A Study of Network security and the role of Cryptography in network security

V. Bhagya sree[1], M.M.Asha[2], S. Kokila[3] C.Sonika[4], R.Ramya[5], P.Leelavathi[6]

[1,2,3,4,5,6]*CSE, Sreenivasa Institute of Technology and Management Studies, India*

ABSTRACT

With the increase in e-commerce applications and social networks, organizations across the world generate a huge amount of data daily so there is a challenge to send the data in secure. Network Security means sending information without any modification or hacking done by unauthorized users. Network security is a approach of attaining data through wireless transmission with the help of cryptography. The task of securing data while transmission, avoid unauthorized access of data, avoids data misuse and modification of network resources was performed by network administrator. Network security is used in diverse computer network sectors such as private and public. Networks used in the institutions, enterprises, institutions etc. in the form of private or public. Cryptography is the approach of securing data with the help of secret keys. Cryptography means encryption and decryption of data with secret keys using various algorithms. This paper discusses the detail study of network security.

Keywords- *Cryptography, Decryption, Encryption, Network Security, Network Security tools*

I. INTRODUCTION

Network security measures are needed to protect data during their transmission it includes both hardware and software technologies and it targets a variety of threat and stops them from entering or spreading on your network. Requires network servers for physical protection and devices from external threats. Enforcing network security measures it allows computers, users and programs to perform their permitted critical functions within a secure environment. Government agencies and businesses use highly skilled information security analysts to implement security plans and constantly monitor the efficacy of these plans. Cryptography is a key technology to achieve information security in communications, computer systems, electronic commerce, and in the emerging information society. Unauthorized access should be prevented. Network security is actual part of information security.

II. NETWORK SECURITY

Network security consists of Security: Configure your systems and networks as correctly as possible, Detection: Identify when the configuration has changed or when some network traffic indicates a problem, Reaction: After identification of problems quickly, you must respond to them and return to a safe state as rapidly as possible [2]

1. The importance of network security is to

1.1 To protect the computers in the network: Computer systems and other devices connected to unsecured networks are highly vulnerable to external threats such as malware, ransom ware and spyware attacks. A single attack can do the entire computer system of an organization and compromise your personal information. With the assistance of a network security specialist we can assure the security of the network and you can stay away from such expensive threats.

1.2 Prevention of identity theft: Regardless whether you are an organization or an individual, your identity is valuable. Suppose if you log in an unsecured network then your identity can become visible to third-parties. To bypass such a situation, you should secure your network. Such a way becomes mandatory if you are a business that deals with client information.

1.3 Protection of shared data: If the data is regarding to a business then special precautions should be taken to protect shared data. So the network security is one of the best ways to do so. Network security can be practiced with different restrictions on different computers depending on the types of files they handle.

1.4 To stabilize the network connection: The activity of network becomes too heavy in an unrestricted, unprotected network. Acute traffic can lead to an unstable computer network and it leads to the entire network will be exposed to various external attacks.

2. How to guarantee network security?

In order to guarantee network security follow the below steps

2.1 Change the router password

Once the network setup is completed change the default service identifiers because hackers can easily track these credentials. To avoid this situation change your password at your earliest.

2.2 Activate encryption

Have to activate a strong encryption on your router it is the most important things you should do. For Wi-Fi connections can activate WPA2 encryption

2.3 Enable advanced authentication methods

Enabling the MAC address filtering is the advanced method for securing your network. Network card (Wired and Wi-Fi) has a unique MAC address with this setting in your router will allow you to allow only specific MAC addresses to connect to your network. These are some of the most common network hazards

1. Improperly installation of hardware or software
2. If no proper updating of Operating systems or firmware
3. Misused hardware or software
4. Poor physical security
5. Insecure passwords
6. Design errors in a device’s operating system or in the network

2.4 Physical Security Considerations

Safety considerations involve the following:

1. Storage of network servers and devices in a secure location
2. Refusing open access to that location to members of your organization
3. To detect anyone who attempts to access that location can be detected by video

Surveillance.

III. NETWORK SECURITY ATTACKS

Illegal access of data against private, corporate or governmental IT assets in order to destroy them, modify them or steal sensitive data is referred as network attack. Mainly two types of network attacks are there they are

- Attackers gets access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact this type is refereed as passive attack
- Attackers not only gets unauthorized access but also modify data, either deleting, encrypting or otherwise harming it is referred as active attack [7]

Network attacks are differentiated from several other types of attacks:

1. Got unauthorized access to user devices, servers or other endpoints, typically compromising them by infecting them with malware is called as End point attacks

2. Malware is used to infecting IT resources and allowing attackers to compromise systems, steal data and do damage. These also include ransom ware attacks and this is referred as Malware attacks

3. Vulnerabilities, exploits and attacks are using vulnerabilities in software used in the organization, to gain unauthorized access, compromise or sabotage systems.

4. These are complex multilayered threats, which include network attacks but also other attack types is called advanced persistent threats

3.1 What are the Common Types of Network Attacks?

Following are common Types of Network Attacks.

3.1.1 Unauthorized access

Attackers using a network without receiving permission are called unauthorized access. Unauthorized access are weak passwords, lacking protection against social engineering, previously compromised accounts, and insider threats.

3.1.2 DDoS attacks

Distributed Network Attacks or Distributed Denial of Service (DDoS) attacks is refereed as same. This attack targets server, websites and online services and avoids the website from functioning correctly. DDoS attacks comprises Internet shopping sites, Online casinos, Any business or organization that depends on providing online services

3.1.3 Man in the middle attacks (MITM)

This attack happens when a offender positions himself in a conversation between a user and an application either to listen in or to imitate one of the parties, making it to show as if a normal exchange of information is underway The objective of an attack is to take away personal information, such as login details and credit card numbers.

3.1.4 Code and SQL injection attacks

This is referred as SQLI and it is a common attack vector that uses wicked SQL code for backend database manipulation to access information that was not intended to be displayed. This information may includes private secret information of company data, user lists or private customer details

3.1.5 Privilege escalation

Once attackers enter s into network, they can use opportunity increase to expand their reach. Horizontal right escalation involves attackers gaining access to additional, adjacent systems, and vertical escalation means attackers gain a higher level of privileges for the same systems.

3.1.6 Insider threats

A network is especially helpless to malicious insiders, who already have privileged access to organizational systems. These threats are hard to detect and protect against, because insiders do not need to penetrate the network in order to do harm. New technologies like User and Even Behavioral Analytics (UEBA) can help identify suspicious behavior by internal users, which can help identify insider attacks.

IV. TYPES OF NETWORK SECURITY TOOLS

The types of network security tools are

4.1. Antivirus and Antimalware Software

It is used to protect against malware, which encompass spyware, ransom ware, Trojans, worms, and viruses. It can contaminate a network when it enters to network and then remain calm for days or even weeks. This type of threat is handled by scanning for malware entry and regularly tracks files afterward in order to detect anomalies, remove malware, and fix damage.

4.2 Application Security

This is required since no app is created perfectly. It is possible for any application to contain of vulnerabilities, or holes, that are used by attackers to enter your network. It encompasses the software, hardware, and processes you select for closing those holes.

4.3 Behavioral Analytics

In order to find abnormal network actions must know what normal network actions looks like. This tool is able to automatically find sensitive activities that deviate from the norm. Security team will be able handle efficiently detect indicators of compromise that pose a potential problem and rapidly remediate threats.

4.4 Data Loss Prevention (DLP)

Organization Company should provide security that their staff does not send sensitive information outside the network. Usage of data loss prevention technologies, network security measures that prevent people from uploading, forwarding, or even printing vital information in an unsafe manner

4.5 Email Security

It plays a crucial role in network security. Number of threats like scams, phishing, malware, and suspicious links, can be attached to or incorporated into emails. Email includes personal information in order to ensure person identity; It is important for an employee to undergo security awareness training to identify authorized Email

4.6 Firewalls

Actually, firewalls are caretaker between a network and the internet. They check sender data packets some times and receiver data packets with standard rules and policies, thereby avoiding threats from intruding the network

4.7 Intrusion Prevention System (IPS)

IPS checks traffic in the network which is used to drop attacks. It includes rules and measures which can be used against the attacks, As the internet is highly insecure Internet protection system is one of the best way to protect the data from the attacks

4.8 Mobile Device Security

Now-a-days, criminals over the internet called as the cyber criminals concentrate on Mobile apps and devices. Organizations of IT will soon support applications that are on personal mobile devices. It is important for an individual to control which devices can have access to their network. It is important for the people to know about the network configuration details in order to verify the network traffic

4.9 Network Segmentation

Segmentation of the network puts network traffic into many classifications and enforces security policies a lot easier. Classifications are really based on endpoint identity, rather than IP addresses. Authorized users can be accessed based on location, role, and more so that the authorized people get the right level of access and unauthorized users are blocked.

4.10 Security Information and Event Management (SIEM)

SIEM include products which offer security for the information of the user in order to recognize and reply to threats. SIEM products are available as both virtual and physical appliances server software

4.11 Virtual Private Network (VPN)

This tool is capable of encrypting the data transmission between a client or an endpoint and the network or internet. VPN uses secure socket layer or IPsec in order to authorize the data communication between endpoint and network.

4.12 Web Security

An employee’s web use will be managed with the help of web security which will not allow the access of suspicious websites and blocks malicious websites

4.13 Wireless Security

Wireless networks are not secure as wired networks and this helps the intruders to attack the network easily. It is important for a wireless network to be strong so that security is maintained. While installing a wireless LAN it is important to place Ethernet ports everywhere. There are some products that are specially designed for protecting a wireless network to control data loss

4.14 Endpoint Security

Used to protect corporate networks when accessed through distant devices such as laptops or several other wireless devices and mobile devices.

4.15 Network Access Control (NAC)

It helps to recognize who can have access to the network. It identifies each authorized user in order to avoid potential attackers.NAC helps to maintain security policies. Authorized users will have limited access

4.16 Technical Network Protection

Used to protect stored and in-transit data from unauthorized software and unauthorized users

4.17 Physical Network Protection

This tool is used to avoid physical interference of the intruder, so that intruder can not attack the physical components of the network. Example components of physical network protection are Door locks and ID passes.

4.18 Administrative Network Protection

It is a security method which deals with network access and network behavior. It includes a process that operates for IT officers, when there is a change in infrastructure this tool incorporates change are Forms of Administrative network protection are Company policies and procedures

V. NETWORK PROTECTION TIPS

Few general network protection tips and best practices that should be followed. Below is a very basic overview of some of the most important should take to ensure network security [7]

Grant Access Carefully

Permission Access to network or servers should be given carefully so that unauthorized persons cannot access the network

Follow Password Best Practices

When you are setting a password use unique passwords so that security is provided to network. A password should not be given in an easy or previously used password. All employees also should follow the rules when setting password for their work accounts so that it can help to keep everyone's data safe.

5.1 Secure Servers and Devices

Place the servers in the secure room or secure area and permission should be given only to authorized persons to access that location. Monitor when the room is not locked or when the server or devices is placed in unsecured place

5.2 Test Your Security

Although our network is full of secured way we should perform testing continuously and troubleshoot the network so that if any suspicious is identified can be immediately fixed. If any updates are given that can be installed .Data backup procedure has to be followed so that if any data loss occurred we can solve the problem easily. Network security plays a crucial role in today's environment so all the IT professional should be aware of all the latest security issues and threats by attending training which helps in continual education.

VI. NETWORK TROUBLESHOOTING APPLICATIONS

In addition to tools there are various independent applications which are be installed separately when working with the system to find the status of the network and to troubleshoot issues. They are

6.1 **Packet Sniffer**:

It is the procedure of capturing each packet that is transmitted over the network and analyzing its content. Mostly it is used to troubleshoot network problems or to gather network statistics.

6.2 **Port Scanner:**

To determine which ports on a network are open or close can be identified by using port scanner. Port scanner is used to analyze which ports are in use and identify points in a network that could be vulnerable to outside attacks

6.3 **Protocol Analyzer**:

Combines diagnostic and reporting capabilities to provide a complete view of an organization's network. Analyzers can be used to troubleshoot network problems and detect interference into your network

6.4 **Wi-Fi Analyzer**:

WiFi analyzer tool provides the detailed information on WiFi networks including hidden ones. It analyzes the performance and it helps to troubleshoot problems in network connectivity over a wireless network.

6.5 **Bandwidth Speed Tester**:

This tool is used to Test the bandwidth and latency of a internet connection. It is normally accessed through a third-party website and can be used to confirm user reports about slow connections or download speeds.

VII. THE ROLE OF CRYPTOGRAPHY IN INFORMATION SECURITY

Method of securing information and connections through use of codes so that only those person for whom the information is proposed can understand it and process it is refereed as cryptography. In cryptography “crypt” means “secreted” and suffix graphy means “script”. Study of cryptography is referred as cryptology. The process of converting data in to a code is called encryption. Decryption is a procedure which converts encrypted or converted data to original data. In Cryptography algorithm is the technique used to protect information and this is obtained from mathematical concepts and a set of rule based calculations which converts messages very difficult to decode it. Key generation by cryptographic, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions are made with the help of these algorithms [3]

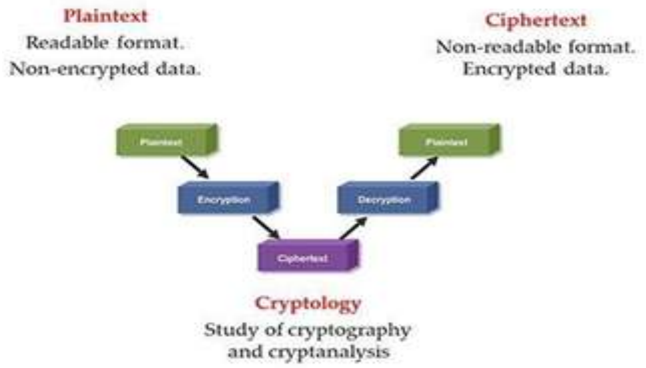

Fig: Cryptography

7.1 **Features Of Cryptography are as follows:**

7.1.1. Confidentiality

Confidentiality refers to authorized access of information which can be accessed by the intended recipient and no other except intended recipient can access it.

7.1.2. Integrity

Integrity ensures that other information or data cannot be modified in stored data or transition data between sender and intended receiver without information being detected or checked.

7.1.3. Non-repudiation:

The sender cannot deny his intention to send information at later stage where there is a need to resend the information

7.1.4. Authentication:

Sender and receiver identities are verified and confirmed and the destination address for the information is also confirmed so that the data reaches the authenticated user.

7.2 **Types of Cryptography:**

There are three types of cryptography:

7.2.1 Symmetric Key Cryptography

It is a system of encryption where the sender and receiver uses a single of message use a single key which is common to both sender and receiver to encrypt and decrypt messages. Symmetric Key cryptographic systems are simple and fast but the problem is in exchanging the key in a secured way. The most popular and widely used symmetric key cryptography system is Data Encryption System(DES).

7.2.2 Hash Functions

Predetermined length hash value is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Passwords are encrypted in many operating systems with the help of hash functions

7.2.3 Asymmetric Key Cryptography

This system uses a pair of keys to encrypt and decrypt messages. For encryption public key is used and a private key is used for decryption. Public key and Private Key are different. Public key is known by everyone but private key is known only by the intended receiver so that receiver can be able to decode the information sent by the sender

7.3 **What problems does cryptography solve?**

- Data in transit as well as idle data's confidentiality and integrity can be assured with cryptography. Senders and recipients authentication to one another and protect against repudiation can be solved by cryptography
- Communication systems have multiple clients and servers. Data transmission takes place through networks that are not trusted. Transmission occurs over public network , the Internet, or private networks which includes external attackers or malicious insiders.
- Cryptography protects data transmission that occurs in unsecured networks
- Cryptographic rules offers security through SSL/TLS which can secure data from unsecured eavesdropping and tampering.
- Data on a removable disk or in a database can be encrypted to prevent revelation of sensitive data should the physical media be lost or stolen. And it can also provide integrity protection of data at rest to detect malicious tampering.

VIII. CONCLUSION

The learning of Network security is an significant which is growing more and more consideration as the internet is developing. The network security threat should be considered to determine the security technology which includes mostly software based, as well as many hardware devices. In addition it consists of the necessities made in an primary computer network communications, strategies adopted by the network administrator to protect the network and the network-accessible resources from illegal access and the effectiveness (or lack) of these measures combined together. To provide a secured network means we need to consider Confidentiality, Authentication, Integrity, and Authorization. The strategy should be developed by considering security problems, potential attackers, needed level of security, and factors that make a network vulnerable to attack. Tools to lessen the weakness of the computer to the network include encryption, authentication mechanisms, intrusion, detection, security management and firewalls. In addition to securing the network from outside issues, imposing organization network usage measures can avoid internal users from pulling in threats due to misuse.

REFERENCES

[1] R.Achary, *Cryptography and Network Security: An Introduction,ISBN-978-1-68392-691-7*

[2] Dr. C.H.Patil, Ms.Vinaya Kulkarni, Ms.Shivali Kirdat , Ms.Sneha Patil ,*Study on Network Security Algorithm, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, ICSITS - 2020 Conference Proceedings*

[3] Kaur, S., Kaur, R., & Raina, C.K, *Review on Network Security and Cryptography,2017*.

[4] Shyam Nandan Kumar, *Review on Network Security and Cryptography, ITECES,2015,3(1)*

[5] Behrouz.A.Foro uzan , *Data Communication and Networking , 4 th.edition*

[6] William Stallings,"*Cryptography and Network Security Principle and Practice*",*Fifth Edition,2011*.

[7] Jie Wang,"*Computer Network Security: Theory and Practice",Second Edition,2006*.

[8] Bellare, Mihir; Canetti, Ran; Krawczyk, Hugo, *"Hash Functions for Message Authentication",1996.*

[9] Kumar, S. N. *Review on network security and cryptography*. *International Transaction of Electrical and Computer Engineers System, 2015.*

[10] Mohan V. Pawar, Anuradha J, *Network Security and Types of Attacks in Network, Procedia Computer Science 48 (2015) 503 – 506*