The Research of Computer Network Security and ProtectionStrategy

[1]**RAJANIKANTA SAHU,** *Gandhi Institute of Excellent Technocrats, Bhubaneswar, India*

[2]**RASHMITA SAHU,** *Kruttika Institute of Technical Education, Khordha, Odisha, India*

Abstract. With the widespread popularity of computer network applications, its security is also received a high degree ofattention.Factorsaffectingthesafetyofnetworkiscomplex,fortodoagoodjobofnetworksecurityisasystematicwork,hasthehighchallenge. Forsafetyandreliabilityproblemsofcomputernetworksystem,thispapercombinedwithpracticalworkexperience,fromthethreatofnetworks ecurity,securitytechnology,networksomeSuggestionsandmeasuresforthesystemdesignprinciple,inordertomakethemassesofusersincomp uternetworkstoenhancesafetyawarenessandmastercertainnetworksecuritytechnology.

Keywords: NetworkSecurity;Technology;Strategies;Principle

INTRODUCTION

Nowadays, the application of computer network has extended to every corner of the world and areas, is anunprecedentedimpactonpeople'sworkandlife,aswellaselectricpower,transportation,andhasincreasinglybecomean integral part of people's life. At the same time, with the expanding of network size, and the understanding ofnetwork knowledge is more and more in-depth, more and more unsafe factors such as the network attack, has been aserious threat to network and information security. Computer network security has become a global concern. Computernetwork and information security technology is the core issue of the computer and network systems for effectiveprotection. Network security protection involves very wide range, from a technical level, mainly including dataencryption, identity authentication, intrusion detection and intrusion protection, virus protection and virtual privatenetworks (VPNS), etc., some of these technologies is active defense, some of them are passive protection, and someare to provide support and platform for the research of security. Computer network security by adopting varioustechnical and management measures, make the normal operation of the network system, to ensure the availability,integrity and privacy of network data. So, to establish the purpose of network security protection is to ensure that thedatatransmissionandexchangethroughthenetwork,nothappensuchasadd,modify,lossandleak.

THEHIDDENTROUBLEINATYPICALCOMPUTERNETWORKSECURITY

Routingprotocoldefects

(1) Sourceroutingoptionusing.SourceroutingintheIPheaderoptionisusedtotheIPpacketrouting,thus,anIPpacket can be specified according to the forecast of routing to arrive at the destination host. But it also createdopportunitiesfortheinvaders,whenahostknowinadvancethatthereisatrustedhost,youcanusethesourceroutingoptions disguised as a trusted host, so as to attack system, the equivalent of make the host may be under attack fromallother hosts.

(2) The forge ARP packet. Forge ARP packet is a kind of very complex technology, involves many aspects ofTCP/IP and Ethernet characteristics, in this as ARP security issues is not very appropriate. Fake ARP packet is themainprocesstotheIPaddressofthe destinationhostandEthernetaddressforanARPpacketsourceaddress,thiscan

causeanotherIPspoof.InthisattackmainlyinswitchedEthernet,switchedEthernet,exchangehubinreceivingeachARPpacketu pdateCache.ConstantlysendspoofARPpacketcanmakebothpackagessenttothedestinationhosttoan intruder, so switched Ethernet can be monitored. The ways to solve the above problems is: will exchange hub setasstaticbinding.Afeasibleapproachiswhenyourhostrunsabnormally(slownetwork,IPpacketspresented .accordingto higher),reflect to thenetworkadministrator.

Windowsoperatingsystemsecurityflaw

ISAPI buffer overflow Microsoft IIS (Internet Information Server) is the most used Microsoft Windows NT andWindows2000Serversoftware.AtthetimeofinstallIIS,multipleISAPI(InternetServicesApplicationProgrammingInterfa ce)isautomaticallyinstalled.ISAPIallowsdeveloperstouseavarietyofdynamiclinklibraryDLLstoextendthe IIS server

performance. Some dynamic link libraries, for example, idq.dll, a programming error, so they are notcorrect boundary check. In particular, they don't block the long string. An attacker can take advantage of this to theDLLtosenddata,resultinbufferoverflow,andthencontroltheIISserver.Solutiontotheproblemoftheaboveisifitisfoundthatsystemhasthiskindofdefect,theninstallthelatestMicrosoftpatches.Atthesametime,shouldcheckand cancel all don't need the ISAPI extension. Regularly check whether these extensions is restored. Least privilegeruletorememberisthatthesystemshouldruntherequired minimumservicesystemtoworknormally.

SafetydefectsexistingintheInternet

TheInternetuseTCP/IPprotocol,sotheflawsoftheTCP/IPprotocolitselfledtothedevelopmentoftheInternetisnotsafe.AlthoughtheTCP/IPprotocolwithstrongability,networkinterconnectiontechnology,supportformultipleindependent application protocol etc., however, due to the agreement, when they were written without consideringsafety factors, so a lot of security problems in the agreement. Mainly include: TCP/IP protocol data flow using cleartexttransmission,especiallyintheuseofHTTP,FTP,Telnetanduseraccountandpasswordinplaintexttransmission,sothe datainformationiseasy tobe onlinehacking, tamperingandforgery.

(1) The Source Address Spoofing (the Source Address Spoofing), TCP/IP protocol in the IP Address as a uniqueidentifier for the network node, the node's IP Address is not completely fixed, so the attacker can directly modify thenode'sIP Address withinacertainscope,pretendingto beatrustednode'sIP Address.

(2) The Source Routing cheating (Source Routing Spoofing), IP packets for test purposes set up an options - IPSource Routing, this option can indicate to the node routing directly, so that the attacker can use this option to cheat,illegalconnection.

(3) Therouting informationprotocol(RIP) Attacks attack.RIPprotocolusedtopublish dynamicroutinginformationinthelocalareanetwork(LAN),itistoprovideconsistent routingforthenodesinthelocalareanetwork(LAN) designed and accessibility of information, but the node to receive the information authenticity checks, so anattacker could issue incorrect routing information online, take advantage of a router or host ICMG redirectioninformation,realize the networkattack.

(4) Identify attack (Authentication Attacks), the current firewall system only to identify the IP address, protocolport,to identify the effectivenessofthe loginuser identity.

ComputerVirus

Computer viruses can be stored, executable and can be hidden in the executable programs and data files withoutbeing found that trigger the access control system after an executable program, it is contagious, latent, triggers anddestructivesexualcharacteristics.Acomputervirusismainlytransmittedbycopyingfiles,files,andruntheprogramoperation. In the course of everyday use, floppy disk, hard disk, CD and network is the main way of spreading thevirus. Computer virus after running light could reduce the system efficiency, or may damage files, delete files, evenmake the data loss, destruction of the system hardware, all kinds of unpredictable consequences. In recent years, theemergence of a variety of malignant viruses are based on the spread of the network, the computer network virusdamageisverybig.

Artificialmaliciousattacks

This is the biggest threat to the computer network attack. Malicious attacks and can be divided into active attackandpassiveattack.Attackinvariouswaystoselectivelydestroythe validityoftheinformationandintegrity;Passiveattack is in normal working conditions, does not affect the network to intercept, and steals, deciphering to obtainimportant confidential information. These two kinds of attacks can cause great harm to computer networks, and leadto a leakage of important data. Now use the network software is more or less exist some shortcomings andvulnerabilities, network hackers often use intrusion into important means of information system, eavesdropping,obtain and attack into important information about the sensitivity, modify, and destroy the normal use of theinformation network, data loss or system paralysis, have significant political influence and economic losses to thecountry.

Thenaturalenvironment

Computer network through wired links or radio waves to connect different areas of computer or terminal, often isinformationtransmissioninline,sothenaturalenvironmentandsocialenvironmentofcomputernetworkwillproducea great impact. Bad for nature, such as temperature, humidity, dust conditions, such as earthquake, cyclone, fire andaccidentcan causeseriousdamagetothenetwork andinfluence;Heavy current,magneticfieldwouldspoiltransmission of data information. Computer network is also easy to lightning strike, lightning can easily through thecableanddamagetothecomputerinthenet,makecomputernetworkparalysis.There'snotagoodsocialatmospherewillincreas

e tothe network man-made destruction,bringdevastatingblowtosystem.

THEAPPLICATIONOFTHE STRATEGYFORNETWORKSECURITYTECHNOLOGY

Security is the security of the network to survive, only safe and secure, network can realize its own value. Thedevelopmentofnetworksecuritytechnologyaspeoplenetworkpracticeanddevelopment,itinvolvestechnicalisverywide,themaintechniquessuchasauthentication,encryption,firewallandintrusiondetectionisanimportantdefenseofnetworksecurity.

VPNTechnology

VPN is the latest to solve the problem of information security, one of the most successful technology subject, avirtual private network (VPN) technology is on the public network to establish dedicated network, make the datathrough the security of encryption "pipe" in the public network. To build on the public communication network VPNthere are two kinds of mainstream mechanism, these two mechanisms for routing filtration technology and tunneltechnology. The current VPN mainly adopts the following four technology to ensure safe: tunnel technology,encryption technology, key management technology and user identity authentication technology and equipment.Amongthem,severalpopulartechniquesforthePPTP,L2TPtunnelandIPsecVPNtunnelmechanismshouldbeablet o have different levels of technology security services, the security services including different intensity of sourceidentification, data encryption, etc. VPN have several classification methods, such as the access into the shuttle VPNanddial-upVPN;Accordingtothetunnelprotocolcanbedividedintothesecondandthirdlayer;Accordingtoawaycanbe dividedinto sponsored bythe client and the server.

Firewalltechnology

Firewall is a network access control devices, to refuse in addition to explicitly allow through all communicationdata,itisdifferentfromsimplerouterwilldeterminethedirectionofnetworkinformationtransmission,butaccess tothe site in the network transmission through relevant to the implementation of a set of one or a set of system accessstrategy. Most firewalls are the combination of several functions to protect themselves, in the form of transmissionnetwork from malicious attacks, one of the most popular technology with static state of packet filtering, dynamicpacketfiltering,filtering,andtheproxyservertechnology,increasetheirlevelofsecurity,butintheconcretepracticeofth esystemshouldnotonlybeconsideredcostperformance,andtoconsidersecuritynetworkconnectivity.In addition,today'sgoodalsoadoptedtheVPNandviewingofafirewallandintrusiondetectiontechnology.Thefirewallsecuritycont rolismainlybasedonIPaddress,itisdifficulttoprovideaconsistent,bothinsideandoutsidethefirewallsecurity strategy for the user; And the firewall only coarse-grained access control, also can't and enterprise internaluse other security mechanisms (such as access control) integrated use; In addition, difficult to manage and configurefirewall by multiple systems (router, filters, proxy server, gateway, forts host) of firewall, management to avoidnegligence.

Intrusiondetectiontechnology

Intrusion Detection technology is a hotspot in the research of the network security, is a kind of active safetyprotection technology, provides the invasions of internal, external and real-time protection misoperation, interceptcorresponding Intrusion before network System compromised. Along with the development of the era, IntrusionDetection technology will develop in the direction of the three: distributed Intrusion Detection, intelligent IntrusionDetection and comprehensive security defense solutions. Intrusion Detection System (Intrusion Detection System,IDS for short) is a combination of software and hardware for Intrusion Detection, its main function is to detect, inaddition to detecting part prevent invasion; Intrusion detection of precursors, thus processing, such as stop, closed,etc.; Invasion of the archive, providing legal basis; Network intrusion events under threat level assessment andrecovery,andother functions.
Technically, there are two kinds of invasive monitoring detection model: (1) anomaly detection model, detectionandacceptablebehavior,thedeviationbetweentheeveryitemifitispossibletodefineacceptablebehavior,theneachuna cceptable behavior is invasion. The test model of non-response rates low, but higher rate of false positives. (2)Featuredetectionmodel;Detectionandthedegreeofmatchbetweenknownunacceptablebehavior,ifitispossibletodefine all the unacceptable behavior, and each can match behavior will cause alarm. It will be all known systemvulnerabilities and attack characteristics of composition an attack to the formal methods, such as libraries, and thenwill capture the packets with mode matching method and the features of library detailed comparison, to determinewhethertoattackormaliciousinvasion,lowrateoffalsepositives,thismodelbutnon-responserateshigher.Withthedevelopment of network technology, this method of testing the shortcomings and the insufficiency of graduallyapparent:needtomatchtheamountofdataistoobig,canonlydetect known

attacks,suchaseasytobedeceived.

Dataencryptiontechnology

Is the purpose of information encryption protection network data, files, password, and control information, andprotecttheonlinetransmissionofdata.Thecommonlyusedmethodsarelinkencryption,theendpointencryptionandencryption threenodes,thepurposeoflinkencryptionistoprotectthenetworknodelinkbetweeninformationsecurity;The end-to-end encryption is the purpose of the source end user to end user's data protection; Node is the purpose ofencryptionbetweenthesourcenode anddestinationnodetransmissionlinktoprovideprotection.
Informationencryptionprocessisaconcreteimplementationbyavarietyofencryptionalgorithm,toprovidehighsecurity and protection at the expense of the smaller. In most cases, information encryption is the only way to ensureinformation confidentiality. If according to the classification and the key is the same to the encryption algorithm canbe divided into conventional cryptographic algorithms and public key cipher algorithm? In conventional password,use the same key, the receiver and the sender is the encryption and decryption keys are the same or equivalent. Inpublickeycryptography,thereceiverandthesenderusekeysarethesame,anditisalmostimpossiblefromdecryptionkey
encryption key is derived in this paper. In practice, of course, people usually use the conventional password andpublic key cryptography together, such as: using DES or IDEA to encrypt information, and RSA is used to transmitthesessionkey.

Authenticationtechnology

Certification is an important technology to prevent malicious attacks, it is important to all kinds of informationsystem security in open environment, themain purposeof thecertification, there are two: 1)authentication informationofthesenderislegal;(2)toverifytheintegrityoftheinformationtoensurethattheinformationhasnotbeentamperedwith in the process of transmission, replay or delay, etc. The relevant certification main techniques are: messageauthentication, identity authentication and digital signature. Message authentication and identity authentication hassolvedthecommunicationpartiesinterestedinconditionstopreventthedamageofathirdpartyandcamouflage.

Digitalsignaturecanpreventothersimpersonatesendingandreceivingofinformation,andpreventIlaterdeniedthatIhave beensendingand receivingactivities.

Accesscontroltechnology

Accesscontrolisthemainstrategyofnetworksecurityandprotection,themaintaskistoensurethatnotbeillegaluse of network resources and access to very much, also is the maintenance of network system security, to protect theimportantmeansofnetworkresources,isoneofthemostimportantcorestrategiesofnetworksecurity.Accesscontroltechnology including network access control, network access control, security control, property safety controldirectory, the web server security control, network monitoring and locking control, network port and node securitycontrolandsoon.Accordingtothelevelofnetworksecurity,networkspaceenvironmentisdifferent,canbeflexiblysetthe amount and type ofaccesscontrol.

DESIGNPRINCIPLE:

The design principle of network security protection system from the perspective of the network security of networksafeprotectionsystemdesignand implementation shouldbeaccordingtothe followingprinciples:
(1) The least privilege principle: any object should only have the privilege of the object need to complete theirassignedtasks,avoid exposureunder attack,and reducelosses causedbyinvasion.
(2) The principle of defense in depth: network security protection system is a multi-layer safety system, avoidbecome"singlefailure point"inthenetwork.
(3) The blocking point principle: the ideal network security protection system should be the safety control pointsin interconnection network, called it "choke points" here, it simplifies the network security management, easy tomonitornetworkcommunicationand audit.
(4) Principle:theweakestlinkchainofsecurityprotectionisthebasicprincipleofthestrengthofitsweakestlinks,thesolutionist o keep the balanceofstrength.
(5) Failure to protect state principle: the network security protection system failure modes should be "fail - safe"type,namely,oncethefailure,restartthefirewallorcollapsewillblocktheinternalnetworksafetyandtherestoftheworld.
(6) The default declined to state principle: from a security point of view, the default declined to state is failureprotectionstate.

CONCLUSION

The network information security is a fast changing, update the field. This means that simply using a certainprotective measures is no guarantee that the network information security, we must comprehensive use of variousprotection strategy, integrating the advantages, cooperate with each other, so as to set up the network informationsecurityprotectionsystem.Basedonmanyyears'networksecurityworkpracticeoftheauthortothecommonnetwork securityhiddendangerhasmadethedetailedelaboration,summarizessomeuseofnetworksecuritystrategy,andthedesign of network security protection system elaborated the basic principle, practice shows that still has a certainreference value. Network security work, is still a need in daily work point guard and will largely reduce networksecurityhidden danger, toprotect the normaluse ofthenetwork.

REFERENCES

1. AndersonJP.ComputerSecurityThreatMonitoringandSurveillance[P].PA15034,USA.2015.8.
2. B.Endicott.ActiveDefensetoCyberAttacks.InformationAssuranceandSecurity[J].2014.9.