REVIEW ON COMPUTER NETWORK SECURITY AND TECHNOLOGIES

SaiMonika S[1] Harshithaa M[2] AnithaKatherin RJ[3] IreneChristinaAndrea P[4] Pavithra S[5]

[12345]DepartmentofComputerandCommunicationEngineering

[12345]PanimalarEngineeringCollege

ABSTRACT

The security of computer network applications is receiving excessive attention due to their widespread popularity and high demand. The variables affecting the network's safety, such as performing network security well and uniformly, are quite complex. In order to address the issues of computer network system safety and reliability, this study combines real-world work experience with risk-averse technologies and eras.

Proposals and arrangements for principle of system design ,with the goal of making the masses of users in computer networksmoreawareofsecurityandmasterycertain networksecuritytechnologies.

Keywords: Network security; Community protection; Security era

INTRODUCTION

These days, the use of computer networks has expanded throughout the world. Itcausesaremarkableimpact On people’s work and life. As networks have become larger and network knowledge has been acknowledged, it has gradually become an essential aspect of people's lives.Security of computer networks is now a major global issue. The efficiency of protecting computer and network systems depends on computer network and information security technology.The scope of network security protection is very broad, starting at the technical level with data encryption, identity verification, intrusion detection and protection, virus prevention, and virtual private networks (VPNS), among other things. These methods include active defences, passive defences, and platforms and assistance for security research.The availability, integrity, and privacy of network data are protected by a number of technical and management measures used in computer network security. In order to ensure that data transmission and exchange across the network do not exist, such as add, alter, loss, and leak, it is crucial to define the objective of network security protection. In order to address these issues, the security operation centre, which we believe to benovel functional block, is proposed in thispaper. Its architecture is described, along with key requirements for the supported functionalities and instructions for integrating it with an optical-layer controller.

THE CONCEALED DIFFICULTY IN A TYPICAL COMPUTER NETWORK SECURITY

Vulnerabilities of Transfer Protocol..

Using the source routing option., An IP packet can be generated in consonance with the predicted routing to reach the destination host by employing the source routing option in the IP header. However, it also gave intruders chances. For example ,if a host is aware of are liable host beforehand ,it can impersonate that host using source routing configurations to assault the system, making that host open to attack from all other hosts.

2.Forging ARP packets is a type of extremely complex technology that incorporates numerous TCP/IP and Ethernet features, so using it to address security issues is not the best use of thistechnology. . The primary approach to an ARP packet source address is a false ARP packet that leverages the Ethernet address and IP address of the destination host.. Another IP spoof may result from this. This attack primarily targets switched Ethernet and the exchange hub that receives and cache search ARP packet update. Frequent sending of spoof ARP packets can result in both packages being forwarded to the destination host by an intrusion, revealing switched Ethernet. The above issues can be resolved by setting the exchange hub to static binding. When your host exhibits unexpected behaviour like slow network, IP packets presented higher ,a feasible solution is to let the network administrator notice .

Vulnerabilities in the security of Windows operating system

ISAPI buffer is the most prevalent version of Microsoft Windows NT in Microsoft IIS(Internet Information Server).Several ISAPIs(Internet Services Application Programming Interface)are hastily installed when IIS is installed. IIS server performance can be increased by developers using a number of dynamic link libraries (DLLs) like idq.dll. This presents an opportunity for an attacker to pass data through the DLL, trigger a buffer overflow ,and take over the IIS server.Ifit is discovered that the system has this kind off law, the solution to the aforementioned problem is to install the most recent Microsoft patches. The system should run the necessary minimal service system in accordance with the notion for it to work consistently.

Internet security flaws

The Transmission control protocol/ Internet protocol is used by the Internet, hence its deficiencies are contributed to the emergence of an unsafe Internet. Despite its strength, the TCP/IP protocol only supports a limited number of independent applications. An exclusive identifier for the network node is provided by the TCP/IP protocol in the IP Address. The IP address of the node is not completely resolved, allowing the attacker to modify it directly while claiming to be a safe node.

.

1.The Internet Protocol Source Routing option is put up in IP packets for testing reasons .The direct presentation of node routing information by this option gives attackers the opportunity to utilise it to establish unauthorised connections.

2..To ensure dependable routing for the Local Area Network nodes(LAN), the Routing Information Protocol (RIP) is used to publish dynamic routing information.

3.The existing fire wall system can only detect IP addresses and protocol ports, aswellastheintegrityofloginuseridentities

Computer Virus

Computer viruses are contagious, latent, triggers, and have destructive qualities. They can be undetectedly stored, executed, and concealed in executable programmes and data files, activating the access control system. The two basic ways that a computer virus is disseminated are by copying data and running programmes. Floppy discs ,hard drives, CDs, and networks are the primary means of virus transmission in daily life. Computer virus may cause the system to operate less efficiently, or it mayerase files, corrupt files, or even cause data loss and hardware destruction. As a result of the proliferation of networks in recent years, a number of harmful viruses have emerged, causing significant damage to computer networks.

Artificial malicious attacks

An attack on a computer network is most vulnerable to malicious software.

Malicious attacks can be classified as either active or passive attacks using a range of techniques to target the accuracy and reliability of the information. A passive assault takes place under regular operating settings, has no impact on the network, and uses theft and decoding to gain sensitive information. The two aforementioned attack types have the potential to seriously damage computer networks and expose sensitive information. Network hackers frequently utilize eaves dropping, in filtration in to sensitive information systems, obtaining and attacking in to key information, and modifying and destroying the regular operation of the network due to the flaws and vulnerabilities that more or less exist in current network software .Information network failure, data loss, or system paralysis significantly affect the politics and economy of the nation.

The Natural environment

As multiple computer or terminal regions are typically connected by cable links or radio waves in computer networks, the physical environment as well as the social context will have a significant impact. Natural disasters that can seriously harm the network and its influence include earthquakes, cyclones, fires, and temperatures that are too hot, humid, or dusty; Transmission of data and information would be hampered by strongcurrent and magnetic fields. Lightning can readily pass through cables and harm computers connected to the internet, paralysing computer networks. This makes computer networks vulnerable to lightning strikes. The network will experience moreman-made devastation, dealing a fatal blow to the system because of the poor socialclimate.

THE STRATEGY FOR NETWORK SECURITY TECHNOLOGY'S APPLICATION

Security is essential for a network' s survival since only in a safe, secure environment can a network fulfil its full potential. The advancement of network security technology is a result of people's increased use of the internet. It involves a variety of technical aspects ,but the main ones include firewalls, intrusion detection systems, and authentication of network safety.

VPN Technology

The newest technology to address the issueofinformationsecurityisthevirtualprivatenetwork (VPN), which creates a dedicatednetwork on the public network and turns data into a secure encryption-enabled "pipe" on the public network. One of the most popular technology topics is VPN. The construction of a virtual private network (VPN) can be accomplished usingeithertunneltechnologyorroutingfiltrationtechnology.

The four technologies listed below are primarily used by the current VPN to ensuresecurity: tunnel construction Technology for key management, encryption, and user identity authentication. Included are a few well-known L2TP tunnelling and IPsec techniques. Different levels of technological security services should be supported by VPN tunnel, PPTP tunnel, and other tunnelling techniques. Including various degrees of source identification, data encryption ,and other security features. There are various ways to categorise VPNs ,including dial-up and shuttle access; According to the tunnel protocol, there are two additional layers; In a manner, it can be separated server-sponsored. Into client-sponsored

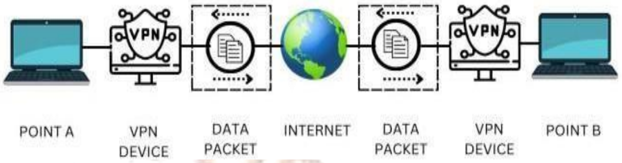
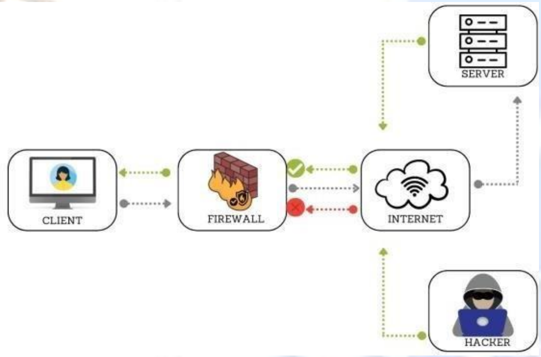


FIG.1 VPN TECHNOLOGY

FirewallTechnology

A firewall is a network access control device that both explicitly permits and denies access to all communication data.;unlike a simple router, which determinesthe direction in which network information is transmitted, A firewall is important forthe execution of a single or many system access control strategies.. Most firewalls combine several features to raise their levelof security against malicious attacks on the transmission network. One of the most widely used technologies includes static state packet filtering, dynamic packet filtering, and proxy server technology, but in actual use, the systemshould take into account security network connectivity as well as cost and performance. Moreover, modern goods have incorporated VPN technology as well as firewall and intrusion detection technologies. Since IP addresses are the primary basis for firewall security control, it is challenging to offer the user a consistent firewall security policy both inside and outside of the firewall, Therefore, because the firewall only allows coarse-grained access control, the internal use of additional security methods, such as access control, is not authorised. Additionally, because firewalls have so many systems, it may be difficult to run and set them.(router, filters, proxy servers, gateways, and forts hosts).

FIG 2. FIREWALL TECHNOLOGY



Intrution Detection Technology

In the field of network security research, intrusion detection technology is a significant approach. It is a type of proactive safety protection technology thatdetects intrusions of internal, external, and real-time protection misoperation and stops the corresponding intrusion before the network system is compromised. The basic purpose of an intrusion detection system, often known as an IDS(Intrusion Detection System),is to identify intrusions. In addition to detecting, it also plays a part in preventing invasion. Precursor intrusion detection leading to processing (e.g., stop, closed).There are technically two different types of invasive monitoring detection models: those that require a legal justification for the invasion of the archive and those that are subject to threat level assessment and recovery.

1. **Anomaly detection model:**. If it is possible to define acceptable conduct, then each undesirable behaviour constitutes an invasion. Detection and acceptable behaviour, the deviation between each item. A higher proportion of false positives in the test model makes up for low non-response rates.
2. **Feature detection model:** If it is possible to characterize all of the inappropriate behaviour and each can match behaviour, detection and the degree of resemblance between known inappropriate conduct would raise concern**.** It will leverage all known system weaknesses and attack features of composition to attack formal procedures**,** like libraries, and then it will capture packets with a mode matching approach and thoroughly Examine the features of libraries to decide whether anattack or harmful invasion is taking place. This model has a low false positive rate, but non-response rates are higher. With the advancement of network technology, the flaws and inadequacies of this testing method have become more and more obvious: the amount of data needed to match is too large, and it can only identify known attacks, such as those that are simple to trick.

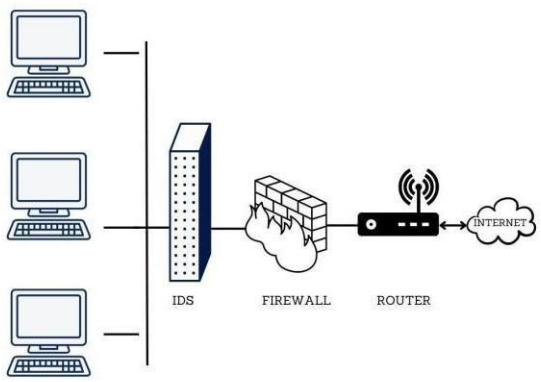


FIG.3 INTRUSION DETECTION TECHNOLOGY

Data encryption Technology

Data encrpytion technology is information encryption intended to protect network data, files, passwords, control information, and secure online data transmission. The three most frequently employed techniques are link encryption, end point encryption, and three node encryption. Link encryption is utilised to safeguard the network nodelink betweeninformationsecurity.

End-to-end encryption is used to safeguard data from source to destination users, whereas encryption between source and destination nodes is used to protect the transmission channel between them. A number of encryption algorithms are used in the information encryption process, which offers excellent which benefits the larger at the expense of the excellent security and protection Information secrecy tends to be only possible with information encryption. The encryption algorithm can be classified into conventional cryptographic algorithms and public key cypher algorithms if the classification and the key are the same. The receiver and sender of a conventional password both utilize the same key, making The keys for encryption and decryption are equivalent or identical. Public key cryptography makes decryption more challenging because the sender and recipient utilise identical keys .In this paper, a key encryption key is derived. Ofcourse, in practise, users typically combine traditional password encryption with public key cryptography ,such as utilising DES or IDEA to encryptdata and RSA to communicate the sessionkey.

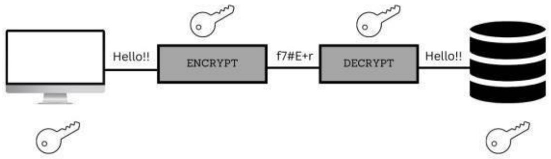


FIG 4.DATA ENCRYPTION TECHNOLOGY

Authentication Technology

For all types of information system security in an open environment, certification is a crucial technology to block malicious attacks. There are two main goals for certification:

1. To confirm that the sender's authentication information is accurate.
2. To check the information's integrity to make sure it hasn't been tampered with as it is being transmitted, replayed, delayed,etc.

The following key certification methods are pertinent: message identity verification, digital signature, and authentication.

The problem of the communication parties interested in circumstances to prevent third-party harm and camouflage has been resolved by message authentication and identity authentication. A digital signature can prevent someone from claiming to send and receive information and from stopping actions that have already been sent and received.

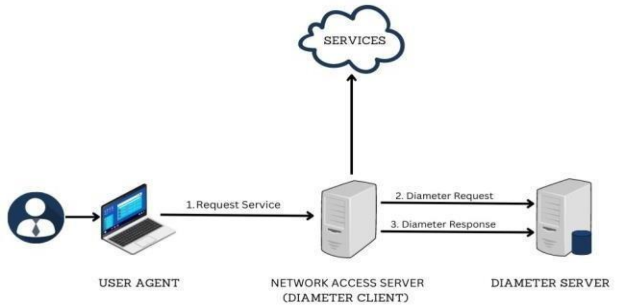


FIG 5. AUTHENTICATION TECHNOLOGY

Access Control Technology

The key objective of access control, which is the primary method of network security and protection, is to prevent unauthorized access to and use of the network's resources. Access control is also one of the most crucial core methods of network security because it safeguards the vital means of the network's resources. Other access control technologies are also included, such as network access control, security control ,property safety control directories, webserver security control, network monitoring and locking control, and network port and node security control .The number and type of access control can be easily adjusted depending on the network security level and network space environment.

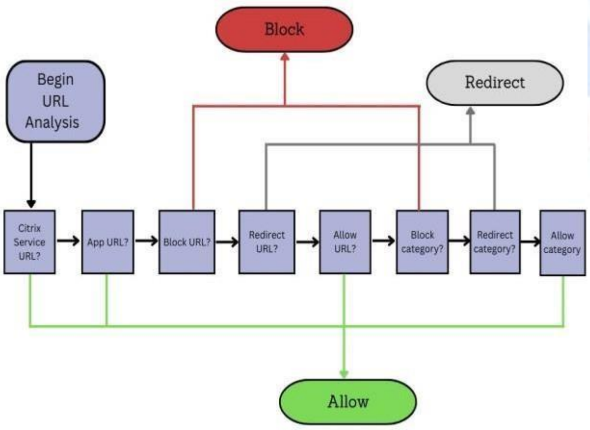


FIG 6 .ACCESS CONTROL TECHNOLOGY

Design Principle

The following principles should be followed Considering network security when creating and putting into place a network security protection system:

1. The principle of least privilege states that any item should only be granted the privileges necessary for them to fulfil their specified responsibilities, stay protected from attack, and less invasion-related casualties.

2.The"defense-in-depth"principle: A multi-layer safety mechanism called network security protection is used top revent cyber attacks. The network's "single failure point " will develop.

3.The blocking point principle states that safety control points should be the optimum network security protection mechanism. It's referred to as "chokespots" in the interconnection network, and It makes network security management simpler and more straight forward Monitoring and auditing network communication.

4. The security chain's weakest link The key to the chain's strength is protection; the answer is to keep the balance of strength.

5.Failure to protect state principle: "Fail-safe"failuremodesshouldbeincludedinthenetworksecurityprotectionsystem**.**, meaning that in the event of a failure, thefirewallshould be restarted or it would collapse and prevent access to the outside world and the internal network. network security is still necessary for pointguard in daily work and will significantlylessennetworksecurityconcealedhazard.

6.The default declined state principle : From a security perspective, failure protection state is the default declined to state.

Conclusion

The field of network information security is rapidly evolving. This means that only employing a few protective measures will note sure network information security; rather,we must make full use of a variety of protection strategies, integrating their benefits and working together toestablisha network information security protectionsystem. Based on many years of network security work, the author has made a detailed elaboration of the common hidden network security danger, summarised some uses of networks security strategy, and elaborated the basic principle of the design of network security protection system. Practice demonstrates that this still holds some value as a reference. Work on

Reference

[1] Anderson J P. Computer SecurityThreatMonitoringandSurveillance[P]. PA15034,USA.2015.8.

[2] B.Endicott.ActiveDefensetoCyber Attacks. Information Assurance andSecurity[J].2014.9.

[3] Yang Junsheng.ApplicationofVirusProtectionTechnologyin Computer Network Security in Big Data Environment[J].ComputerFan,2018(11)78.

[4] DongChengwu.Briefdiscussiononcampusinformationnetworksecurityprotectionandmanagementin HigherVocationalColleges[J].Informationrecordingmaterials,2018,19(11):141-142.

[5] Chen Liangliang. Analysis of the mainhidden dangers and management measuresof computer network security [J]. Networksecuritytechnologyandapplication,2018(10):6+64

[6] QiuShichen. Preliminary study on computer network information security and protection

[7] InformationCommunication,2018(10): 137-138.5.LiuZhipeng.Analysisofnetworksecurityissues under the Internet+ new mode .Computer knowledge and technology,2018,14(28):21-2