Network Security Trends and Approaches

Yasir Abubakar Sulaiman, Dr.Alok Katiyar
UG Scholar,School of Computing Science and Engineering, Galgotias University,Greater Noida, U,P,India
Factuly, School of Computing Science and Engineering, Galgotias University, Greater Noida, U,P,India

Abstract— **The necessity of network security has been recognized by individuals, organisations become a big issue, and a deeper understanding of the history of security technology is possible. Many security flaws were possible due to the internet structure. The amount of possible attacks that can be sent across the internet is lowered when the internet's design is changed. Knowing how to attack enables for the development of adequate security. To protect themselves from the internet, many businesses use firewalls and encryption."**
Network security is a large field that is constantly evolving. The scope of the research encompasses both a brief history of the internet's beginnings and contemporary network security developments. A basic understanding of the internet, its vulnerabilities, internet-based assault strategies, and security technology is required to understand today's study, and these are discussed.

Index Terms: **network security trends & approaches, Types of network security, Cybersecurity attacks & Trends, Solutions, Conclusion.**

INTRODUCTION

Networks and their services must be protected from unauthorised alteration, revealing or destroyingas well as the assurance that the network will function properly in critical situations without harming users or employees, is characterised as network security[1]. It also comprises network administrator-enacted policies to prohibit unauthorised access to the network and network-accessible resources, as well as safeguards built into the underlying computer network infrastructure.

1. The Internet's design and vulnerable security issues
2. The Internet's design and vulnerable security issues.

A. Security Attacks

The following are the different types of security attacks:

Passive Attacks

Attempts to break the system utilising observable data fall under this category. A passive attacks would be a plain text. [2,3], in which the attacker has plain and encrypted material at their disposal.

The following are the characteristics of passive attacks:

- Data privacy is jeopardised by eavesdropping and "man-in-the-middle" attacks.
- Website trade: a breach of privacy. Examples, network tracking and CRT radiation.

Active Attacks

The attacks must stop the data stream in one or both directions, to carry out this type of assault. [2,3] Active attacks have the following characteristics:

- Denial-of-service attacks are an example of interruption assaults.
- Modification is a form of integrity violation, and forgery poses a threat to dependability.

BACKGROUND

According to Flauzac [6] introduced a revolutionary technique called grid of security for implementing distributed security solutions in a controlled collaborative manner, devices verifies that a device is reliable and system regulations manage interactions between devices. Wu Kehe [8] network business security, data security, and network system security into three categories, as well as a paradigm for network business security. A theoretical underpinning for securing business automation production systems has also accepted. Wuzheng has created wireless network architecture (PKI) [9]. [10, 11, 12, 13-14] define a number of cryptography and network security methodologies and treatments.

Network Security Protections:

Network Segmentation

Network segmentation defines boundaries between network segments where assets within the group havea common function, risk or role within an organization. The perimeter gateway, for example, separates a company network from the Internet. Potential dangers from outside the network are avoided, ensuring that sensitive data stays inside the network. Organizations can take it a step further by setting extra internal network borders, which can increase security and

access control.

Firewalls

Firewalls control incoming and outgoing traffic on networks, with predetermined security rules.[8,11]. Firewalls keep unwanted traffic out and are an essential aspect of everyday computing. Firewalls, particularly Next Generation Firewalls, are critical for network security since they focus on preventing malware and application-layer attacks.

POPULAR CYBER-ATTACK SOLUTION

1) Back up your data:

In the event of a crisis (typically a cyber attack), you must have your data backed up in order to avoid significant downtime, data loss, and financial damage.

2) Wifi Security:

One of the safest things you can do for your systems is to secure and hide your wifi networks. There are thousands of devices that can connect to your network and compromise you as technologyadvances.

3) Passwords:

Having the same password setup for everything can be dangerous. Once a hacker figures out your password, they now have access to everything in your system and any application you use.

Having separate passwords for each application you use will improve your security, and changing them frequently will keep you safe from both external and internal dangers.

Security Solutions for Networks:

There are numerous various approaches a network, just as there are many different ways to infiltrate one[19].

The following are frequent types of network security solutions:

- Antivirus software can be put on all network devices in order to scan them for harmful malware. To address any faults or vulnerabilities, it should be updated on a regular basis.
- Encryption is the process of encrypting data until it is unintelligible and then providing only authorized parties with the key (typically a decryption key or password) to decrypt it. This prevents unauthorized users from reading data that has been intercepted or seen.
- Firewalls are software programs, hardware devices, or a mix of both that prevent unwanted traffic from accessing a network. They can be set up to only block suspicious or unauthorized traffic while allowing valid requests to pass through.
- straightforward: Users must submit two separate forms of identification to log into an account. Users must provide unique credentials from two of the three categories something you know, something you have, and something you are – for multi-factor authentication to be completely successful.
- Network segmentation is the process of breaking down a larger network into smaller subnetworks or segments. Because the sub networks exist independently of one another, if one is penetrated or compromised, the others remain unaffected.

CONCLUSION

As technology evolves, network security has become increasingly important. The potential threats and protocol IP should be examined to give the full security features and give the complete security features, and the potential hazards and protocol IP should be reviewed. Software and multiple hardware devices constitute the majority of security technology. Furthermore, the security of the network is a clause include in a fundamental network infrastructure, laws enacted by the network manager to safeguard the network and infrastructure resources from security breaches, and the efficiency of all these measures when merged.

The security of the network holds similar importance as the computer security and encryption of messages.

The following must be taken into consideration when creating a network which is to be considered very secure.

1) Principle of accountability: This is to make absolute a user of the network can't deny or doesn't contest using the Network.

2) Message authenticity: This is making sure information has not been manipulated in Transit

3) Verification: to ascertain subscribers are who they claim to be.

4) Permission: enabling licensed subscribers to engage with the system

An optimal network security framework should be prepared with knowledge of vulnerabilities, potential attackers, required security levels, and factors that make a network susceptible to damage. Cryptography, verification processes, vulnerability scanning, access controls, and firewalls are all tools that can help reduce a computer's frailty to the network.

Upholding organization's network utilization laws can avert internal users from introducing threats due to misappropriation, in additament to safeguard the network from external threats.

REFERENCE

[1] Sherf, E., 2022. The importance of cyber security in journalism. Network Security, 2022(4).

[2] Satybaldin, A., Temirova, G. and Zhunisbekova, T., 2020. Food security of Kazakhstan: state and opportunities. The economy: strategy and practice, 15(2), pp.11-20.

[3] Network Security, 2002. Application Security — A Serious Pitfall.2002(9), p.7.

[4] Satybaldin, A., Temirova, G. and Zhunisbekova, T., 2020. Food security of Kazakhstan: state and opportunities. The economy: strategy and practice, 15(2), pp.11-20.

[5] Network Security, 2002.The Importance of Hardware-based Cryptography for Added Security.2002(3), p.5.

[6] Barnum, S. and McGraw, G., 2005.Knowledge for Software Security. IEEE Security and Privacy Magazine, 3(2), pp.74-78.

[7] Network Security, 2009. DHS needs to fix web site security. 2009(10), p.2.

[8] Li, S., 2021. Development Trend of Computer Network Security Technology Based on the Big Data Era. Journal of Physics: Conference Series, 1744(4), p.042223.

[9] LI, W., LUO, C. and CHU, X., 2009. Private key updating scheme of identity-based public key cryptography under distributed network. Journal of Computer Applications, 29(7), pp.1825-1827.

[10] Network Security, 2008. Researcher demonstrates Cisco rootkit. 2008(6), p.2.

[11] Network Security, 2002.Application Security — A Serious Pitfall. 2002(9), p.7.

[12] Farrow, M. and Farrow, J., 2019. Recognizing Intergenerational Assets With in Religious Communities of Colour. Journal of Childhood Studies, pp.71-84.

[13] Network Security, 2021. Practical IoT Hacking. 2021(5), pp.4-4.

[14] Wright, C., 2020. Essentials for selecting a network monitoring tool. Network Security, 2020(4), pp.11-14.

[15] Chen, H., Meng, C. and Chen, J., 2021. DDoS Attack Simulation and Machine Learning-Based Detection Approach in Internet of Things Experimental Environment. International Journal of Information Security and Privacy, 15(3), pp.1-18.

[16] Bayuk, J., 2011. Systems Security Engineering. IEEE Security & Privacy Magazine, 9(2), pp.72-74.

[17] Reactions Weekly, 2022. Cybersecurity attacks top ECRI list of health technology hazards for 2022. 1892(1), pp.1-1.

[18] Azubuike, S., 2021. Cybersecurity Attacks: Regulatory and Practical Approach Towards Preventing Data Breach and Cyber-Attacks in USA. SSRN Electronic Journal,.

[19] Gervais, M., 2011.Cyber Attacks and the Laws of War. SSRN Electronic Journal,.