Vedic Science, International Multidisciplinary Peer Reviewed Research Journal
Vol. 2026, Issue 1 (Jan.- March), PP. 51-58
ISSN No. 0975-0312
DOI: https://doi.org/10.66718/vsj.v28.i1.06

COMPUTER NETWORK SECURITY & TECHNOLOGY

Dr. Devkumar Gole

Kaliachak B.K.A Sanskrit Mahavidyalaya

Kaliachak, Purba Medinipur, Pin-721430, W.B

ABSTRACT

By writing this paper a small effort has been put to understand the growing network needs and its security. Various types of network threats and security services are discussed. Many security devices are being developed and deployed to defend against cyber threats and to prevent unintended data breaches. Network security has become more important to personal computer users, organizations, and the military. *This research addresses network security technology such as authentication, encryption, firewall technology, intrusion detection system (IDS), antivirus technology and virtual private network (VPN).* With the continuous development of internet, people cannot live without computers and networks. However, in the process of using network, there are often a lot of security problems. Computer networks are essential part of our life by which we can share the information through different technologies like wired or wireless networks. Now a day wireless technologies are adopted because of its advantages and secured information transmission. Within this paper I will talk to you about the importance of network security and how it can change your day-to-day life using cyber security. It is recommended to hire a professional team to check in time, popularize security knowledge, change passwords, download and purchase network firewalls Software, timely discovery of security vulnerabilities, and the government's introduction of cyber security laws.

KEYWORDS

Network Security, Internet, Data Security, Cyber Security, Network Security, Security threats.

INTRODUCTION

Network security encompasses all the steps taken to protect the integrity of a computer network and the data within it. Network security is essential because it keeps sensitive data safe from cyber-attacks and ensures the network is usable and trustworthy. Successful network security strategies employ multiple security solutions to protect users and organizations from malware and cyber attacks, like distributed denial of service. Most of the commercial organizations exchange information with their collaborators and clients through the Internet. Educational institutes are uploading study materials and research findings over the Internet for the speedy propagation of the information. Governments provide information to the citizens

through the Internet. Individuals use the Internet for accessing the information, online shopping and communicating with others through emails and social networking etc. Computer networks and data are protected by a set of configurations and rules known as network security. Its purpose is to ensure confidentiality, integrity, and accessibility. It involves various technologies, devices, and processes. It is crucial to safeguard a network and its data against potential risks, such as unauthorized entry, misuse, malfunction, changeover or inappropriate disclosure. A network may be described as interconnections of autonomous nodes, which are physically separated. These interconnected nodes may be routers, switches, firewalls, servers, etc. Many networks connected together, i.e., hybrid kind of network is called Internet. Internet is a vast bank of information shared among individuals in any part of the world without any physical geographic limitation. Network security architecture comprises tools that protect the network itself and the applications that run over it. Effective network security strategies employ multiple lines of defense that are scalable and automated. Each defensive layer enforces a set of security policies determined by the administrator. Devices like phones, laptops, and desktops are very unrestricted as they can be used to commit identity theft and even fraud. When the network is running, a large amount of data and information is stored on the external memory of the host or terminal, so how we prevent unauthorized users from accessing it is important to solve network security problems. A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network. The convenience of computers for our daily life is the simplest, because its real function is not here. For example, automation, medicine and health, scientific research, criminal investigation and so on, computers are playing an irreplaceable role. There is a lot of information in these industries is very secret, because these information cannot be understood by irrelevant people, otherwise it will cause irreparable losses.

ADVANTAGE OF NETWORK SECURITY

Complementary Cyber Security refers to the use of multiple Cyber Security strategies, techniques, and tools in combination to enhance overall Cyber Security posture. Here are some advantages of complementary Cyber Security are:

1. **Updates from a central location:** A centralized network security solution has the advantage of providing frequent updates without requiring individual knowledge.
2. **Eliminating Abuse of Your Corporate Site:** Unless you have fully secured your network, your business site remains exposed to hacking, pushing viruses, and several other cyber abuses.
3. **Keeping Your Network Centralized:** Under the current digital mode of business operation, your network needs to remain under the command of the proprietor.
4. **Defense-in-Depth:** Complementary Cyber Security follows the principle of defense-in-depth, which involves layering multiple security measures to provide overlapping protection.
5. **Diversified Protection:** Different Cyber Security solutions have different strengths and weaknesses.

6. **Advantage of Regular Corporate Update:** You can regularly update your site only when your network is functioning without any hitch caused by hacking.
7. Protection from malicious attacks on your network.
8. **Network Segmentation:** If you are running a large company, you need to do segmentation to classify and break a network into smaller segments.
9. Deletion and/or guaranteeing malicious elements within a preexisting network.
10. **Wireless Security:** Unless you secure your network, your wireless security system is at risk. Network security's implementation can secure it.
11. **Keep your data safe:** A network holds a lot of sensitive information, such as personal customer information.
12. **Protects against cyber-attacks:** Computers will not be harmed as a result of these attacks if network protection is in place.
13. **Accessibility levels:** After the user's authentication, the authorization approach is used to determine whether the user is authorized to access a specific resource.
14. **Centrally Controlled:** Network security software, unlike desktop security software, is managed by a single user known as the network administrator.

DISADVANTAGE OF NETWORK SECURITY

Network security is extremely helpful to all business establishments. However, it has some minor disadvantages. Here are some disadvantages of Cyber Security are:

1. Some of the software on some networks is difficult to use. To maintain double security, it requires authentication using two passwords, one of which must be entered every time you update a document.
2. There is a risk of potential overlap or gaps in Cyber Security coverage with complementary Cyber Security. Complementary cyber security can introduce complexity in terms of managing multiple security solutions, coordinating their configuration, and ensuring their compatibility.
3. To fully secure your network, you need to buy the latest software and digital tools, which involves additional expenses.
4. Organizations need to carefully consider their budget and resources to ensure they can afford the additional costs associated with complementary cyber security.
5. You need to employ some well-trained personnel to constantly monitor network operation and detect intrusions.
6. Managing huge networks is a difficult endeavor. It necessitates highly trained experts capable of dealing with any security issue that may develop.
7. At the initial phase, your computer may slow down due to the loading of software and other digital means.
8. Integrating different cyber security solutions and ensuring their seamless operation can be complex, especially if they come from different vendors or have different

configurations.

TYPES OF ATTACKS

There are many types of cyber-attacks these are:

- **Malware:** Malware can steal data, corrupt files, disrupt operations, or even take control of systems. Examples include viruses, worms, Trojan horses, ransomware, and spyware.
- **Phishing:** Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity, often through emails or messages. **Impact** Can lead to identity theft, financial loss, or unauthorized access to accounts.
- **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks:** DoS attacks aim to overwhelm a network or system with traffic, making it unavailable to legitimate users. These attacks aim to overwhelm a network, system, or application.
- **Man-in-the-Middle (MitM) Attacks:** In MitM attacks, an attacker intercepts and possibly alters communication between two parties without their knowledge. It allows the attacker to eavesdrop, steal data, or impersonate one of the parties.
- **SQL Injection:** Attackers exploit vulnerabilities in poorly coded web applications to inject malicious SQL queries, gaining unauthorized access to databases or executing unintended commands.
- **Zero-day Exploits:** Zero-day vulnerabilities are software vulnerabilities unknown to the vendor, making them highly valuable to attackers. They exploit these vulnerabilities before the vendor releases a patch or fix.
- **Password Attacks:** These attacks involve various techniques like brute-force or dictionary attacks to gain unauthorized access to user accounts. These attacks target passwords to gain unauthorized access to a network or system.
- **Social Engineering:** Social engineering attacks exploit human psychology to trick individuals into revealing sensitive information or performing actions that compromise security, often through manipulation or deception.
- **Insider Threats:** These threats arise from malicious or careless actions by individuals within an organization who have authorized access. It can involve data theft, sabotage, or unintentional data breaches.
- **Wireless Attacks:** Attackers exploit weaknesses in wireless networks, such as Wi-Fi, by eavesdropping, unauthorized access, or intercepting data transmissions.
- **Eavesdropping:** Also known as sniffing or snooping, this attack involves capturing network traffic to gather sensitive information like passwords, credit card details, or confidential data.
- **Data Breaches:** Data breaches occur when unauthorized individuals gain access to sensitive or confidential data, potentially resulting in financial loss, reputation damage, or legal consequences.

SECURITY IN DIFFERENT NETWORKS

Intranet is a private computer network that uses internet protocols. Intranets differ from "Extranets" in that the former are generally restricted to employees of the organization while extranets can generally be accessed by customers, suppliers, or other approved parties. There does not necessarily have to be any access from the organization's internal network to the Internet itself. When such access is provided it is usually through a gateway with a firewall, along with user authentication, encryption of messages, and often makes use of virtual private networks (VPNs).

Network security is basically 5 things.

1. Protecting your data, software, and hardware from outside attacks and/or malware.
2. Preventing system users from intentionally or accidentally accessing potentially harmful sites.
3. Preventing system users from accessing sites that may cause future problems.
4. Scanning all media that is attached to the network for malware is part of network security.
5. Training of employees.

COMPUTER NETWORK SECURITY ANALYSIS

Computer Network Security Analysis Computer network hardware security is defined by the level of privacy and protection required by the network environment to store data across the network for devices used in the network environment. In order to build reliable network security architecture, these 3 factors must be taken into consideration:

1. Electromagnetic field and radioactivity

2. Operational errors

3. Natural disasters

Network security analysis is essential for safeguarding an organization's sensitive data, maintaining industry compliance, and staying ahead of threats. These assessments scan network systems, identify vulnerabilities, simulate attacks, and provide actionable recommendations for continuous improvement.

COMPUTER NETWORK SECURITY REQUIREMENTS

It becomes simpler to implement appropriate security policies and safeguards once the sources of potential threats and the types of potential damage are identified. Organizations have a wide range of options, from antivirus software packages to network firewalls, intrusion detection systems, and network security hardware. Methodological issues in computer network security have their own characteristics, each of which has advantages and disadvantages.

Network security relies on a few essential security measures:

- Authentication. It ensures that only the right people and devices can access a network. ...

- Virtual private network (VPN). ...
- Network encryption. ...
- Firewalls. ...
- Intrusion detection and prevention systems (IDPS). ...
- Access control.

FUTURE TRENDS IN SECURITY

The future will possibly be that the security is similar to an immune system. Many security developments that are taking place are within the same set of security technology that is being used today with some minor adjustments.

The future of network security is likely to be shaped by several key trends and developments:

1. **Artificial Intelligence and Machine Learning**: AI and ML will play a significant role in threat detection and response.
2. **IoT Security**: With the proliferation of Internet of Things (IoT) devices, securing these endpoints will be critical.
3. **Supply Chain Security**: Cyberattacks targeting supply chains are on the rise.
4. **Cyber security Skills Gap**: The shortage of skilled cybersecurity professionals will continue to be a challenge.
5. **Quantum Computing Threats**: As quantum computing technology advances, it poses potential risks to current encryption methods.
6. **Increased Focus on Cloud Security**: As more organizations migrate to the cloud, securing cloud infrastructures will become a priority.
7. **Incident Response and Recovery**: There will be a greater emphasis on developing comprehensive incident response plans and recovery strategies to minimize downtime and data loss in the event of a breach.
8. **Zero Trust Architecture**: This security model assumes that threats could be both outside and inside the network.

CONCLUSION

By securing your network, you can stay ahead of the latest threats and ensure that your business is protected against new and emerging risks. Everything seems to indicate that the number of threats that users will have to face will continue to grow. The aim of this paper is to explore the process of building and implementing a successful, secure and robust network infrastructure. We have discussed various techniques to overcome possible security threats. Computers are advancing and the internet and networking is only getting bigger and brighter. With this, there are many things to be aware of when in the use of the internet. Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary changes in security technology. Network security is an important area that is gaining more and more

attention as the Internet expands. Network security plays an important role in authorizing the users so that they can secure their data from the hacker or unauthorized users. People put more and more attention on the security of computer network. At the same time, the beneficiaries and users of computer networks need to emphasize the protection of our own information security.

REFERENCE

1. Academia.edu. (n.d.). Network security and cyber security: A review. https://www.academia.edu/83766623/Network_Security_and_Cyber_Security_A_Review
2. ADMI USA. (2024). Proceedings paper UP5. http://www.admiusa.org/admi2024/ADMIProceedings/UP5.pdf
3. FireMon. (n.d.). Network security assessment: A guide. https://www.firemon.com/blog/network-security-assessment-a-guide/#types-of-security-assessments-for-networks
4. Inderscience Publishers. (n.d.). International Journal of Network Security. https://www.inderscience.com/jhome.php?jcode=ijnsec
5. International Journal of Computer Trends and Technology. (2023). Article V71I5P113. https://ijcttjournal.org/2023/Volume-71%20Issue-5/IJCTT-V71I5P113.pdf
6. International Journal of Scientific Research Publications (IJSRP). (2013). Research paper P20131. https://www.ijsrp.org/research-paper-0813/ijsrp-p20131.pdf
7. IOP Science. (n.d.). Journal of Physics: Conference Series article (1992/3/032069). https://iopscience.iop.org/article/10.1088/1742-6596/1992/3/032069/pdf
8. IRJMETS. (2020). Research article (Volume 2, Issue 6). https://www.irjmets.com/uploadedfiles/paper/volume2/issue_6_june_2020/1803/1628083058.pdf
9. NordVPN. (n.d.). Network security standards. https://nordvpn.com/blog/network-security-standards/
10. Quora. (n.d.). What are the types of network security systems? https://www.quora.com/What-are-the-types-of-network-security-systems
11. Quora. (n.d.). What is the concept of network security? https://www.quora.com/What-is-the-concept-of-network-security
12. ResearchGate. (n.d.). Networking and security measures. https://www.researchgate.net/publication/265141277_Networking_and_Security_Measures
13. ScienceDirect. (n.d.). Article (S1877050922015204). https://www.sciencedirect.com/science/article/pii/S1877050922015204/pdf
14. Stamus Networks. (n.d.). What are the 4 types of attacks in network security? https://www.stamus-networks.com/blog/what-are-the-4-types-of-attacks-in-network-security

15. Stanford University. (2011). Introduction to computer security (CS155 lecture notes). https://crypto.stanford.edu/cs155old/cs155-spring11/lectures/01-intro-thompson.pdf