ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 12, December 2024

Network Security and Measures

[1] Kanishk, [2] Gaurav Shukla, [3] Poorvi Parashar, [4] Vishakha Chaudhary

[1] [2] [3] [4] CSE Department, Dronacharya Group of Institute, Greater Noida

Corresponding Author Email: [1] kanishk999111sorout@gmail.com, [2] shuklasanskar75@gmail.com, [3] poorviparashar2024@gmail.com, [4] chaudharyvishakha45@gmail.com

***Abstract*— These days, a secure network is essential for any business. Growing security risks are making internet services and high-speed wired and wireless networks more unstable and insecure. Security precautions are now more important than ever in order to satisfy the creative demands of growing companies. In industries like defense, where secure and authenticated resource access are the primary information security issues, the necessity is also urged. The important procedures and requirements related to important industry/organizational needs for establishing a secure network have been described by the paper's author. Wi-Fi networks are popular because they allow devices to connect wirelessly and provide network access to a wide range of resources. Numerous standards are needed to address Wi-Fi threats and network hacking attempts. This article looks at important security practices related to different network scenarios in order to establish a totally safe network environment within a corporation.**

***Index Terms*— Security precautions, secure network, Internet services, Growing companies, Internet services.**

I. INTRODUCTION

The protection of networks and their services against unauthorised modification, destruction, or disclosure, as well as the guarantee that the network functions properly in emergency situations and does not negatively impact users or employees, is known as network security. In order to prevent unwanted access to the network and its accessible resources, the network administrator has implemented policies and set provisions in the underlying computer network infrastructure.

II. TYPES OF NETWORK SECURITY PROBLEMS

There are mainly two kinds of computer security problems:

1) threats to information in the system
2) threats to equipment in the system

The computer system is influenced by a variety of causes, some of which may be purposeful, while network communication may be inadvertent, man-made, non-man-made, or the result of environmental influences. In general, the following are the risks to computer system security:

- Data theft
- Trojan horse virus
- Vulnerabilities
- Mobile threat
- Electromagnetic interference

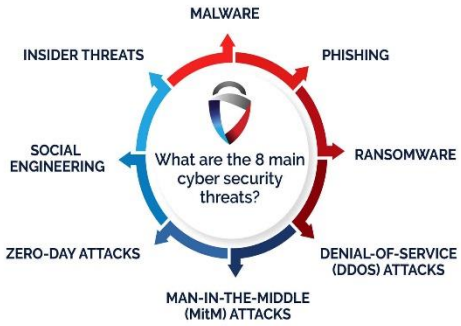


Fig. 1. Types of computer network security threats

III. THE FOLLOWING SUCCINCTLY DESCRIBES THE RESTRICTIONS OF NETWORK SECURITY DESIGN

A. Security Attacks

The following categories can be used to group security attacks:

Passive Attacks:

Attempts to compromise the system using observed data are included in this category of attacks. Plain text assaults, in which the attacker already knows both the plain text and the ciphertext, are an example of a passive attack

The attributes of passive attacks are as follows:

- Interception: attacks confidentiality such as eavesdropping, "man-in-the-middle" attacks.
- Traffic Analysis: attacks confidentiality, or anonymity. It can include trace back on a network, CRT radiation.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 12, December 2024

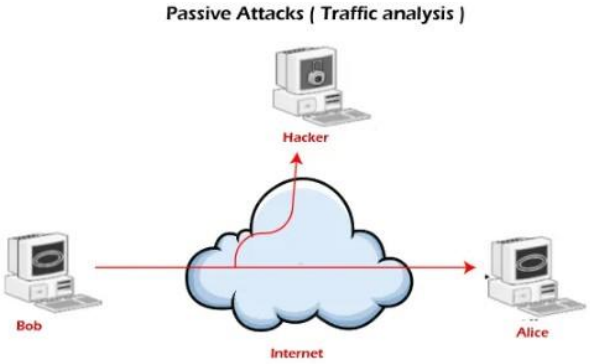


Fig. 2. Passive Attacks

Active Attacks:

For this kind of attack, the attacker must either stop the data stream in one or both ways or send data to one or both sides.

The attributes of active attacks are as follows:

- Interruption: attacks availability such as denial-of-service attacks.
- Modification: attacks integrity. • Fabrication: attacks authenticity.

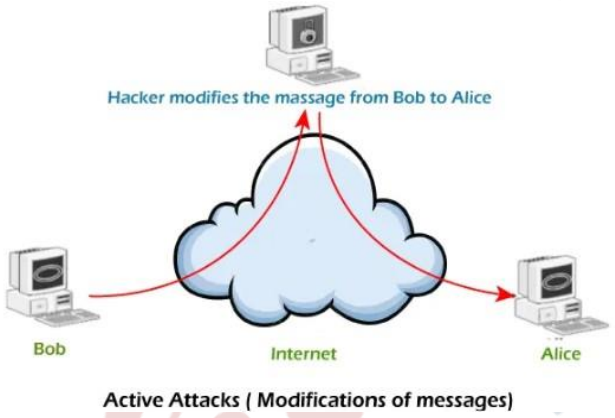


Fig. 3. Active Attacks

B. Network Security Measures:

Following measures are to be taken to secure the network:

1. A strong Antivirus software package and Internet Security Software package should be installed.
2. Prepare a network analyzer or network monitor and use it when needed.
3. Fire asphyxiators can be used for fire-sensitive areas like server rooms and security rooms.
4. Security barriers to restrict the organization's perimeter.
5. A strong firewall and proxy to be used to keep unwanted people out.
6. For authentication, use strong passwords and change it on a weekly/bi-weekly basis.
7. When using a wireless connection, use a robust password.
8. Employees should be cautious about physical security.
9. Implementation of physical security measures like closed circuit television for entry areas and restricted zones.

C. Network Security Tools:

Following tools are used to secure the network:

- Net Cat is a simple utility that reads and writes data across TCP or UDP network connections.
- Wire shark or Ethereal is an open source network protocol analyzer for UNIX and Windows.
- N-map Security Scanner is a free and open source utility for network exploration or security auditing.
- Nessus is the best free network vulnerability scanner available.
- Kismet is a powerful wireless sniffer.
- Snort is light-weight network intrusion detection and prevention system excels at traffic analysis and packet logging on IP networks.

IV. PREVENTION MEASURES AND TECHNIQUES FOR THE FORMATION OF COMPUTER NETWORK SECURITY PROBLEMS

There are security hazards associated with each network service. How to reduce the danger is the issue. The following are the current countermeasures for network security protection:

A. Firewalls

A firewall is simply a group of components that collectively form a barrier between two networks. There arethree basic types of firewalls:

1. Application Gateways

As shown below, this is the initial firewall and is sometimes referred to as a proxy gateway. These do serve as proxy servers because they are composed of bastion hosts. The ISO/OSI Reference Model's Application Layer is where this software operates. To access Internet services, clients behind the firewall need to be ranked and categorized. This is the most secure since it prevents anything from flowing by default, but in order to start the traffic passing, programs must be developed and activated.

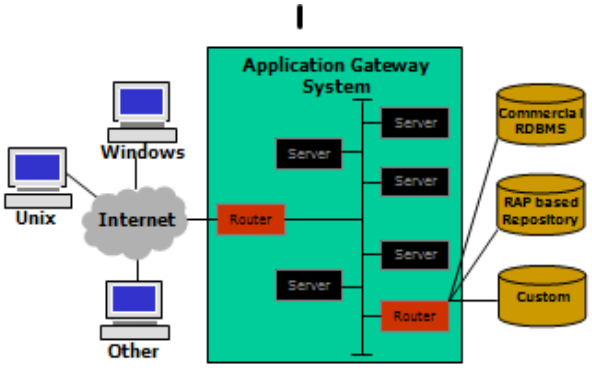


Fig. 4. structure of application gateway

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 12, December 2024

2. Packet Filtering

ACLs (Access Control Lists) are activated on routers as part of the packet filtering mechanism. As seen in the figure, a router will by default allow all traffic to travel through it without any limitations. ACLs are a way to specify the kind of access that the external world is permitted to have on an internal network and vice versa.

Because access control is implemented at a lower ISO/OSI layer, this is less complicated than an application gateway. A packet filtering gateway is frequently far faster than its application layer siblings due to its low complexity and the fact that packet filtering is carried out by routers, which are specialized computers designed for networking-related activities. At a deeper level, enabling new apps either happens on its own or just requires letting a particular kind of packet through the gateway. There are issues with this approach, even though TCP/IP has no way of ensuring that the originating address is who it says it is. Therefore, in order to localize the traffic, layers of packet filters must be used.

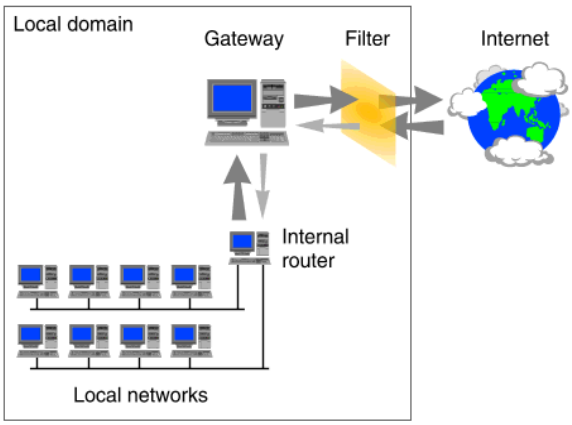


Fig. 5. Structure of filtering gateway

It has the ability to distinguish between packets originating from our internal network and those from the Internet. Additionally, the network from which the packet originated can be determined with certainty, but it cannot be further detailed.

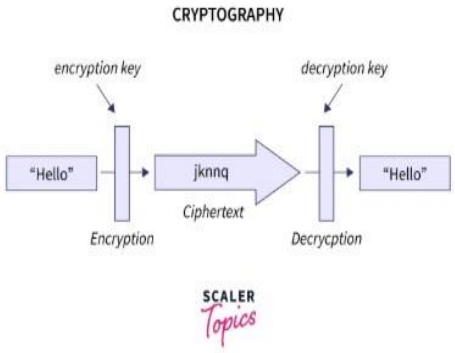
3. Hybrid Systems

Some developers have built systems that combine the flexibility and speed of packet filtering with the security features of application layer gateways, attempting to merge the two concepts. New connections in certain of these systems require application layer authentication and approval. The remaining portion of the connection is then sent to the session layer, where packet filters monitor the connection to make sure that only packets that are a part of an active (previously approved and authenticated) conversation are being sent.

Other options include using application layer proxies and packet filtering. Here, the advantages include offering some defense against your computers that serve the Internet (like a public web server) and offering the security of an application layer gateway to the internal network. Furthermore, an attacker will need to breach the access router, the bastion host, and the choke router in order to gain access to services on the internal network.

B. Cryptography

- The most widely used tool for securing information and services.
- Cryptography relies on ciphers, which is nothing but mathematical functions used for encryption and decryption of a message.



C. Create a secure environment of network

It is very significant to create a secure network environment, including monitoring users, setting user permissions, using access control, identification, monitoring routers and so on.

D. Computer virus prevention

Computer viruses are written artificially by exploiting loopholes in computer software. Due to the fast development of computer and the emergence of new viruses, the speed of transmission becomes faster and faster. Also, the harm is becoming more and more serious. The most commonly used preventive measure against computer viruses is to install antivirus software to check and kill files infected with the virus.

E. There are also the following measures to prevent the virus:

- Do not download files from unknown websites at will.
- Do not easily open the e-mail of the store address of unknown origin (attachment).
- Update system patches should be installed frequently to reduce the number of viruses that exploit system vulnerabilities to attack and destroy.
- Do not use programs and data of unknown origin.
- After downloading the file, disinfect the virus before using it.
- Often do a good backup of important data and so on.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 12, December 2024

F. Data encryption

Because network hackers may invade the system, steal data or eavesdrop on data in the network. Data encryption can make the stolen data will not be simply opened, thus reducing the loss a little. At present, the encryption technology has been relatively mature, and there are two kinds of encryption technologies commonly used: 1) symmetric key encryption technology, and 2) public key encryption technology.

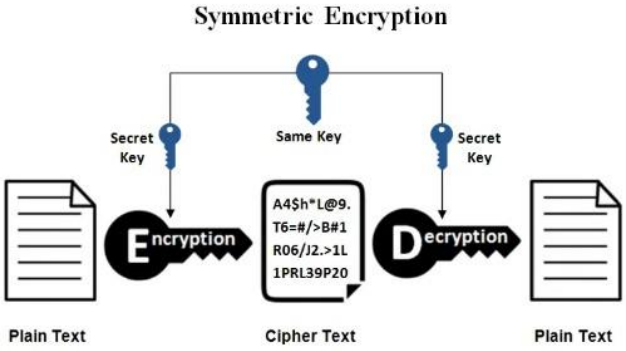


Fig. 6. Symmetric Encryption

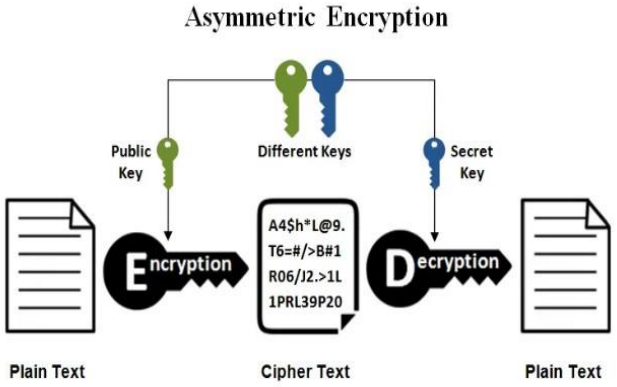


Fig. 7. Asymmetric Encryption

G. Digital signature

The digital signature is able to be utilized to verify that the message was given by the sender. Moreover, when a digital signature is used to store data or a program, it can be utilized to prove the integrality of the data or program. Like ordinary handwritten signatures, it has the ability be used to verify the authenticity of information.

H. Digital certificate

Compared with the online ID card, the digital certificate uses the digital signature to authenticate the identity on the Internet through the third-party authoritative authentication, which has the function of authenticity. Digital certificates are secure, confidential, tamper-proof and effectively protect enterprise information.

V. SECURE MANAGEMENT ISSUES

- Adopting technologies that are easy and cost effective to deploy and manage day-to–day network security operations and troubleshoots in the long run.
- Ensuring the security strength of the organization is a big challenge nowadays. Organizations have some pre-defined security policies and procedures but they are not implementing it accordingly. Through the use of technology, we should impose these policies on people and process.
- On a day-to-day basis, enterprises face the challenge of having to scale up their infrastructure to a rapidly increasing user group, both from within and outside of the organizations. At the same time, they also have to ensure that performance is not compromised.
- The implementation and conceptualization of security blueprint is a challenge. Security is a combination of people, processes, and technology; while IT managers are traditionally tuned to address only the technology controls.
- Organizations sometimes have to deal with a number of point products in the network. Securing all of them totally while ensuring seamless functionality is one of the biggest challenges they face while planning and implementing a security blueprint.
- Ensuring a fully secure networking environment without degradation in the performance of business applications.
- Building and affirming high-quality resources for deployment and efficient management of network security infrastructure.

Since network security affects every function, top-level initiative and comprehension are crucial.

At the local level, security is also very important, and staff awareness is a major priority to guarantee this. For many IT managers, staying current with the different options and the fragmented market is a challenge. The operational phase takes on more significance in the security domain. The business development team, finance, and the CEO's office must collaborate with IT to provide a blueprint because compliance actively contributes to security.

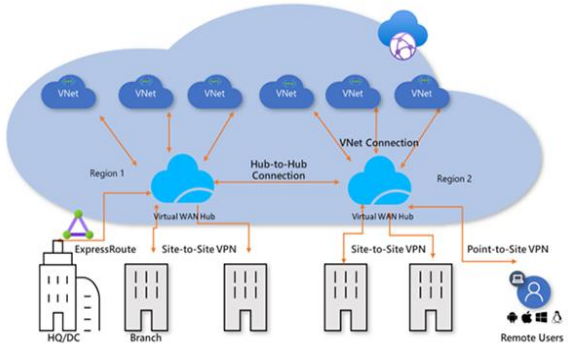
VI. WAN SECURITY

The issue of network system security is much more daunting for companies with satellite offices spread across several countries. To better automate the management of these dispersed machines, the business might need to implement a system similar to an Uplogic network security solution. Working with networks that span multiple locations is a big problem. Imagine having to take a plane to that location if the support isn't provided remotely.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 12, December 2024



VII. STEPS TO BE TAKEN BY THE COMPANIES/ ORGANIZATION

- The ideal solution for internal security challenges is not only a conventional security product but it must contain the threats (like worms), divide the network, protect the desktop, server and the data center.
- Organization should be prepared to cope with the growth of the organization, which in turn would entail new enhancements in the network both in terms of applications and size. They should plan security according to the changing requirements, which may grow to include various factors like remote and third-party access
- Threats are no longer focused on network layer; application layer is the new playground of hackers. Attack protection solutions must protect network, services and applications; provide secure office connection, secure remote employee access, resilient network availability, and controllable Internet access.
- About 72 percent of new attacks target Web-enabled applications and their number is growing. Enterprises should, therefore, deploy Web security solutions that provide secure Web access as well as protect Web servers and applications. The security solutions must be easy to deploy, and they should also provide integrated access control.

VIII. CONCLUSION

For big computing companies, security has become a crucial concern. From the viewpoint of various individuals, security and risk measures have various definitions and concepts. The design and provision of security measures should begin with an understanding of the organization's security requirements at various levels, followed by implementation at those levels. Prior to deployment, security policies should be created in a way that makes future acceptance and modification acceptable and manageable. For the end user to feel comfortable the security system needs to be both rigid and adaptable; he shouldn't feel as though it is moving all around him. Users will find methods around security policies and systems if they feel they are overly restrictive.

REFERENCES

[1] Analysis of computer network security measures; Science & Technology Information; 2011; Yang Guang, Li Feifei, and Yang Yang.

[2] The 2001 Cisco Systems book A Beginner's Guide to Network Security is available at http://www.cisco.com/warp/public/cc/so/neso/sqso/beggu_pl.pdf.

[3] Introductory to Network Security by Matt Curtin, March 1997, http://www.cs.cornell.edu/Courses/cs519/2003sp/slides/15_securitybasics.pdf.

[4] Network Security Tools by R. Farrow, available at http://sageweb.sage.org/pubs/whitepapers/farrow.pdf

[5] Computer Knowledge and Technology, Ren Xingzhou, The Analysis and Solutions to Computer Net Security; 2005.

[6] A Study of Hidden Danger in Network Safety and Safety Measures [J]; The Science Education Article Gathers; 2012 U Zhang Suying

[7] Network Security Essentials: Applications and Standards, Third Edition, Prentice Hall, Stallings, W. (2007)

[8] http://www.pandc.org/peter/presentations/ohio-tech-2004/Ohio-tech-security-handout.pdf Murray, P., Network Security