred daily across the systems, applications, devices and networks, sensitive data is constantly being exchanged across various platforms, devices, and networks.

Transactional data is a type of data which is in an active state or undergoing transmission by various computer networks including local area networks (LANs), wide area networks (WANs) or via the internet. Due to this flaw, the common criminals like the hackers, attackers and malicious people in the computer based environment launches various attacks like man-in-the-middle attack, eavesdropping attack or packet sniffing attack, where the criminals can easily capture, modify or even steal the information without being aware by the communicating parties.

Encryption is typically the conversion of data to another form which can only be understood by those requiring to get access to information. Despite the fact that information can be transmitted via a network, encrypted information does not make much sense to the interceptor since it is configured to be unreadable unless decrypted using the decryption key. Conversely, secure protocols ensure that the channel used to transfer data is protected against intruder's access and modification. Additional measures to safeguard data during transit include; the use of robust authentication, periodic update of cryptographic processing to meet emerging threats, the use of network monitoring and intrusion detection systems. All of them, in turn, constitute a multilevel protection from the modern threats in the sphere of cyber security.

1.2 Motivation

In today's global village security is paramount given such as viruses, hacker, eavesdropping and fraud. With the increased use of computer systems and networks in organizational and individual processing, analysis, storage, and transmittal of information, organizations and individuals have to protect the data content integrity and the networks and systems from breaches and attacks.

Some people are convinced that security issues relate to companies with classified information and fast connections only; however, anyone might become a target. Most systems, even if they are not storing significant data, can be used to plant more attacks towards other networks for instance DDoS.

In the past, nobody had the time to pay much attention to it and it was handled by people with much experience, but now with increased awareness even novices are getting to learn a few things about it. The level of security needed differs from one company to another, for this reason, there is a need to analyze, design, implement and monitor using Systems Engineering approach. The assessment phase aims at evaluating both the software and the hardware to learn the strengths, weaknesses, need and requirements, present and in the near future.

1.3 Rationale of the Study

The rationale for this study on "Shielding Data in Transit: The foundation behind “The Practical Guide to Implementing Security Measures: Secure Protocols and Encryption for Network Protection” lies in the rising security concerns concerning transmission, of sensitive data, in computer networks. With the increase in the strength of the interception, hacking and data breaches securing data in transit is has become a big concern to everybody including businesses, government and individuals.

Data implementation can be secured through the use of some forms of protocols, which include encryption when passing through channels applying use of TLS/SSL. However, due to fast growth of cyber threats and questionable stability of these technologies, people need to know more about how to use and control these security elements.

In this research, the use of encryption and Secure Sockets Layer protocols to protect information in transit is reviewed, the merits and demerits given and smooth practices for organizations seeking to protect their information given. The idea is to empower organizations and security practitioners enhance their network resilience and mitigate threat actors specifically in a world that continuously goes digital.

1.4 Objectives

- **Understand the Importance of Data Protection in Transit:**

  In order to establish the importance of implementing security measures in data communication, appreciate the confidentiality, integrity as well as authenticity of data that is in transition on the internet as well as private networks.

- **Identify Common Threats to Data in Transit:**

  In order to understand what threats exist that could endanger information that is in transit and the implications of the risks on business and individuals: eavesdropping, man-in-the-middle attack, data interception, unauthorized access.

- **Explore Secure Protocols for Data Transmission:**

  There is therefore constantly on emergence of new protocols in the network security to tackle different threats as well as enhance performance and security of data and connection to different resources over public and private networks such as TLS 1.3, SASE or Secure Access Service Edge, Zero trust Network Access or ZTNA for short, MACsec or Media Access Control Security among others all of which provide encryption and other secure ways that data can be sent over the internet.

- **Understand the Role of Encryption in Securing Data in Transit:**
  To learn about the principles of encryption and how data is protected during transmission using; symmetric and asymmetric encryption, PKI; the advantages of cryptographic functions such as; AES, RSA and ECC.

- **Enhance Awareness of Security Tools and Technologies:**
  To become conversant with the current network security aids like Virtual Private Networks, firewalls and the intrusion detection systems apart from other security protocols and encryption as part of a holistic security solution to protect data during transfer.

1.5 Expected Output

- **Analysis of TLS 1.3:**

  This research will also investigate the advancements that have been made in TLS 1.3 such as; increased security level of encryption, better identification and crucial responsibilities of securing communications against threats such as MITM and eavesdropping during web interaction.

- **Exploration of SASE**:

  Of course, it will also look into how to approach SASE as a composition of security functions (SWG, CASB, ZTNA, etc.) and how this results in the delivery of secure access to cloud services, improved security for both remote and hybrid working environments, and secure transit of data.

- **Understanding MACsec:**

  This paper will describe how MACsec secures data at Layer 2 in both LAN and WAN to apply encryption to Ethernet frames to protect data integrity as well as confidentiality inside enterprise networks.

- **Protocol Comparison and Integration:**

  Relative analysis will compare and contrast TLS 1.3, SASE, and MACsec to fill the gaps of organizations about the proper integration of these layered security protocols.

1.7 Goal/Aim

As articulated in this dissertation, the main goal is to develop superior knowledge of Network security standards. Particular emphasis will be placed on those applications and standards that are or will likely be most frequently adopted.

CHAPTER 2
BACKGROUND

2.1 Network and protocols

In this chapter only introduction about data communication network will be discussed. The network layer protocols are the most prominent component of a communication network. This chapter fraughts such topics as the place of the network layer protocols in communication model and the functional characteristics of the protocols in various levels of data transmission. These parameters take the form of protocol header fields. Having discussed these protocols, we'll focus on the header field and understand how an attacker may use or modify the header fields of these protocols to suit his/her needs. The structure of OSI layer protocols & TCP/IP layer protocols with their deeper understanding can perform this objective.

2.2 Network

Network can be as explained as a set of linked computers, a network is a combination of hardware devices in the same or different geographical location connected by physical or logical means such as wired or wirelessly connected interfaces and channels and nodes in this connected unite are computers; printers; or telecommunication gadgets that include mobile phones, towers and others. Every node has its unique network identifier. The main goal is to distribute resources to such nodes and work only under certain rules of authenticity and security.

A network protocol may be defined as a system of standard practices that dictate the decentralized transmission of messages. It specifies how two systems enter into communication and depends on the particular activity or messages between nodes in a network detection network and the original single-mode brain tumor detection technique are compared, and the three evaluation indexes of dice, SN, and SE are optimized, respectively. In order to create web-based software that can classify brain cancers (glioma, meningioma, and pituitary) based on high-precision T1 contrast magnetic resonance.

2.3 The Open System Interconnected Model (OSI)

In early 1997, ISO introduced the OSI Reference Model widely known as OSI model which enables communication between dissimilar systems. The OSI model allows any computer to interconnect with another provided the two use this OSI model standards.

OSI Reference Model is split into seven layers where each layer has its precise function. These layers are however, independent but are connected and possess a structured flow. Each of them concerns different aspects of communication and bears a different name and function. Given bellow Fig 2.1 about OSI Reference Model Layer Architecture

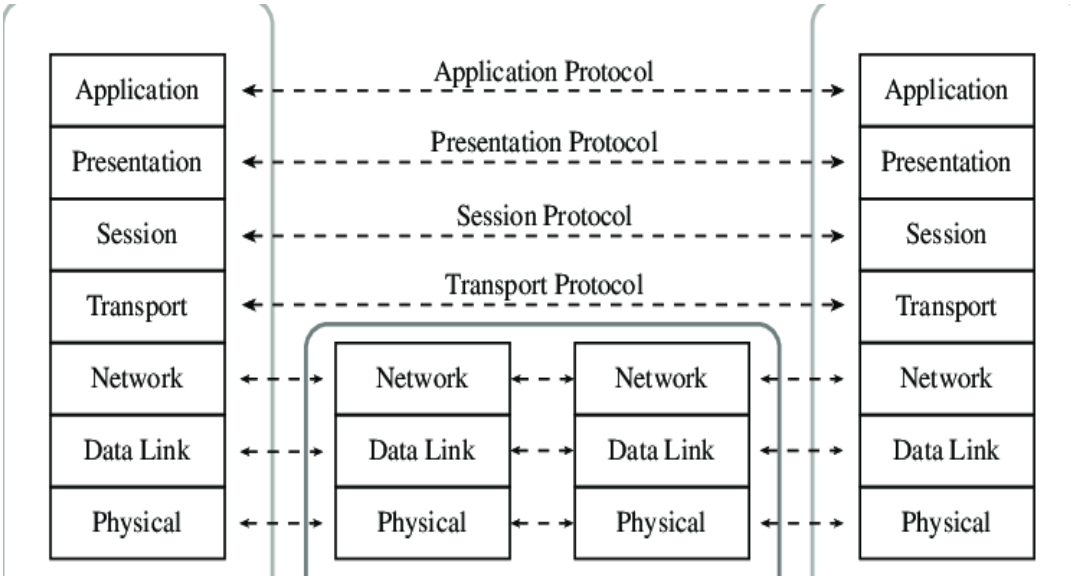


Fig 2.1: OSI Reference Model Layer Architecture

On other hand if we look that OSI has an organization of system architecture three level of abstraction are recognize at OSI; the system architecture, the service architecture and the protocol architecture (Refer figure 2.2 OSI System Architecture) The OSI service specifications are supposed to be for particular service between user and system in a given layer. That which type of protocol is running against the specific communication service is due to parallel OSI protocol specifications. Therefore it can be seen that amalgamation of these two segments transforms into OSI system architecture.

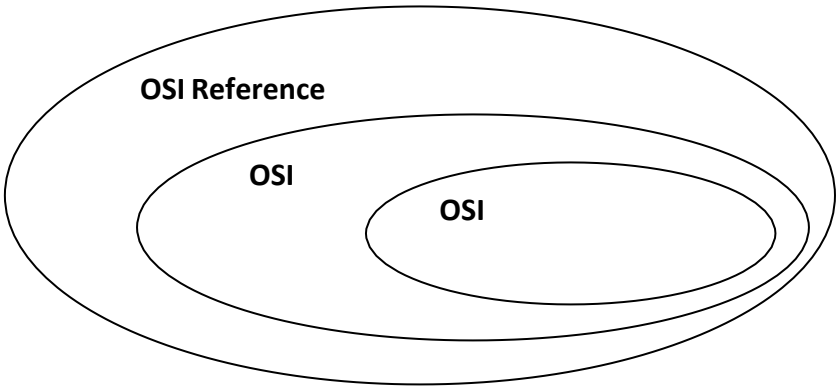


Fig 2.2: OSI System Architecture

Physical Layer

Physical layer is the lowest layer of OSI model; it provides connection between system interface cards and physical medium. This layer encodes and decode electrical/electronic signals in discrete form known as 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.

Data Link Layer

In OSI Reference Model, Data Link Layer is number two layer. While Data Link layer is in charge of control, methods for proper format of data can be checked by accessing data flow errors in physical layer. Consequently, the data link layer is responsible to form data into frames. Hence we can conclude that the data link layer involves definition of data formats which specifically include the entity through which information is conveyed. The link control procedures and error control procedures may take place in the physical layer . Like cyclic redundancy cheque (CRC); the error checking that used to run at the time of transmission of a frame from the source end. The same mechanism will exist in the receiver side if they got any difference after comparison then the receiver sends.

It is mandatory to perform the additional division of the data link layer which is split into two sub layers – the Logical link Control (LLC); and the Media Access Control. The given LMC has to do with flow control as well as error detection in data. The media access control is on the other hand in charge of traffic jam ush and physical address rearrangement.

Network Layer

The OSI Reference Model, the third layer is known as the Network Layer. This layer is supposed to come up with a logical connection between the source and the destination Packets are the form of the data at this layer. For this target, the network layer protocols offer the following services:

Connection mode:

At the network layer there exist two kind of connection between source and destination, the first one is called connectionless- communication where there exist no connection acknowledgement. Connectionless communication example is Internet Protocol (IP). The second type of connection is connection oriented which guarantees connection acknowledgement. TCP is an example of this connection .it gave way to other plans and priorities, but never really disappeared from the parliamentary agenda.

IP Addressing:

Every node or device in computer networks must have its identification number. Thus, always, the sender and receiver are making the correct connection through this unique ID. This is due to the functionality of network layer protocol, which has the source address and the destination address embedded in its header fields. Therefore there is low probability of having packet drops, traffic jam and broadcasting.

Transport Layer

Next layer to the communication layer in OSI reference model is the transport layer and it is the fourth layer. It has two types of protocols one is the Transport Control Protocol (TCP), which is a connection-oriented protocol, and supports some other upper layer protocols such as HTTP and SMTP. The second one is User Datagram Protocol (UDP) which operates in the connection less service. As with TCP, it also supports some higher level protocols such as DNS, SNMP and FTP. The most important aspect of transport layer protocols is that they use port addresses in the field of the package header.

Session Layer

OSI Reference Model has Session Layer which is the fifth layer. Additionally, the Session Layer is involved in the management of sessions which entails issue of start and termination of sessions involving end-user application. It is used in applications like, live TV, video conferencing, VoIP. In these applications, before sending the data the sender sets up multiple sessions with receiver. An example of such protocol is known as Session Initiation protocols (SIP).

Presentation Layer

Presentation Layer is working as the sixth layer in the OSI Reference Model. This layer is used in presenting transmitted/received data in Graphical Mode. The key service of this layer is data compression and decompression. Before transmission, the data encryption is performed in presentation layer.

Application Layer

The seventh and the last floor of OSI Reference Model is Application Layer. This layer provides configuration to all the system level application such as FTP, E-mail services etc.

2.4 TCP/IP Protocol Suite

TCP/IP model is older than the OSI; it has just four layers contrary to OSI, which has seven layers. The TCP/IP model is more realistic from the view of practical communication than OSI model which lacks higher level traffic managing and reliable inherent data processing. Some of the TCP/IP suite consist of protocols of reliable communications and data security whereby every layer has its duty to perform. TCP (Transmission Control Protocol) is the important transport layer protocols which provides account, reliable data transmission, UDP (User Datagram Protocol) is important for real time data like video conferencing and VOIP where pointer is not important. Given show that Fig 2.3: Layer difference between OSI and TCP/IP Suite.

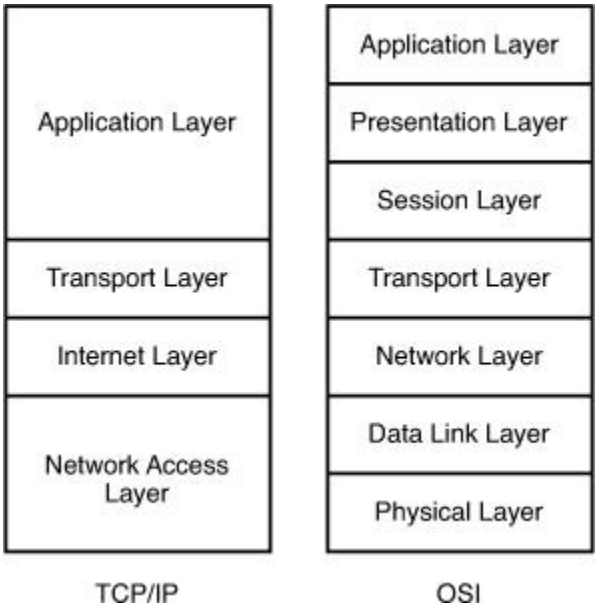


Fig 2.3: Layer difference between OSI and TCP/IP Suite

TCP/IP suite has layer structure similarity to OSI Model. In TCP/IP Suite the Link Layer categories the OSI last two layers which are physical layer and data link layer. Application Layer of OSI model. Bellow explain in Fig 2.4: Different Layers Protocols in TCP/IP suit do not exist in TCP/IP protocol suite.

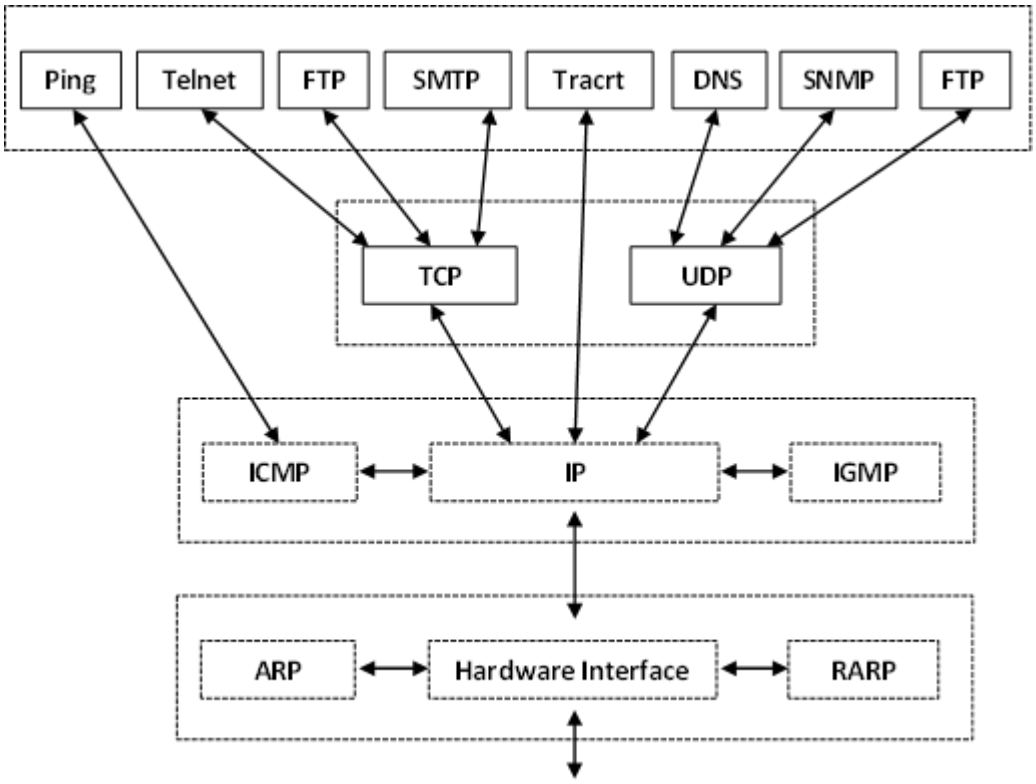


Fig 2.4: Different Layers Protocols in TCP/IP suit do not exist in TCP/IP protocol suite

2.4 Existing Security Protocol

2.4.1 IPSec Protocol

IPSec is actually an internet layer protocol designed to offer security at internet layer. The understanding of IPSec on internet layer is that it gives security to a user at a transparent level. It presents the data access authentication as well as the data encryption on the same level. Two important security services of networking are provided by IPSec namely is traffic authentication and key management. Refer Fig 2.5: IPSec Architecture data flow and Fig 2.6: IPSec Packet flow Scenario.

Protocol Identifier

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

1.Authentication Header (AH)

2.Encapsulation Security Payload (ESP

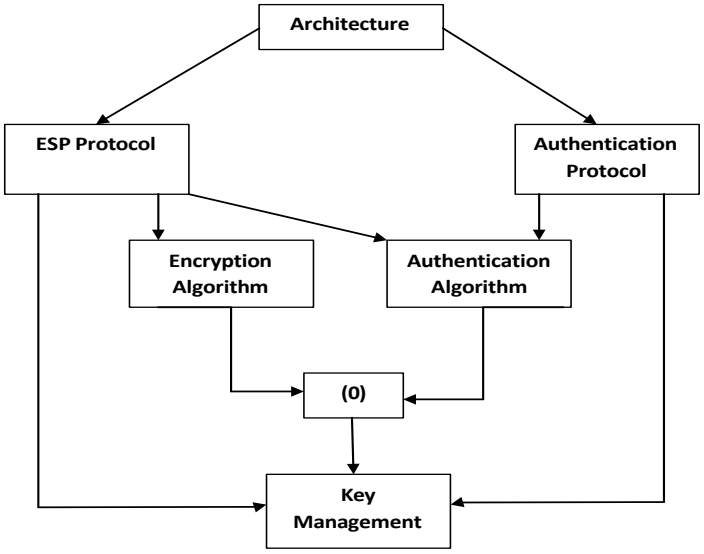


Fig 2.5: IPSec Architecture data flow

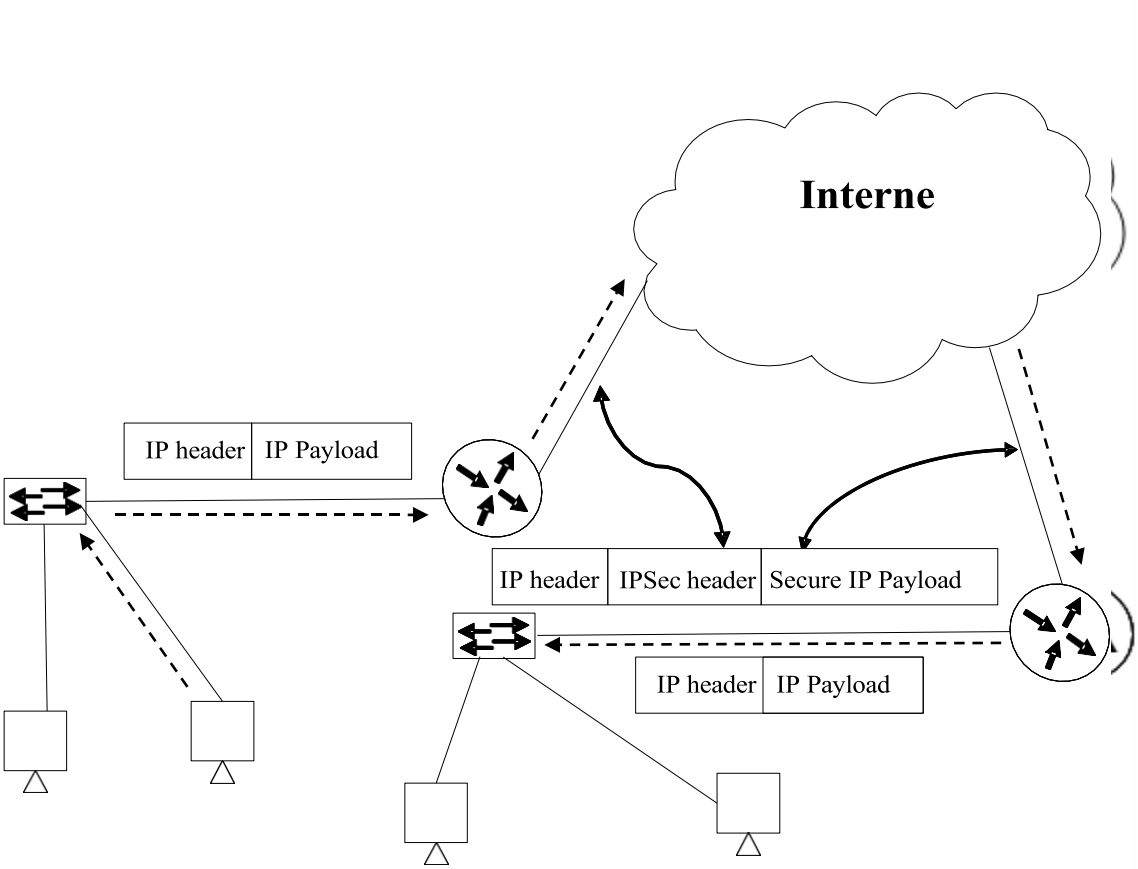


Fig 2.6: IPSec Packet flow Scenario

2.4.2 Cryptography

The most important application that I have come across is that is used to ensure that information being sent cannot be intercepted. This means that one needs to be certain you have put measures to ensure that intended data is not viewable by any unauthorized user. Cryptography as can be defined as the science of sending information in forms which would not be comprehensible for other persons except the recipient of communication. That is why there are two fundamental cryptographic terms in the field, Plain Text, the message or data which we wish to encrypt and Cypher Text the encrypted Plain Text.

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: To 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.

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:

Plain Text: The original message or data which we want to be encrypted.

Encryption Algorithm: Encryption algorithm performs different transformations on the data.

Secret Key: Secret key is the input to the encryption algorithm. Different transformations performed by the encryption algorithms depend on the secret key.

Cipher Text: This is the out put of scrambled message.

Decryption Algorithm: Reverse of the encryption algorithm, it produces the plain text with the help of same secret key and the cipher text. Given bellow refer fig 2.7 about Model of Conventional Encryption.

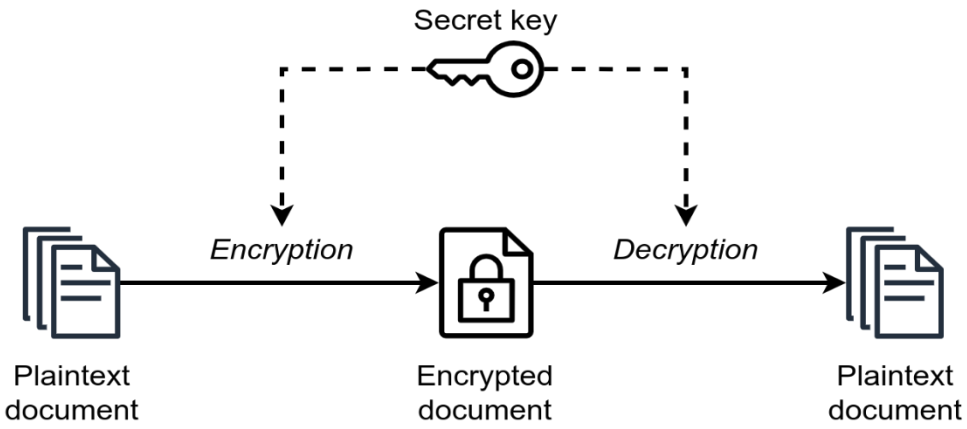


Fig 2.7: Model of Conventional Encryption

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.

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:

1. Widely used encryption scheme.
2. Algorithm referred to as Data Encryption Algorithm (DEA).
3. Is a block cipher.
4. The block of the plain text is 64-bit long.
5. The secret key is of 56-bit long

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.

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 output scrambled message.
5.Decryption Algorithm: Reverse of the encryption algorithm.

2.4.3 SSL/TLS

Web security can be done at various level of the TCP/IP model with each providing a different level of security. One is to offer security at the IP layer and this is done through IPSec, it is invisible to the users and one is able to filter traffic. A more popular band aid fix is to provide secure transport using SSL (Secure Sockets Layer) which has morphed into TLS (Transport Layer Security).

TLS/SSL works at the top of TCP, and is widely used in secure transmission, for instance, HTTPS, use port 443, HTTP uses port 80. TLS provides end to end authorization of messages and conversation and can use encryption keys for secure communication.

The SSL/TLS handshake involves:

1. Server Authentication: The client checks the digital certificate of the server provided by CA and issued to the server.
2. Client Authentication: Client verifies server's certificate and its published public ID which is also signed by a trusted CA.
3. Encrypted Connection: SSL uses public key security protocol at the beginning of link connection and possibly during each connection with the server.

SSL consists of two main sub-protocols: Record Layer, addressing the data format and the Handshake Layer addressing the process of authentication as well as connection establishment. The purpose of handshake is important to have confidence that both server and client are who they claim to be before entering into encrypted communication. bellow show that Fig 2.8: TCP/IP STACK and Fig 2.9: SSL Protocol Stack

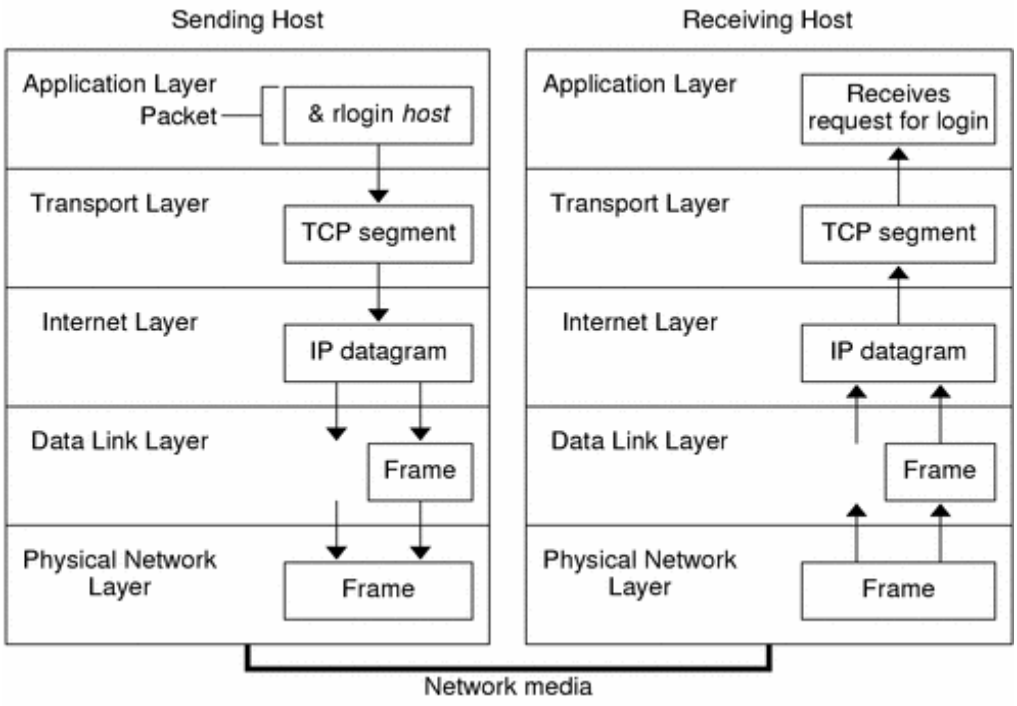


Fig 2.8: TCP/IP STACK

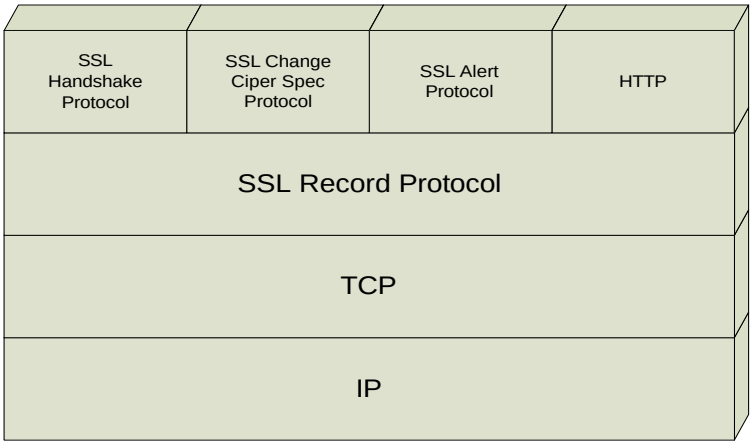


Fig 2.9: SSL Protocol Stack

2.4.4 Intrusion Detection System (IDS)

The IDS is the system which identifies any improper entry or violation of Systems or networks security. This is a security solution that remains in a system or a network and plays no active role in fending off these intrusions. In a network deployment the function of the IDS is to either scan the traffic or network activity with no effect on the traffic [43]. What it means is that an IDS in a network only detects or identify in any case of change on the network but does not take any resistive measure against such change. This customize rule based IDS are set or fixed by the network/system administrator based on previous behavior of the network. The IDS system has two methods of alerting intrusion in a network; the two techniques are:

Network based intrusion detection system (NIDS)

Network based intrusion detection system function in a network. It watches all the network traffic especially the traffic at the hardware layer based traffic. The operational aspects of the hardware layers in the context of TCP/IP suite have been discussed in chapter two as in link layer.

Host Based Intrusion detection system (HIDS)

Location and functionality of Host based IDS is somewhat different than the NIDS. The host-based intrusion detection system is implemented on a single machine or the system, and only that machine is protected by it. It is reasonable for track local system based activities or break-ins, for example, CPU utilization, file-sharing resources and operational capabilities of some application programs including web-server application and mail-service.given bellow Fig 2.10: HIDS Based Network.

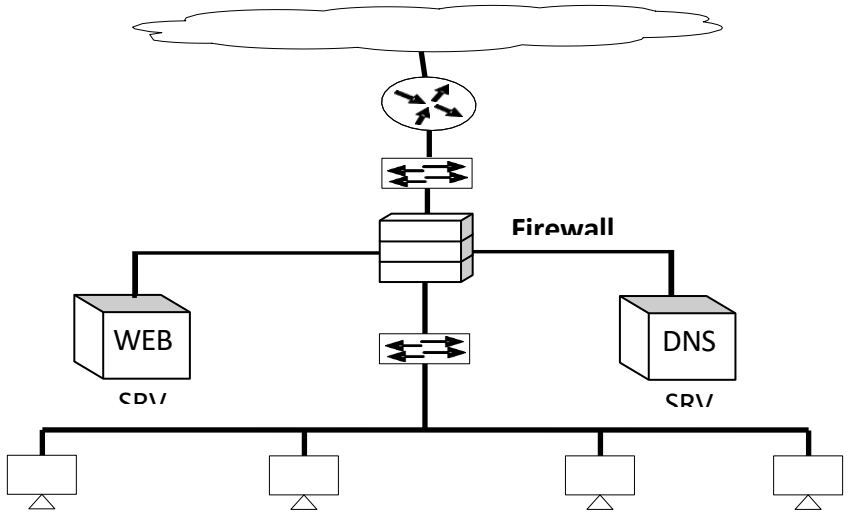


Fig 2.10: HIDS Based Network

2.4.5 Intrusion Prevention System (IPS)

The Intrusion Prevention System plays a function of preventing intrusion that happens in a network or local system. It operates based on IDS system log files as its output. Because of this reason we can pointed out that the IPS system is an extension of the IDS system However there are distinct difference between IDS and IPS. IDS system, for example, works only in the passive mode, that means it only able to notice any unwanted intrusion in the network, while an IPS works in an active mode. Depending on the design of the actual IPS, an IPS is capable of initiating action if it detects packet drops or unauthorized connection.

2.5 Challenges

Implementing secure protocols and encryption for network protection comes with several key challenges:

1. Performance Overhead: Encryption always creates some delay and requires processing power, which is not suitable for network-based real-time applications and generally for network devices with limited processing power.
2. scalability: Moreover, these networks and distributed systems' security involves key and certificate management, as well as creation of secure connections, to large scales, which is not an easy feat In such systems, integrity involves key, certificate and secure connections management that is not an easy task.
3. Key Management: The management of identification keys such as storage, replacement and withdrawal is essential though difficult notably when keys are hacked.
4. Human Error: This results because misconfiguration in the encryption protocols or weak implementation are sometimes created due to lack of knowledge or supervision.
5. MitM Attacks: As with any secure connection, if certificate validation is not implemented correctly, encryption can still be a candidate for man-in-the-middle attacks and therefore needs to be monitored and set up securely.

Summing up, the main issues affecting secure encryption protocol implementation are performance, scalability, compliance, security mechanism management and growth of threats.

CHAPTER 3
NETWORK SECURITY THREATS AND ATTACKS

3.1 Network Security

When we start discussing security it begins with what constitutes network security. If you took 10 administrators and asked them what network security is they all would have about 10 different responses. However as its name suggest network security is the protection of networks; their applications or services against authorized access that prevents form modification, disclosure or destruction of data. It also confirms that the network is working accurately without inducing any adverse impacts. While this is admittedly a very broad definition, a general definition better prepare network administrators for new types of attack. Every organization develops its own security policy that comes with an access level that is either allowed or restricted. Therefore, any organization must have such a security mechanism, which is extensive, and assists in addressing new forms of an attack.

3.1.1 Security Threats

When it comes to post threat conversation can be anyone or anything that poses a threat to the loss or devastation of data or network Threats can also be natural for example wind, lightning or flooding or even an accidentals threats such as accidentally deleting a file. Given bellow Fig 3.1 about Network Security Threat.

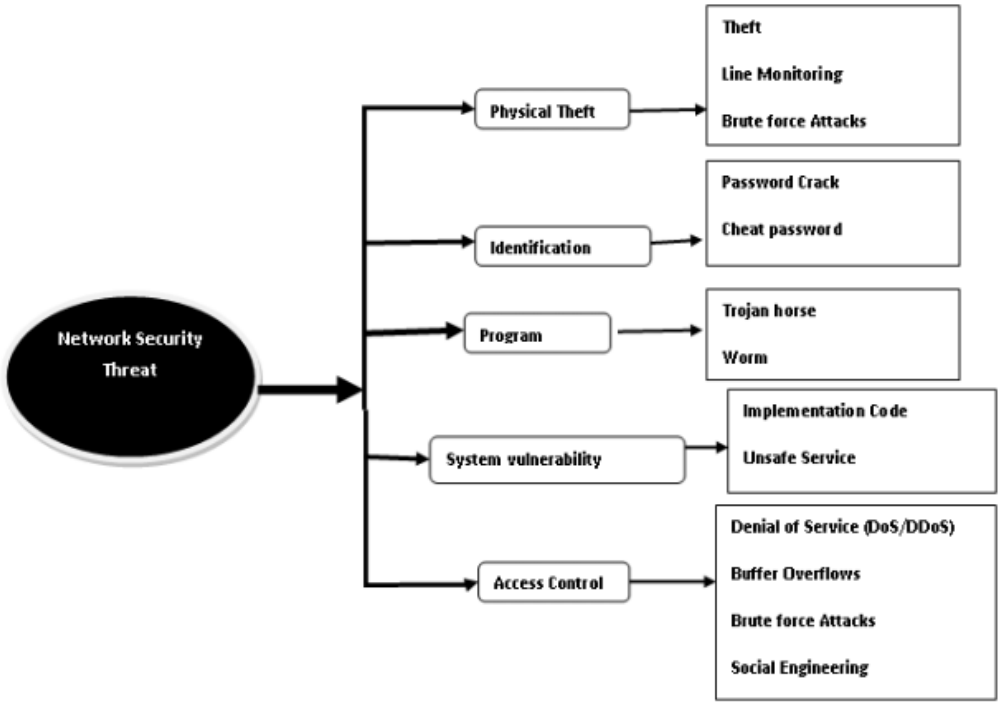


Fig 3.1: Network Security Threat

3.1.2 Unauthorized Access

Interception of available wireless networks is prohibited in a lot of regions, including Canada, where such actions are punishable by the law as theft of telecommunications. In the context of networks, sharing is the whole idea behind it but this is risky because anybody can get on the network and access any file or printer.

Common methods of obtaining unauthorized access to networks include:

1. Password Sharing: A user may unknowingly reveal his/her password.
2. Password Guessing: Malicious parties attempt to use universal credentials, common words, short length passwords of 1-3 characters, or social security numbers, dates of birth, and family name to crack passwords.
3. Password Capturing: Delaying, blocking or intercepting passwords by such methods for instance packet sniffing.

Moreover, these methods demonstrate the need for using essential and specific passwords to lock the networks and encryption.

3.1.3 Malware

Malware in Network Security can be defined as a malicious software that is intended to penetrate, corrupt or harm computer based networks, systems, and data. With regard to the security of a network; malware has the capacity to move from one system to another within the network and corrupt the different system's data, steal the respective organization's credit information or cause network breakdown. Given that network environments have become increasingly heterogeneous and intertwined, it is important to comprehend how malware function in network security as well as to identify such threats.

1. Viruses: Programs that can attach to files or other programs and which can spread after the particular file or program is run.
2. Worms: A virus that will copy itself when it has infected other systems without necessarily having to be triggered by a user.
3. Trojans: Actually viruses which are in the form of other programs with a sole aim of stealing data or permitting the hacker have remote access to a particular computer.
4. Ransomware: A type of malicious software that targeted has its files encrypted and then threatens to delete the key unless the targeted individual pays.

3.1.4 Software Vulnerabilities

Software vulnerabilities, therefore, align with the following term definitions: Flaws, weakness or bug in the software that makes a system susceptible to attack or menace from an attacker, interfering with the normal running of services offered or endangering the security of a system. Some of these risks can be in any layer of software, including operating systems and applications, and it is used by hackers frequently in their operations. Hackers take advantage of these openings in using different tactics in order to run illicit code, sabotage, or data theft.

3.1.5 Misconfigured Network Devices and Firewalls

In particular, routers, firewalls, switches – all network devices can be misconfigured and become a security threat. These devices regulate traffic and security from unknown entities, but when misconfigured, they introduce different risks to networks.

Risks:

1. Unauthorized Access: Making company internal systems open to the attackers.
2. Poor Traffic Filtering: In this case, the fathers allow the internet, which transmits and receives traffic, to permit bad traffic.
3. Weak Network Segmentation: Allowing the attackers to navigate laterally.
4. Denial of Service (DoS): Vulnerability Exploitation: Devices with vulnerabilities still waiting for the latest security updates to be installed being attacked.The disruption of service because of misconfigured load balancers or firewalls.
5. Data Exposure: Information that needs to be protected exhibited for people who ought not to approach it.

To sum up, misconfigurations cause breaches, data leaks and outages. You cannot avoid such risks but you can limit them by performing regular audits, configure everything properly and follow security best practices.

3.1.6 Vulnerabilities in IoT Devices and Smart Networks

IoT devices and smart networks are transforming many elements of technological interactions in everyday life, including smart homes, smart healthcare, manufacturing and industrial applications, and enterprise solutions. Because many Internet of Things devices are poorly designed, have little to no security, and have a large attack surface, more and more of the electronic devices we use are becoming favorites for cybercriminals as the IoT expands. Numerous IoT devices are connected to a wider network, making them targets not only as standalone sources but also as points of entry into bigger networks

3.2 General Categories of Security Attacks

There are many parameters that can be used to categorize security attacks but based on the main goals, security attacks can be categorized into the following categories.

Security attacks threaten confidentiality and integrity of a system; availability and authenticity of a system. There are four main categories of security attacks:

i. Interruption: This attack targets data availability through accidental events which include; system crashes, natural disasters and through the intentional acts of an attacker which include; Denial of service (DoS) attack, Distributed DoS (DDoS) attacks. It restricts the use of resources by the particular persons who were permitted to use those resources earlier. Contingent measures which act as backups assist in avoiding these attacks.
ii. Interception: This is violated by unauthorized access to personal and sensitive information. When information is exposed, or recorded by the attackers, invasion of security become apparent. Interception can however be prevented with the implementing proper authentication and access controls in place.
iii. Modification: This attack changes information, whether intentionally or unintentionally. It prevents data loss by either adding or converting information. There are validations applied to prevent such changes, as well as integrity checks.
iv. Fabrication: This is an attack on the authenticity of a message which in effect fake data messages or messages of some identifiable source and can originate from an internal or an external threat. Password, smart cards or other digital certificates mechanisms can be used for user identity check and for confirming the integrity of the communication.

In other words, threats target the availability of services, confidentiality, data integrity and identity, while safeguards are arranged against these dangers. In Fig 3.2 show that Basic types of Security Attacks

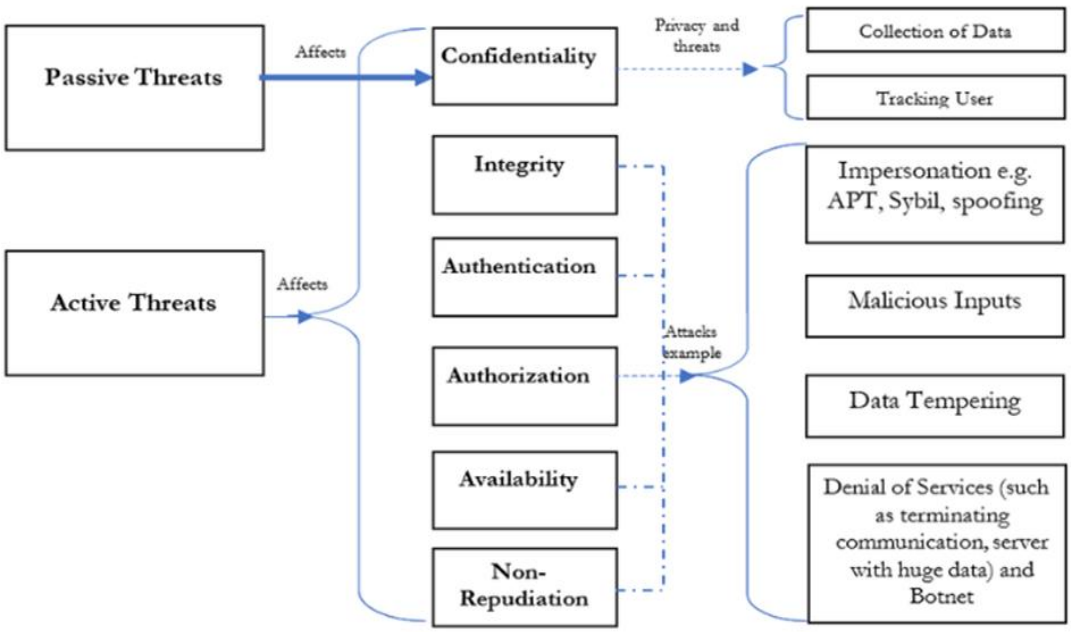


Fig3.2: Basic types of Security Attacks

3.3 Security Policies

Security policy takes an active part in a network. When policy is formulated after the topology and workings of its subnets have been well understood it results in a much safer and faster converging network.

3.3.1Authority of resources

The accreditation of systems or networks, and the assets that relate to the legitimacy of them, play a significant security measure backstop in a counter system. And after quite reasonable scan of the net we could possibly suggest an adequate degree of authorization of the resources of the system. A policy that is used in antivirus or the list of routers or firewalls can impose an authority for proper network usage**.**

3.3.2 Detect malicious activities

consequently, intrusion detection system is an important component of a security countermeasure. Successful and comparing the contents of the log files with the suspicious

activities in a network can redeemed a system. Compared to numerous other malign aims, it provides a futuristic safety stance.

3.3.3 Mitigate possible attacks

Communication flow at every stage of the attack gives information of which kind of protection is required for a system against that attack. From the above work, it can be suggested that we can change or modify the parameter of the security system through generating a strong resistive block against the attack.

3.4 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).

3.4.1 DOS Attack

DoS attacks involve pinpointing a target and flooding them, thus making them unresponsive or taking so long to reply that the end users considering them legitimate cannot wait. The attackers overwhelm the target system with traffic making it impossible for normal operation to take place. Such attacks can be directed at a single computer, or an entire network and can invade or egress traffic.

Common DoS attacks include:

1. Ping of Death: Continued sending of ping requests to until they crash.
2. YN Flood: The attacker begins the connection by sending a SYN request to the target but does not establish a connection, with many half-open connections that must be filled in the server’s connection table.

3.4.2 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 systems control with different software like Trino and Shaft. Example of DDOS attacks are SMURF 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. In Fig 3.3 about Distributed Denial of Service Attack.

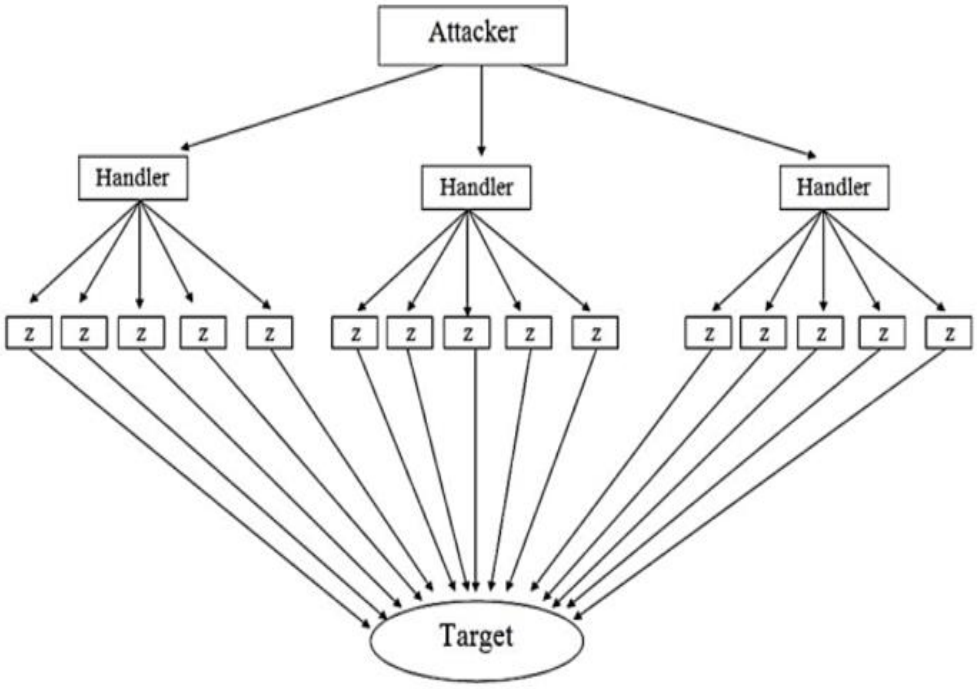


Fig 3.3: Distributed Denial of Service Attack

CHAPTER 4
SECURITY SOLUTIONS

4.1 TLS 1.3

TLS 1.3 is the planned upgradation of Transport Layer Security (TLS), the chief purpose of which is the protection of connection-oriented communication over networks. While TLS 1.4 is yet to be implemented (as of my knowledge cutoff in 2023) but it is predicted that it will have better security features added to it and better performance than TLS 1.2.

Stronger Encryption:

In TLS 1.3, attempts are planned to improve encryption paradigms to counter further advanced attacks. It shall also cover post of use of post-quantum cryptography algorithms to ensure communications are safe from threats associated with quantum computers.

Faster Handshakes:

Expanding on the relatively simplified TLS 1.2 handshake, TLS 1.3is anticipated to further optimize the handshake process for much faster connections while keeping latency low

Improved Privacy:

Some expected advancements in the coming TLS 1.3 are likely to enhance the protection of user data possibly with an enhanced forward secrecy as well as traffic analysis countermeasures.

4.2 SASE (Secure Access Service Edge)

SASE is a new cloud-first platform that MARGIN summarizes enterprise network security and large-scale networking, known as WAN. Stemming from Gartner it was first introduced in 2019 and is intended to deliver trusted and optimized application and data access irrespective of the user's physical location or location of the hosted resources. SASE consolidates multiple security functions such as Secure Web Gateway, Zero Trust Network Access, CASB, and Firewall as a Service and comprehensive network functionality

through SD WAN. It empowers cloud-first, as well as the remote and distributed working model, and hence offers improved security, speed, and flexibility

- SD-WAN (Software-Defined WAN):
  This in turn leads to improved access, secure and reliable access to branch offices, remote users and cloud services. SD-WAN provides the option of performing adaptive path selection, traffic flow, and WAN control in a unified manner.
- Zero Trust Network Access (ZTNA):
  ZTNA polices that only genuine legitimated user, devices, and applications are allowed to access the network resources. This concept is critical for implementing Information Security “never trust, always verify” best practices.
- Secure Web Gateway (SWG):
  Keeps its users safe from all internet threats, filters traffic, scans for viruses and other dangers, and blocks access to dangerous sites and data leakage.
- Firewall as a Service:
  A type of a firewall that enables the provision of web traffic filtering, protection against intrusions as well as threat identification through a-cloud based delivery model.
- Data Loss Prevention (DLP):
  An effective human component for guaranteeing that sensitive information is administered in a proper way and it is not leaked from the organization to the external environment, significantly where the use of cloud services is expected.

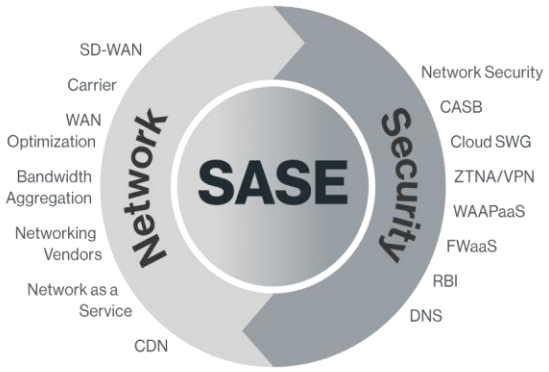


Fig4.1: SASE architecture

4.2.1Key Benefits of SASE:

simplified Network and Security Management:

SASE consolidates multiple security services to form an architecture that eliminates overhead, fosters cost savings, and offers architectural coordination and management of the complete network and security plane.

Improved User Experience:

SASE can allow to connect users to applications and resources in a secure and optimal fashion regardless the location and it enhances the usage of cloud solutions as well as work from home requirements.

Cost Efficiency:

SASE can help to decrease the use of standalone point solutions for such activities as SD-WAN, firewalls and web content filtering and access.

Scalability and Flexibility:

This is so because the SASE can naturally grow with the organization as the amount of traffic or security requirements increases over time.

4.2.2 SASE vs. Traditional Networking & Security

Traditional Networking: Usually depends on the centralized data centers and appliances, for instance, firewalls hardware, VPN.

SASE: A cloud-based focus for policy enforcement is achieved to deliver security closer to the user and the applications that need to be used.

4.3 MACsec (Media Access Control Security)

MACsec is a security technology that intends to enable protection of data flowing through Ethernet channels by offering encryption at the data link layer of OSI model. It provides privacy, accuracy and trustworthiness in the process of data transmission for the local area network (LAN) or even between switches.

4.3.1 Key Features of MACsec:

1. Transforms the data that is exchanged between devices so as to guarantee that it is not intercepted by other devises.
2. Ensures the received and transmitted data are of high standard, and are genuine.
3. Common in data center networks, enterprise backbone networks, or between switches to secure the data against intruders.

4.3.2 MAC (Media Access Control) in network devices

Overview: MAC stands for Media Access Control is a for 48 bit identifier assigned to network interfaces that work at the second layer of OSI model.

Security Context: At times it is applied for network control, where certain devices are permitted or denied about the connection to the network depending on the MAC address of their local adapter. But this is typically not effective security measure in isolation since MAC addresses can be easily faked.

4.3.3 Benefits of MACsec Over Traditional Security

1. Layer 2 Protection: It is essential to mention two things about traditional network security – firstly, quite often it is limited to upper OSI layers (transport and application mostly), while MACsec is a Layer 2 technology by design. This means that before even getting out of the local network; whether to another switch or a router, or the devices; the traffic is shielded.
2. No Impact on Application Layer: MACsec works at the MAC layer, and interconnects with application or other service layers without relying on different application protocols. This can be really useful in preserving the applications or protocols that do not include encryption in their design.
3. Secure Physical Network Infrastructure: MACsec entails that even the physically imbedded elements of a network such as Ethernet cables and switches are protected from dangers such as man-in-the-middle or DDoS attacks or manipulation.
4. Ideal for Data Centers and Enterprise LANs: MACsec is especially beneficial where fast transmission and minimum times for encryption and decryption are required including data centers, enterprise LANs and high performance computing.

CHAPTER 5
EXPERIMENTAL RESULTS AND DISCUSSION

5.1 Overview

As detail study of the network elements “hardware & Protocols”, we can find out the existence network vulnerabilities, which can be examined by a real-life office network.

5.2 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.

5.3 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 Host to Host

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. In Fig 5.1 show that Network Scenario diagram.

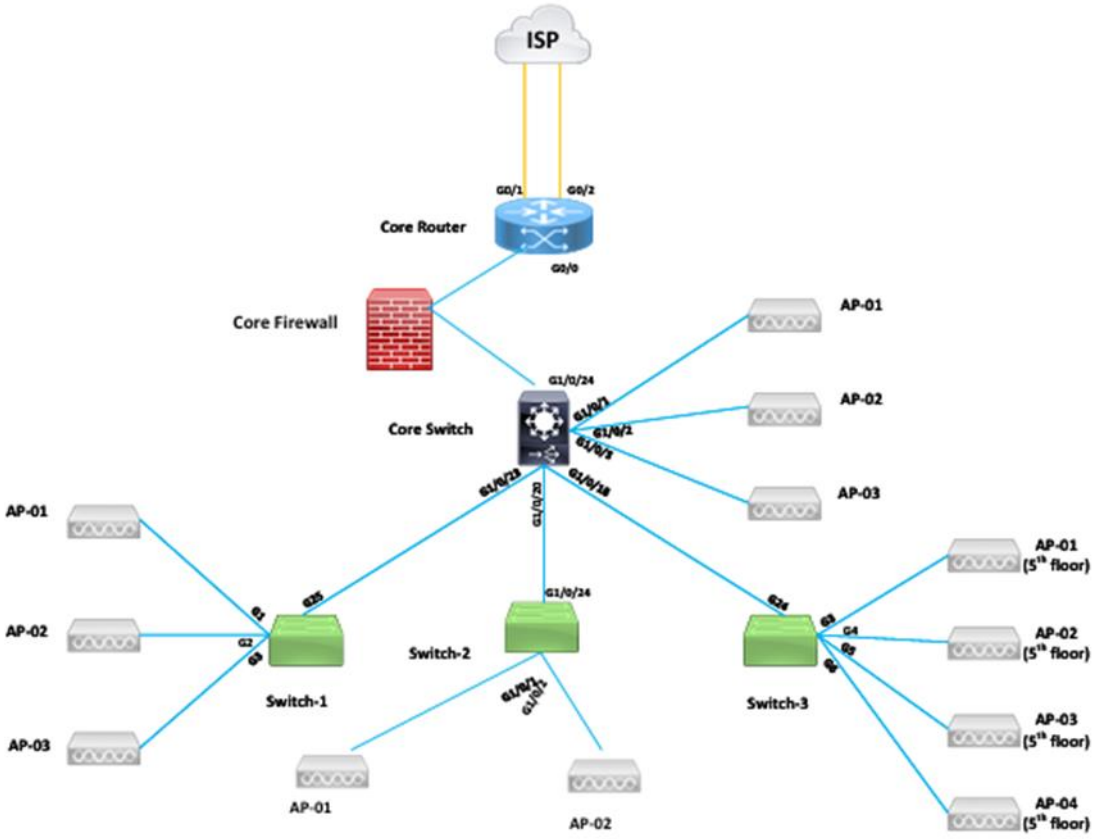


Fig 5.1: Network Scenario

5.4 Object Modules

NO	Object Name	Object Model	Object Module Description
1	Application	Application Config	Default Support (Access, Email, File Transfer FTP, File Print, File Transfer FTP, Video Conferencing, VOIP, Web Browsing HTTP)
2	Profile	Profile Config	Sample Profile: (Engineer (Web Browsing HTTP, Email, File Transfer FTP, File Transfer FTP)
3	VPN	IP VPN Config	Support VPN tunneling establishment between specific end routers
4	IP Config	IP VPN Config	
5	Internet	IP v4	Form ISP
6	Router	Port	IP based Gateway Router, support VPN connection.
7	Firewall	Port	Packet filter Firewall, allow and deny specific application through firewall across the two different network
8	Client 40-50	Ethernet Port Wireless	Laptop

Table 5.1: Object Modules

5.5 Applications/Services

In Client HTTP: Traffic Received (bytes/sec)

In Client FTP: Traffic Sent (bytes/sec)

5.6 Task Assignments

No	Client Title	Section	Job Description	Authorization Permission; Access/Deny Level
1	Client A	Network	Network/System Administrator	1. Permit: (HTTP traffic) Download/Access http traffic form server 2. Permit: (FTP Connection) Upload/Established FTP connection to sever
2	Client B	Network	Network Assistant	1. Permit: (HTTP traffic) Download/Access http traffic form server 2. Deny:(FTP connection) Upload/Established FTP connection to sever

Table 5.2: Task Assignments

5.7 Result

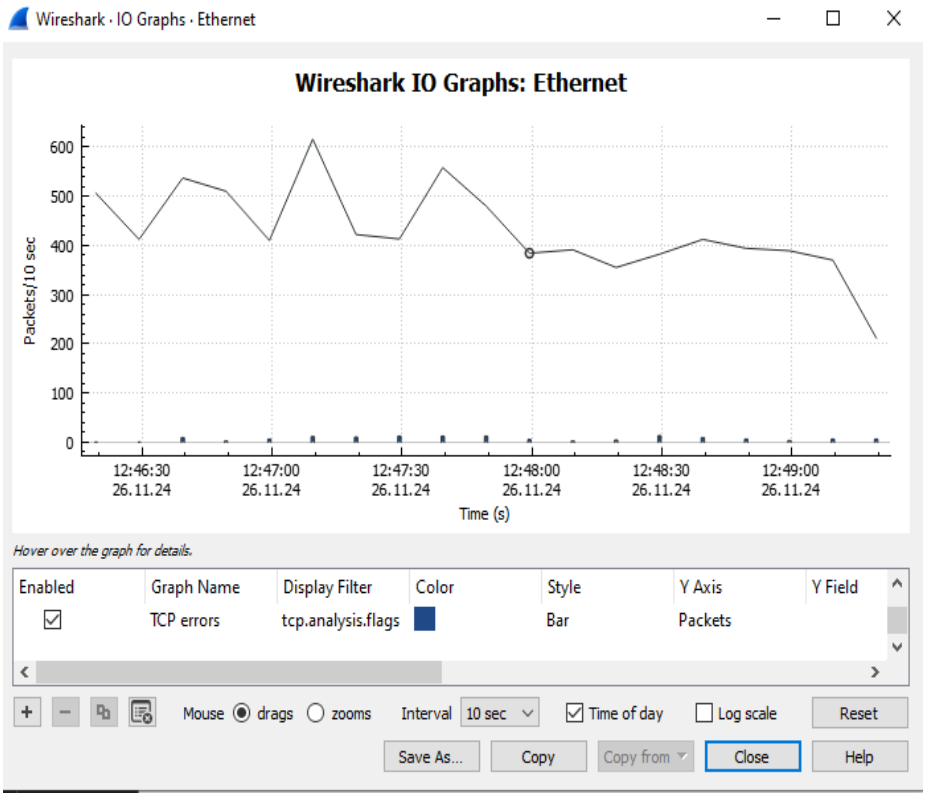


Fig 5.2: General Network (Default Mode)

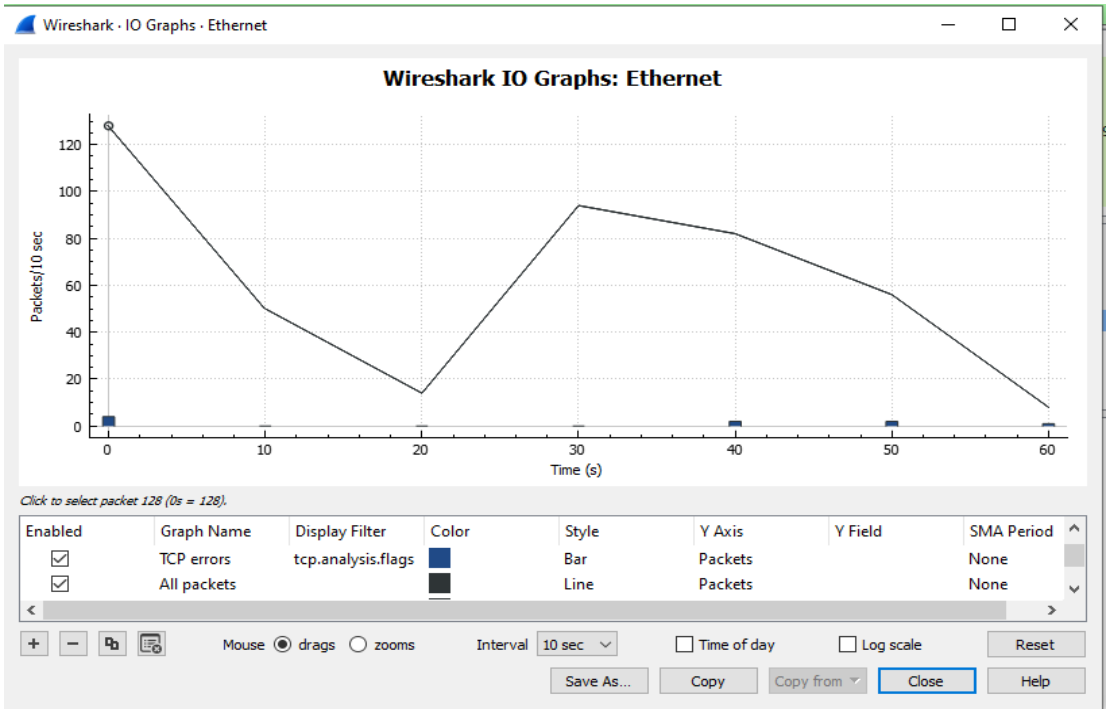


Fig 5.3: General Network (http traffic)

5.7.1 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 are allowed HTTP traffic from server where client A is "Network/System Admin", Client B "Network Assistant are allowed to see HTTP traffic. At the same time all of them loose access right to create FTP connection with the server to the clients. This is a good thing which fulfills our one need which was mentioned in DoD, but as per network requirement we also need access rights to establish a FTP connection with server for uploading any record=data to the server or updating server database through only one client which is a "Network/System Admin". However after implementing the above states network policy of the organization, we also relinquish the control of Client A.

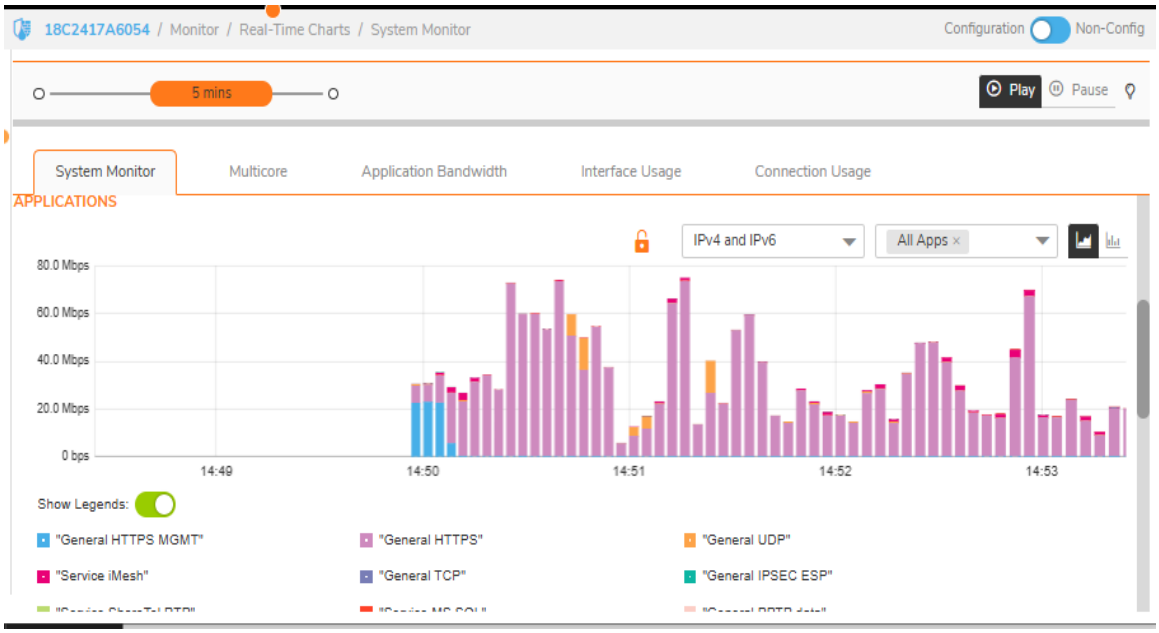


Fig 5.4: Firewall Based Network (System Monitor)

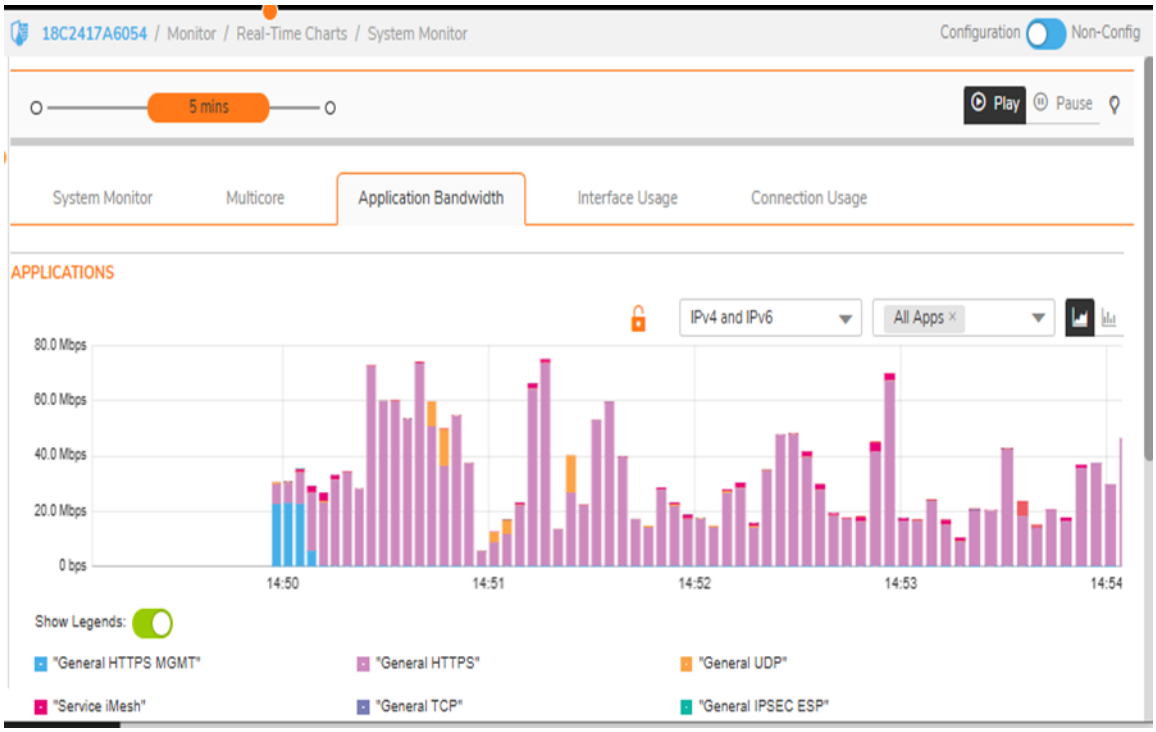


Fig 5.5: Firewall Based Network (Application Bandwidth)

5.8 Bandwidth Utilization

Here we have analyzed the effect 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.

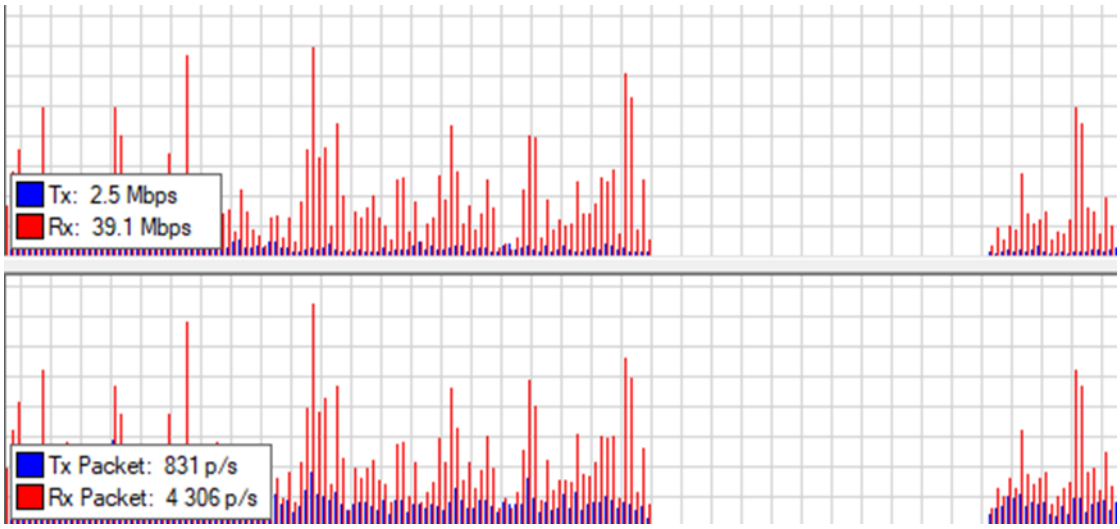


Fig 5.6 General Network(Total TX & RX Bandwidth)

CHAPTER 6

IMPACT ON SOCIETY, ENVIRONMENT AND SUSTAINABILITY

6.1 IMPACT ON SOCIETY

It is clear that network security plays an enormous role in social utility since it safeguards privacy, supports the economy, and guards necessary infrastructure. Trust in the technology lowers risks brought about by hackings, cybersecurity generates employment, and shields organizations against losses. But also in national security as it prevents cyber attacks on government and infrastructures systems. Still it poses questions of ethical and legal concern like privacy and security. In addition, as moving to the world of operational and technical networks develops, network security helps to minimize digital divide, and provide international cooperation and while such problems as, for instance, fake news, ranked interference with the elections, environmental issues by developing further.

6.2 IMPACT ON ENVIRONMENT

The influence of network security on the environment is mainly shown through the use of energy resources in data centers and other facilities that support the network security controls such as encryption, firewall, and monitoring devices. Data centres are known to be power hungry and many are equipped with cooling mechanisms adding to the carbon footprint and electronics waste. Since cyber security requirements increases with the progress of digital age, so does the energy requirement. Although, such initiatives as the existence of energy-efficient data centers utilizing renewable energy and following green IT practices are attempted for environmental mitigation of network security. There is a shift on how companies within the tech industry look at how they can have strong cybersecurity defenses and be sustainable at the same time.

6.3 Sustainability Plan

A Sustainability Plan for Network Security is centred on reducing the effects of security on the environment while providing substantial protection. Key elements include:

1. Energy-Efficient Infrastructure: Select energy proportional servers, storage and network devices. In this model, use of virtualization to ensure that resources are utilized in the best way possible without requiring addition of more hardware.
2. Renewable Energy: Extinguish carbon footprints To reduce carbon footprints influence power data centers and security operations with the renewable energy source, such as solar and wind.
3. Cloud-Based Security Solutions: Common pool technologies to support cloud services so as to minimize resource energy use and hardware deployment.
4. Optimized Security Practices: Create security policies which help offload computational work, or utilize preferred encryption types or compact control instruments.
5. E-Waste Reduction: Make reuse of old hardware by seeking codes for responsible disposal of the outdated gadgets and supporting initiatives geared at the management of products' cycle.
6. Collaboration for Green Standards: Partner with professional organizations to develop and establish appropriate, responsible cybersecurity measures as well as protections of the environment within their specific business.

When these practices have been incorporated, organizations run reduced risks on network threats while minimizing their effects on the environment.

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 CONCLUSION

The plan of this thesis is to discover threats in the network, compare types of attacks, and assess security. Security is not about a particular product, including firewalls, antivirus programs; it is about sound, proper practices which include the use of a new password weekly, proper configuration of the firewalls, and proper upgrade of the antivirus systems. Even security devices configured incorrectly are a worse case than having no security devices at all as evidenced in simulations where the security devices defaulted and misconfigured ones let in unauthorized access in network operations.

Although, no network can be made entirely secure, information security assessment can be done frequently and flaws found can be dealt with. Security solutions, say firewalls, must first be evaluated on the platform for compatibility, dependability, capacity for greater expansion, and preparedness for future advancement.

Conveniently enough, Sun Tzu in The Art of War also never stated that security was the aim of making oneself safe from an attack, but rather, the goal is to be prepared and make one's network virtually invulnerable.

7.2 Future Work

They revealed that today's major problem is not the IT security technology but how to implement the right procedure and control to attain the IT security desired. Hackers will still be around in the market while they appear to be multiplying in some measure. IT trends emerging in the market will be taking the world to some extent, where computers are currently doing much more than what they are doing in the present scenario. There is no technology development stay stagnant. Malicious tools will remain active, as will security

tools, attacking tools will also progress as will security tools. If someone wants to learn about every new threat soon he/she will be stress. It is more desirable to seek for significant threats and thereby attempt to address them with existing tools.

RRFERENCES

[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:

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

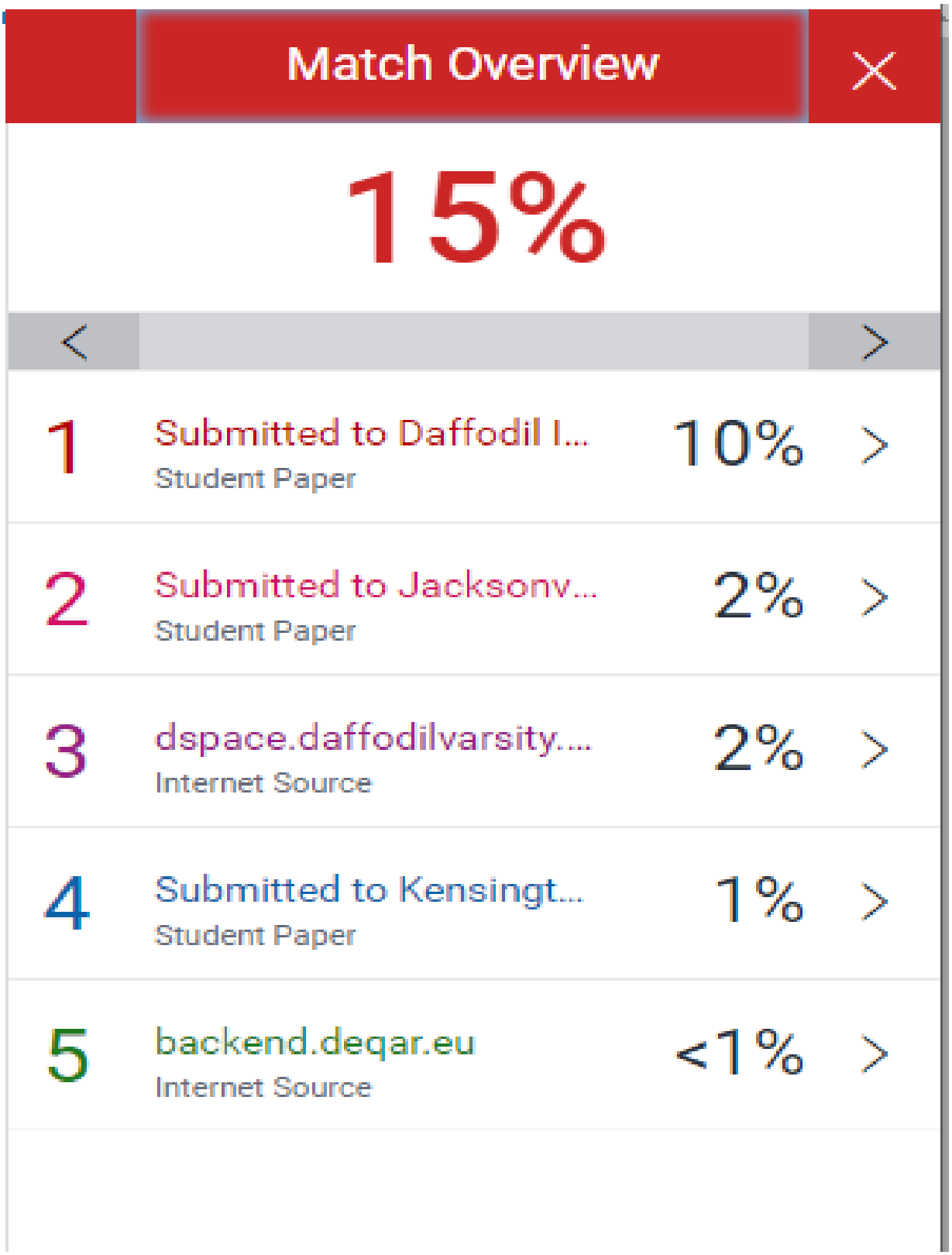
[37] Dr. K.Duraiswamy and Mrs. R.Uma Rani “Security Through Obscurity“ http://www.rootsecure.net/content/downloads/pdf/security_through_obscurity.pdf

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

[38] 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

[39] “Unauthorized Network access becomes a felony”,

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


Match Overview
15%
1
Submitted to Daffodil I...
Student Paper
10%
2
Submitted to Jacksonv...
Student Paper
2%
3
dspace.daffodilvarsity....
Internet Source
2%
4
Submitted to Kensingt...
Student Paper
1%
5
backend.deqar.eu
Internet Source
<1%