A REVIEW PAPER ON COMPUTER NETWORK SECURITY PROBLEMS AND COUNTERMEASURES

Koushik Achar *[1], Pradeep Nayak *[2], Manikanta*[3], Krupashree R*[4], Laya R*[5]

Alvas Institute of Engineering and Technology, Mijar, Karnataka, India

Department of Information Science and Engineering.

ABSTRACT

Network security is a crucial aspect of computer networks, involving the control of information access by the network administrator. It is essential for personal computer users, organizations, and military, as it protects digital information resources and ensures confidentiality, integrity, and availability. Effective network security focuses on preventing threats from entering or spreading on the network. Social network sites have introduced new information security issues such as identity theft, privacy leaks, and junk information. This paper focuses on network security, addressing major issues affecting the network, existing problems of online computer security, and recommending precautionary measures. By addressing these issues, network administrators can ensure the safety and integrity of their networks.

Keyword : - *Computer Network , Network Security, Phising, and virus prevention*

INTRODUCTION

The increasing use of computer networks in various sectors, including government, schools, and companies, has led to a growing concern for security problems. The network's unique characteristics, such as connection diversity, terminal distribution inhomogeneity, and openness, make it vulnerable to hackers and malicious software attacks. Therefore, ensuring the integrity and confidentiality of network information is crucial. To combat these threats, network security measures must respond to their own vulnerabilities and various network threats. This paper analyzes common attack methods such as virus attacks, system vulnerability attacks, spoofing attacks, and hacker attacks, discussing access control strategies, information encryption strategies, virus attack coping strategies, system vulnerability attack strategies, and hacker attack coping strategies. It also examines conventional cryptographic and public key cryptography algorithms.

One particular methodology that is able to provide comprehensive security solutions is needed in order to secure the data and the network system as a whole."-Network security depends on the developing technology known as cryptography. It is an approach to storing and sending information in a specific manner so that only those intended to read and interpret it may do so. It is the study of secret writing, or cryptography. In order to protect everything from business emails to bank transactions and online shopping, which prevents eavesdroppers, cryptography is a crucial technology for today's computer and communications networks.

NETWORK SECURITY PROBLEMS

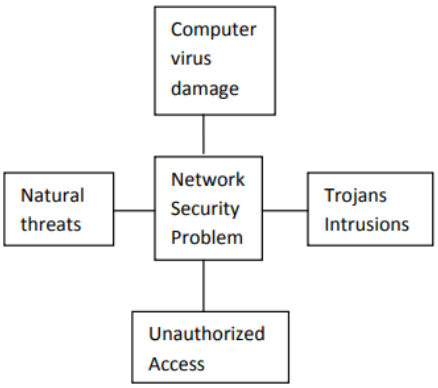

Fig-I Computer Network Security Problems

The lack of network security regulations and safeguards, along with security control systems, is making people more conscious of these hazards (Fig-I). Different natural disasters, unfavorable site conditions, electromagnetic radiation and obstruction, network equipment, and other aspects of aging naturally can all be sources of natural risks. They will have an effect on exchange and storage. Trojan horses are hacking tools with hidden, unauthorized, and remote control features.

A server program and a controller program are the two types of Trojans that are typically present. If a computer has the controller application installed, a Trojan server program must be installed as well [3]. Unauthorized usage of a computer or network is known as unauthorized access. An unauthorized user trying to get access to a computer or network is known as a cracker or hacker. A computer virus replicates itself covertly by attaching itself to another software or overwriting it with its own copy. It has the ability to quickly use up all of the RAM on your computer, drastically slowing down or even shutting it down. Files can be corrupted by viruses.

TYPES OF COMPUTER NETWORK SECURITY THREAT

Network security vulnerabilities that could allow for illegal access, information disclosure, resource depletion, resource theft, or resource destruction are possibly exploited by network threats. Threats to network security come from a variety of sources and evolve over time.. Cybersecurity threats can be of numerous types:

Hazardous Physical State: involving misidentification, espionage, and theft. Computer theft has happened recently as well, particularly with regard to the machine's critical documents, which makes it simple to do criminal acts of theft and cause needless losses.

System weaknesses:comprising configuration, startup, and hazardous service. System vulnerabilities may quickly lead to network security risks, therefore it's a good idea to periodically audit the system and update the system patch to help stop vulnerabilities and security threats.

Threat to Identity: Including a cursory analysis of algorithms, free password generators, password crackers, and password traps. In order to access the Internet, users occasionally need to provide their login and password. In these situations, choosing a strong password is crucial and should not be done at random. Consequently, a certain level of difficulty should exist, serving as a safeguard.

Threat to cable connection: This includes dial-in entry, impersonation, and eavesdropping. Cable hazards can lead to eavesdropping, while in a broadcast network architecture, each node collects data from the Internet for monitoring purposes.

Programs are harmful: Include infections, trojans, updates, and downloads. As people rely more on computers and networks, viruses pose a significant threat to both. Because the network system's devices are interconnected, a

virus assault on one device may harm the entire network. The virus is destructive, concealed, contagious, latent, and unpredictable.

CURRENT STATUS OF COMPUTER NETWORK SECURITY

Computer networks are influenced by a variety of factors, including network design and computer flaws.

Poor safety supervision: To improve computer network security, a robust surveillance system is necessary. Proper supervision helps prevent hidden threats and improve network security. Currently, there is a lack of scientific and effective regulatory review mechanisms for computer network security, posing a risk to their safe functioning.

Issues related to the network: There are vulnerabilities in the majority of today's computer networks, and hackers use these vulnerabilities to target computers in an attempt to operate remotely. This puts computer network staff members at risk. Here are the primary causes of the aforementioned issues:

(1) Stability and extensibility are constrained. There was a direct influence of many gaps in the network system's functioning in the early stages of its design because of the lack of thorough study, which led to the computer system's normative and rational existence;
(2) A network file server vulnerability. The file server acts as the center of the computer network, and its functioning has a stronger influence on other computer network operations. From a practical standpoint, a lot of designers go through the design process without completely taking into account the influence of computer network security, which can result in unreasonable and imperfect existence;
(3) weakness in the way the network system is used. We should give this careful thought since there aren't enough standard specifications for the switches, firewalls, and other equipment that are provided. This makes it difficult to install the network quickly and safely while maintaining the necessary degree of security and data.

COMMON INTERNET ATTACK METHODS:

The categories of common internet attack techniques are shown in Table 1.Certain assaults, including phishing and eavesdropping, get personal information or system knowledge. Attacks like viruses, worms, and trojans can potentially prevent the system from functioning as intended. The other type of assault is a denial of service (DoS) attack, which is when the system's resources are spent pointlessly.

Security Attributes	Attack Methods	Technology for Security
Confidentiality	Eavesdropping, phishing, Denial of Service	IDS, Firewall, Cryptographic systems, SSL
Integrity	Viruses, worms, Trojans, Eavesdropping, Dos	IDS, Firewall, Anti malware software, SSL
Privacy	Email bombing, spamming, hacking, Dos and cookies	IDS, Firewall, Anti malware software, SSL
Availability	Dos, Email bombing, spamming, and systems Boot record infectors	IDS, Firewall, Anti malware software

Table-1: Attack methods and Security Technology [4]

Eavesdropping: Interception of communications by an unauthorized person is termed eavesdropping. Passive eavesdropping is when the individual just discreetly listens to the networked messages. When someone listens and adds anything to the communication stream, it's known as active eavesdropping [4].

Viruses: Viruses are self-replicating programs that spread by infecting and using data [4]. The virus will begin to operate on the system as soon as a file is opened.
Worms: Although they are both self-replicating, worms do not need files in order to spread, making them comparable to viruses [4].
Trojans: A Trojan is any malicious computer software that deceives users about its actual purpose in order to gain access to a computer [4].
Phishing:phishing is the act of attempting to gain private information from a person, group, or entity [5]. Phishers deceive people into divulging sensitive information, including credit card details, internet banking logins, and other personal data.
Attacks Using IP Spoofing: IP spoofing is the process of creating Internet Protocol (IP) packets with a fictitious source IP address in order to conceal the sender's identity or pass for a different computer system [4].
Denial of Service: A denial-of-service (DoS) attack is any kind in which the hackers trying to enter the system try to stop authorized users from using it.

PROTECTION STRATEGIES OF COMPUTER NETWORK SECURITY

Safe Encryption: Encryption technology gives people peace of mind regarding their online transactions by guaranteeing security while conducting business. Asymmetric and symmetric encryption are at the forefront of security encryption technology development due to the ongoing advancements and improvements in information technology. The term "symmetric encryption" refers to encryption technology that primarily uses passwords; the same password key is used for both encryption and decryption.
Firewall for networks: One technology that primarily regulates network access is the network firewall.
The purpose of a firewall is to stop hackers from breaking into a network using illicit methods in order to steal data and resources, safeguarding the internet network environment and network connectivity hardware. The firewall's primary functions include dynamically monitoring the network state and examining different network transmission data through pertinent security procedures to decide whether to permit access to network communications.

Translation of Network Addresses: The goal of network address translation is to fully preserve the IP address, which is then given to the private network for further usage, enabling an address on the Internet. It can also be used in conjunction with firewall technology and concealed behind several IP addresses, preventing external networks from accessing internal hardware. When appropriate preparations are made for the usage of network addresses, network address translation can also circumvent address constraints.

Network Virus Prevention: Openness is a property of the network environment. Viruses may take many different shapes when attacking a user's computer, and they have the potential to cause enormous harm and even disastrous consequences. Thus, one of the most important aspects of network security is virus prevention. The two primary components of network virus prevention technologies are virus detection and prevention. Virus detection involves identifying a computer's virus-poisoning characteristics, such as keyword and self-checks, in order to determine whether the machine has a virus. To avoid computer damage and poisoning, virus prevention involves efficiently managing the system through its memory and determining whether viruses have infiltrated the system. improving fog levels using deep learning and AI.

Security oversight: There is not perfect security and dependability in the network system. As a result, creating a strong management system is essential to ensuring network security. Effective network security control and the prevention of virus and hacker invasion are only achievable when users and managers collaborate and utilize all available technologies and solutions.

SOLUTION TO COMPUTER NETWORK SECURITY PROBLEMS

Solutions for computer network security issues when we already have a network in place are covered in this section. It also pertains to those who are thinking about constructing tiny networks.

Prior to anything else, we must create a strategy for evaluating the network's vulnerabilities. A vulnerability assessment strategy ought to address the major locations that might compromise the network or result in massive data loss if they are compromised. These items include: 1. Server protection (main computer in peer-to-peer networks); 2. Firewalls and antivirus software on the server; 3. The protocol your server uses to connect to other computers; and 4. The ways in which other network peripherals, such as computers and printers, can endanger the network.

CURRENT DEVELOPMENT IN NETWORK SECURITY

The field of network security is moving in the same direction. Biometric identification is being added while maintaining the same methods. Passwords are not as effective as biometric authentication. This might significantly lower the likelihood of illegal access to secure systems.

Research on network security is revealing new technologies like smart cards. Network security's software component is always changing. New firewalls and encryption techniques are being deployed on a regular basis.

CONCLUSION

The security of computer networks is increasingly important due to the rapid development of the network security industry and the acceleration of the information process. With immeasurable opportunities, network security is a hot area for researchers to explore, with future technology making significant progress. Researchers should consider safety factors to establish reasonable objectives and relevant laws and regulations. With the development of the Internet, computer network security is becoming increasingly important due to its vulnerability to various attacks and destruction. There are natural and man-made factors that form potential security threats in both local and wide area networks. To ensure a safe and stable environment, it is crucial to standardize Internet behaviour, establish network rules and regulations, and limit free access to unknown sites. Network security is a big system engineering task, as data information transmitted on the Internet is easy to leak and be destroyed due to sharing and communication security defects.

REFERENCE

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

[2] U Zhang Suying; An Inquiry into Hidden Danger in Network Safety and the Safety Precautions [J]; The Science Education Article Collects; 2012.

[3] Xiong Fangfang; A brief discussion on the problems of computer Network Security and its Countermeasures [J]; Electronics World; 2012.

[4] Wang Z. Design and realization of computer network security perception control system[C]// IEEE, International Conference on Communication Software and Networks. IEEE, 2015:163-166.

[5] Guo J C, Fan D, Che H Y, et al. An approach to network security evaluation of computer network information system with triangular fuzzy information[J]. Journal of Intelligent & Fuzzy Systems, 2015, 28(5):2029-2035.

[6] Shao K N. Research on Data Encryption Technology in Computer Network Communication Security[J]. Information Security & Technology, 2016.

[7] Liu Z, Amp S V. Computer network information security and protection strategy[J]. Electronic Test, 2016.

[8] Wager R, Yarochkin F, Dahlgren Z. Recursive multi-layer examination for computer network security remediation[J]. 2017.

[9] Zhou X Z, Xin L I. Computer network security technology in molybdenum mining field of applied research[J]. World Nonferrous Metals, 2016.

[10] Zhu L S. Computer network security precautions in the process of metal metallurgy analysis[J]. World Nonferrous Metals, 2016.