IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

Network Security in IT Infrastructure

Sanket Vilas Thakare and Sahil Lahu Parab
Students, Master of Computer Application
Late Bhausaheb Hiray S. S. Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allows for many security threats to occur. If the architecture of the internet is modified, it can reduce the possible attacks that can be sent across the network. Knowing the attack methods allows us to emerge with appropriate security. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an "intranet" to remain connected to the internet but secured from possible threats. The entire field of network security is vast and in an evolutionary stage. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed.*

Keywords: Network security

I. INTRODUCTION

The world is becoming more interconnected due to Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of utmost importance because of intellectual property that can be easily acquired through the internet. There can be breach in intellectual property. There are two types of fundamentally different networks: data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as "Trojan horses," planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet.

The network security is analysed by researching the following:

1. Internet architecture and vulnerable security aspects of the Internet
2. Types of internet attacks and security methods
3. Security for networks with internet access
4. Current development in network security hardware and software

II. NETWORK SECURITY

System and network technology is a key technology for a wide variety of applications. Networks and applications need security. Although, network security is a critical requirement, there is a significant lack of security methods that can be implemented easily. There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed process that is based on the Open Systems Interface (OSI) model. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well-developed process. There isn't a methodology to manage the complexity of security requirements. Secure network design does not contain the same advantages as network design. Network security doesn't mean securing both end computers. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the encrypted data, and decrypt it and re-insert a false message. Securing the middle network is just as important as securing the computers and encrypting the message.

When developing a secure network, the following need to be considered:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

1. Access– Authorized users are provided the means to communicate to and from a particular network
2. Confidentiality– Information in the network remains private
3. Authentication – Ensure the users of the network are who they say they are
4. Integrity – Ensure the message has not been modified in transit
5. Non-repudiation – Ensure the user does not refute that he used the network.

With the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack an effective network security plan is developed. To make the computer less vulnerable to the network there are many products available. These tools are encryption, firewalls, intrusion-detection, and security management and authentication mechanisms. Businesses throughout the world are using a combination of some of these tools. “Intranets” are both connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in the network. Understanding the security issues of the internet greatly helps to develop secure solutions to protect the networks from the internet. The types of attacks through the internet need to also be studied to be able to detect and guard against them. Intrusion detection systems are established based on the types of attacks most commonly used.

Network intrusions consist of packets that are introduced to cause problems for the following reasons:

- To consume resources uselessly
- To interfere with any system resource’s intended function
- To gain system knowledge like passwords, logins that can be exploited in later attacks.

III. LITERATURE REVIEW

Fear of security breaches on the Internet is causing organizations to use protected private networks or intranets. The Internet Engineering Task Force (IETF) has introduced security mechanisms at various layers of the Internet Protocol Suite. These security mechanisms allow for the logical protection of data units that are transferred across the network. The current version and new version of the Internet Protocol are analyzed to determine the security implications. Although security may exist within the protocol, not all attacks are guarded against. These attacks are analyzed to determine other security mechanisms that may be necessary.

The security architecture of the internet protocol known as IP Security is a standardization of internet security. IP security, IP sec, covers the new generation of IP (IPv6) as well as the current version (IPv4). Although new techniques, such as IP sec, have been developed to overcome internet’s best-known deficiencies, they seem to be insufficient IP sec is a point-to-point protocol, one side encrypts, the other decrypts and both sides share key or keys. IPsec can be used in two modes, namely transport mode and tunnel modes.

The businesses today use combinations of firewalls, encryption, and authentication mechanisms to create “intranets” that are connected to the internet but protected from it at the same time. 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). Although intranets can be set up quickly to share data in a controlled environment, that data is still at risk unless there is tight security. The disadvantage of a closed intranet is that vital data might not get into the hands of those who need it. Intranets have a place within agencies. But for broader data sharing, it might be better to keep the networks open, with these safeguards:

1. Firewalls that detect and report intrusion attempts
2. Sophisticated virus checking at the firewall
3. Enforced rules for employee opening of e- Mail attachments
4. Encryption for all connections and data transfers
5. Authentication by synchronized, timed passwords or security certificates

It was mentioned that if the intranet wanted access to the internet, virtual private networks are often used. Intranets that exist across multiple locations generally run over separate leased lines or a newer approach of VPN can be utilized. VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

IV. ATTACKS THROUGH THE CURRENT INTERNET PROTOCOL IPV4

Common Internet Attack Methods: Common internet attacks methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eaves dropping and phishing. The other form of attack is when the system's resources are consumes uselessly, these can be caused by denial of service (DoS) attack. Other forms of network intrusions also exist, such as land attacks, surf attacks, and teardrop attacks. These attacks are not as well-known as DoS attacks, but they are used in some form or another even if they aren't mentioned by name.

Eavesdropping Interception of communications by an unauthorized party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. On the other hand, active eaves dropping are when the intruder listens and inserts something into the communication stream. This can lead to the messages being distorted. Sensitive information can be stolen this way.

- Viruses: Viruses are self-replication programs that use files to infect and propagate. Once a file is opened, the virus will activate within the system.
- Worms: A worm is similar to a virus because they both are self-replicating, but the worm does not require a file to allow it to propagate. There are two main types of worms, mass-mailing worms and network- aware worms. Mass mailing worms use email as a means to infect other computers. Network-aware worms are a major problem for the Internet. A network-aware worm selects a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise.
- Trojans: Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as a virus.
- Phishing: Phishing is an attempt to obtain confidential information from an individual, group, or organization. Phishers trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information.

IP Spoofing Attacks Spoofing means to have the address of the computer mirror the address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IP- spoofed packets cannot be eliminated.

Denial of Service Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.

Technology for Internet Security: Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different defence and detection mechanisms were developed to deal with these attacks.

Cryptographic systems: Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data. These unintelligible data is thus transferred in the network safely.

- Firewall: A firewall is a typical border control mechanism or perimeter defence. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the frontline defence mechanism against intruders. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both
- Intrusion Detection Systems: An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack. Anti-Malware Software and Scanners Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so-called anti-Malware tools are used to detect them and cure an infected system.
- Secure Socket Layer (SSL): The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so

ISSN 2581-9429 IJARSCT

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity.

V. DEVELOPMENTS IN NETWORK SECURITY

The network security field is continuing down the same route. The same methodologies are being used with the addition of biometric identification. Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorized access of secure systems. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented. The research being performed assist in understanding current development and projecting the future developments of the field.

5.1 Hardware

Developments Hardware developments are not developing rapidly. Biometric systems and smart cards are the only new hardware technologies that are widely impacting security. The most obvious use of biometrics for network security is for secure workstation logons for a work station connected to a network. Each workstation requires some software support for biometric identification of the user as well as, depending on the biometric being used, some hardware device. The cost of hardware devices is one thing that may lead to the widespread use of voice biometric security identification, especially among companies and organizations on a low budget. Hardware device such as computer mice with built in thumbprint readers would be the next step up. These devices would be more expensive to implement on several computers, as each machine would require its own hardware device.

5.2 Software Developments

The software aspect of network security is very vast. It includes firewalls, antivirus, VPN, intrusion detection, and much more. The research development of all security software is not feasible to study at this point. The goal is to obtain a view of where the security software is heading based on emphasis being placed now

VI. FUTURE TRENDS IN SECURITY

What is going to drive the Internet security is the set of applications more than anything else. The future will possibly be that the security is similar to an immune system. The immune system fights off attacks and builds itself to fight tougher enemies. Similarly, the network security will be able to function as an immune system. The trend towards biometrics could have taken place a while ago, but it seems that it isn't being actively pursued. Many security developments that are taking place are within the same set of security technology that is being used today with some minor adjustments.

VII. CONCLUSION

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. The security technology is mostly software based, but many common hardware devices are used. The current development in network security is not very impressive. Originally it was assumed that with the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development taking place in the same. technologies being currently used. Combined use of IPv6 and security tools such as firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding intellectual property for the near future. The network security field may have to evolve more rapidly to deal with the threats further in the future.

REFERENCES

[1]. IEEE Security & Privacy (Volume: 3, Issue: 6, Nov.-Dec. 2005)
[2]. Heberlein, L T; Dias, G V; Levitt, K N; Mukherjee, B; Wood, J; Wolber, D
[3]. https://www.osti.gov/biblio/6223037
[4]. https://books.google.co.in/books?hl=en&lr=&id=bSPsPmtSMboC&oi=fnd&pg=PR17&dq=network+security&ots=H9XN8Rot8q&sig=K7e1nAgrtSCpQYzkBp-UHNLLgn4&redir_esc=y#v=onepage&q=network%20security&f=false
[5]. https://www.researchgate.net/publication/267691532_MODERN_NETWORK_SECURITY_ISSUES_AND_CHALLENGES