NetworkSecurity

[1]**NALINI KUMAR SETHY,** *Gandhi Institute of Excellent Technocrats, Bhubaneswar,India*
[2]**RASHMI RANJAN DASH,** *Kruttika Institute of Technical Education, Khordha, Odisha, India*

***Abstract*-**Networksecurityhasbecomemoreimportanttopersonal computer users, organizations, and themilitary.Withthe advent of the internet, security became a major concern andthehistoryofsecurityallowsabetterunderstandingoftheemergence of security technology. The internet structure itselfallows formany security threats to occur. If the architecture oftheinternetismodified,itcanreducethepossibleattacksthatcan be sent across the network. Knowing the attackmethodsallows us to emerge with appropriate security. Many businessessecure themselves from the internet by means of firewalls andencryption mechanisms. The businesses create an "intranet" toremainconnectedtotheinternetbutsecuredfrompossiblethreats. The entire field of network security is vast and in anevolutionary stage. Inordertounderstandthe research beingperformedtoday,backgroundknowledgeoftheinternet,itsvulnerabilities, attack methods through theinternet, and securitytechnologyisimportantand thereforetheyarereviewed.

***IndexTerms*-**
DataSecurity,InternetArchitecture,IPv4,NetworkSecurity.

I. INTRODUCTION

Theworldisbecomingmoreinterconnectedduetointernetandnew networkingtechnology.Thereisalargeamountofpersonal,commercial,military,andgovernmentinformationonnetworkinginfrastructure sworldwide.Networksecurityisbecomingofutmostimportancebecauseofintellectualpropertythatcanbeeasilyacquiredthroughtheinternet.Therecanbe breachinintellectualproperty.

Therearetwotypesoffundamentallydifferentnetworks:data networks and synchronous network comprised of switches.The internet is considered a data network.Since the current datanetwork consists of computer-based routers, information can beobtained by special programs, such as "Trojan horses," planted inthe routers. The synchronous network that consists of switchesdoes not buffer data and therefore are not threatened by attackers.That is why security is emphasized in data networks, such as theinternet,and other networksthatlinkto the internet.

The vast topic of network security is analyzed by researchingthefollowing:

1. Internetarchitectureandvulnerable security aspects oftheInternet
2. Typesofinternetattacksand securitymethods
3. Securityfornetworkswithinternetaccess
4. Currentdevelopmentinnetworksecurityhardwareand software

II. NETWORKSECURITY

System and network technology is a key technology for awidevarietyofapplications.Networksandapplicationsneedsecurity.Although,network security is a critical requirement,thereisasignificantlackofsecuritymethodsthatcanbeimplemented easily.

There exists a "communication gap" between the developersofsecuritytechnologyanddevelopersofnetworks.Networkdesign is a well-developed process that is based on the OpenSystems Interface (OSI) model. The protocols of different layerscan be easily combined to create stacks which allow modulardevelopment.The implementation of individual layers can bechangedlaterwithoutmakingotheradjustments,allowingflexibility in development. In contrast to network design, securenetwork design is not a well-developed process. There isn't amethodology to manage the complexity of security requirements.Secure network design does not contain the same advantages asnetworkdesign.

Network security doesn't mean securing both end computers.Whentransmittingdatathecommunicationchannelshouldnotbevulnerabletoattack.Apossiblehackercouldtargetthecommunication channel, obtain the encrypted data, and decrypt itand re-insert a false message. Securing the middle network is justasimportantassecuringthecomputersandencryptingthemessage.

When developing a secure network, the following need to beconsidered [1]:

1. Access–Authorizedusersareprovidedthemeanstocommunicatetoand froma particular network
2. Confidentiality–Informationinthenetworkremainsprivate
3. Authentication–Ensuretheusersofthenetworkarewhotheysaytheyare
4. Integrity–Ensurethemessagehasnotbeenmodifiedintransit
5. Non-repudiation–Ensuretheuserdoesnotrefutethatheused thenetwork

With the understanding of security issues, potential attackers,neededlevelofsecurity,andfactorsthatmakeanetworkvulnerabletoattackaneffectivenetworksecurityplanisdeveloped[1].To makethecomputerlessvulnerabletothenetworktherearemanyproductsavailable.Thesetoolsareencryption,firewalls,intrusion-detection,andsecuritymanagementandauthenticationmechanisms.Businesesthroughout the world are using a combination of some of thesetools."Intranets"arebothconnectedtotheinternetandreasonablyprotectedfromit.Theinternet architectureitselfleads

tovulnerabilitiesinthenetwork.Understandingthesecurityissues of the internet greatly helps to develop secure solutions toprotectthe networksfromtheinternet.

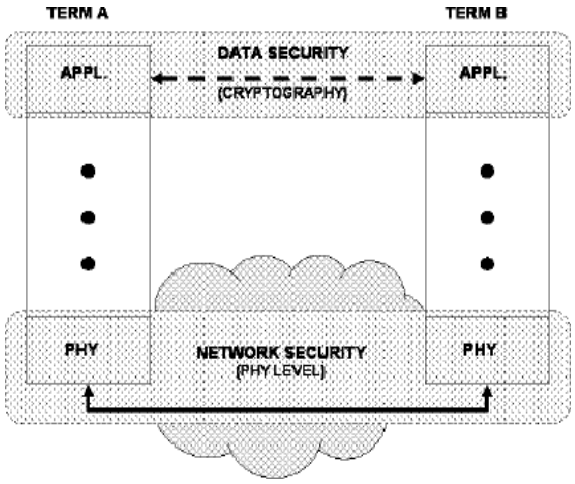
The types of attacks through the internet needtoalso bestudied to be able to detect and guard against them. Intrusiondetection systems are established based on the types of attacksmost commonly used. Network intrusions consist of packetsthatareintroducedtocauseproblemsforthe followingreasons:

- Toconsumeresourcesuselessly
- Tointerferewithanysystemresource'sintendedfunction
- To gain system knowledge like passwords, logins thatcanbe exploitedinlaterattacks

III. DIFFERENTIATINGDATASECURITYAND NETWORKSECURITY

Data security is the aspect of security that allows a client'sdata to be transformed into unintelligible data for transmission.Even if this unintelligible data is intercepted, a key is needed todecode the message. This method of security is effective to acertain degree. Strong cryptography in the past can beeasilybrokentoday.Duetoadvancementofhackers,cryptographic methodshaveto develop constantlyto beonestep ahead.

When transferring cipher text over a network, it is helpful tohave a secure network. This will allow for the cipher text to beprotected, so that it is less likely for many people to even attemptto break the code.A secure network will also prevent someonefrominsertingunauthorizedmessagesintothenetwork.Ther efore,hardciphersareneededaswellasattack-hardnetworks.



[1] **Figure1**

The relationship of network security and data security to theOSImodelisshowninFigure1.Itcanbeseenthatthecryptographyo ccursattheapplicationlayer;thereforetheapplicationwritersareawar eofitsexistence.Theusercanpossibly choose different methodsofdatasecurity.Networksecurityismostlycontainedwithint hephysicallayer.Layers above the physical layer are also used to accomplish the networksecurity required. Authentication is performed on a layer abovethe physical layer. Network security in the physical layer requiresfailuredetection,attack detectionmechanisms,andintelligentcountermeasure strategies[2].

IV. INTERNETARCHITECTUREANDVULNERABLE SECURITYASPECTS

FearofsecuritybreachesontheInternetiscausingorganizations to use protected private networks or intranets. TheInternet Engineering Task Force (IETF)has introduced securitymechanisms at various layers of the Internet Protocol Suite [4].These security mechanisms allow for the logical protection ofdata units that are transferred across the network. The currentversion and new version of the Internet Protocol are analyzed todetermine the security implications. Although security may existwithin the protocol, not all attacks are guarded against. Theseattacks are analyzed to determine other security mechanisms thatmaybe necessary.

The security architecture of the internet protocol known as IPSecurity is a standardization of internet security. IP security, IPsec, covers the new generation of IP (IPv6) as well as the currentversion (IPv4). Although new techniques, such as IP sec, havebeen developed to overcome internet's best-known deficiencies,theyseemtobe insufficient[5].

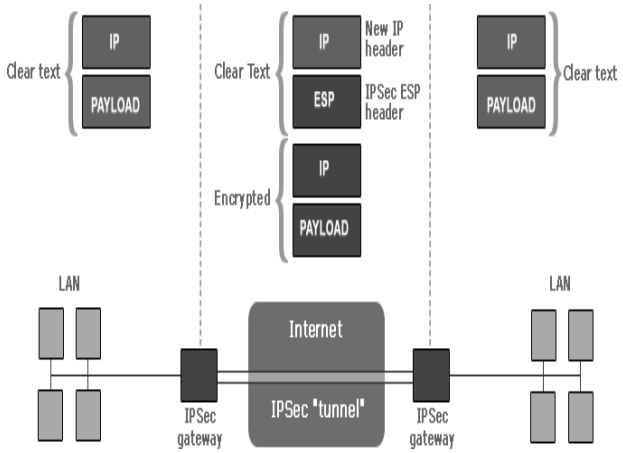


Figure2:showsavisualrepresentationofhow IPsecisimplementedto providesecurecommunications.

IPsec is a point-to-point protocol, one side encrypts, theotherdecrypts andboth sides sharekey orkeys.IPseccan beusedintwomodes,namelytransport modeandtunnelmodes.

V. ATTACKSTHROUGHTHECURRENTINTERNET PROTOCOLIPV4

1. CommonInternetAttackMethods

Commoninternetattacksmethodsarebrokendownintocategorie s.Some attacks gain system knowledge or personalinformation,suchaseavesdroppingandphishing.Attacksca n

alsointerferewiththesystem'sintendedfunction,suchasviruses, worms and trojans. The other form of attack is when thesystem's resources are consumes uselessly, these can be causedbydenialofservice(DoS)attack.Otherformsofnetworkintrusi onsalsoexist,suchaslandattacks,surfattacks,andteardrop attacks. Theseattacksare notaswell-knownasDoSattacks,buttheyare used in some form oranother even if theyaren'tmentionedbyname.

1.1 Eavesdropping

Interception of communications by an unauthorized party iscalled eavesdropping. Passive eavesdropping is when the personony secretly listens to the networked messages. On the otherhand, active eaves dropping are when the intruder listens andinserts something into the communication stream. This can leadto the messages being distorted. Sensitive information can bestolenthisway[8].

1.2 Viruses

Viruses are self-replication programs that use files to infectand propagate [8]. Once a file is opened, the virus will activatewithinthe system.

1.3 Worms

Awormissimilartoavirusbecausetheybothareself-replicating, but the worm does not require a file to allow it topropagate [8]. There are two main types of worms, mass-mailingworms andnetwork-aware worms. Mass mailing worms useemailasameanstoinfectothercomputers.Network-awareworms are a major problem for the Internet. A network-awareworm selects a target and once the worm accesses the target host,itcaninfectit bymeansofa Trojanor otherwise.

1.4 Trojans

Trojans appear to be benign programs to the user, but willactuallyhavesomemaliciouspurpose.Trojansusuallycarrysome payloadsuchasavirus[8].

1.5 Phishing

Phishingisanattempttoobtainconfidentialinformationfrom anindividual,group,ororganization[9].Phisherstrickusers into disclosing personal data, such as credit card numbers,onlinebankingcredentials,and other sensitiveinformation.

1.6 IPSpoofing Attacks

Spoofing means to have the address of the computer mirrorthe address of a trusted computer in order to gain access to othercomputers. The identity of the intruder is hidden by differentmeansmakingdetectionandpreventiondifficult.Withthecu rrent IP protocol technology, IP-spoofed packets cannot beeliminated [8].

1.7 DenialofService

Denial of Service is an attack when the system receiving toomany requests cannotreturn communication with the requestors[9].Thesystemthenconsumesresourceswaitingforthehan dshake to complete. Eventually, the system cannot respond toanymorerequestsrenderingitwithoutservice.

2. TechnologyforInternetSecurity

Internet threats will continue to be a major issue in the globalworld as long as information is accessible and transferred acrossthe Internet. Different defense and detection mechanisms weredeveloped todealwiththeseattacks.

*2.1 Cryptographicsy*stems

Cryptography is a useful and widely used tool in securityengineering today. It involved the use of codes and ciphers totransforminformationintounintelligibledata.Theseunintelligible dataisthustransferred inthenetworksafely.

2.2 Firewall

A firewall is a typical border control mechanism or perimeterdefense. The purpose of a firewall is to block traffic from theoutside, but it could also be used to block traffic from the inside.A firewall is the frontline defense mechanism against intruders. Itis a system designed to prevent unauthorized access to or from aprivate network. Firewalls can be implemented in both hardwareand software,ora combinationofboth[8].

2.3 IntrusionDetectionSystems

AnIntrusionDetectionSystem(IDS)isanadditionalprotection measure that helps ward off computer intrusions. IDSsystems can be software and hardware devices used to detect anattack.IDSproductsareusedtomonitorconnectionindetermining whetherattacksarebeenlaunched.SomeIDSsystems just monitor and alert of an attack, whereas others try toblockthe attack.

2.4 Anti-MalwareSoftwareandScanners

Viruses,wormsandTrojanhorsesareallexamplesofmalicioussof tware,orMalwareforshort.Specialso-calledanti-Malware tools are used to detect them and cure an infectedsystem.

2.5 SecureSocketLayer(SSL)

TheSecureSocketLayer(SSL)isasuiteofprotocolsthatisa standard way to achieve a good level of security between a webbrowserandawebsite.SSLisdesignedtocreateasecurechannel, or tunnel, between a web browser and the web server, sothat any information exchanged is protected within the securedtunnel. SSL provides authentication of clients to server throughthe use of certificates. Clients present a certificate to the server toprovetheiridentity.

VI. SECURITY ISSUES OF IP PROTOCOL

IPV6IPv6isthenextthingeveryone'stalkingabout.Froma security point of view, IPv6 is a considerable advancement overtheIPv4internetprotocolDespitetheIPv6'sgreatsecuritymecha nisms; it still continues to be vulnerable to threats. SomeareasoftheIPv6protocolstillposeapotentialsecurityissue.The new internet protocol does not protect against is configureservers,poorlydesignedapplications,orpoorlyprotectedsit es.

Thepossiblesecurityproblemsemergeduetothefollowing:

1. Headermanipulationissues
2. Floodingissues

3. Mobilityissues

HeadermanipulationissuesariseduetotheIPsec'sembeddedfunctionality[7].Extensionheadersdetersomecommon sources of attacks because of header manipulation. Theproblem is that extension headers need to be processed by allstacks, and this can lead toa long chain of extension headers.The large number of extension headers can overwhelm a certainnode and is a form of attack if it is deliberate. Spoofing continuesto be a security threat on IPv6 protocol. A type of attack calledportscanningoccurswhenawholesectionofanetworkisscanned to find potentialtargets with open services [5]. Theaddress space of the IPv6 protocol is large but the protocol is stillnot invulnerable to this type of attack. Mobility is a new featurethat is incorporated into the internet protocol IPv6. The featurerequires special security measures. Network administrators needto be aware of these security needs when using IPv6's mobilityfeature.

VII. SECURITYINDIFFERENTNETWORKS

Thebusinessestodayusecombinationsoffirewalls,encryption, and authentication mechanisms to create "intranets"that are connectedto the internet but protectedfrom it at thesametime.Intranetisaprivatecomputernetworkthatusesinternet protocols. Intranets differ from "Extranets" in that theformer are generally restricted to employees of the organizationwhileextranetscangenerallybeaccessedbycustomers,suppliers,or otherapproved parties.

There does not necessarily have to be any access from theorganization's internal network to the Internet itself.When suchaccess is provided it is usually through a gateway with a firewall,along with user authentication, encryption of messages, and oftenmakesuse of virtual privatenetworks(VPNs).

Although intranets can be set up quickly to share data in acontrolled environment, that data is still at risk unless there istight security. The disadvantage of a closed intranet is that vitaldata might not get into the hands of those who need it. Intranetshave a place within agencies.But for broader data sharing, itmightbebettertokeepthenetworksopen, withthesesafeguards:

1. Firewallsthatdetectandreportintrusionattempts
2. Sophisticatedviruscheckingatthe firewall
3. Enforced rulesforemployeeopeningofe-Mailattachments
4. Encryptionforallconnectionsanddatatransfers
5. Authenticationbysynchronized,timedpasswordsorsecuritycertificates

It was mentioned that if the intranet wanted access to theinternet, virtual private networks are often used. Intranets thatexist across multiple locations generally run over separate leasedlines or a newer approach of VPN can be utilized. VPN is aprivate network that uses a public network (usually the Internet)toconnectremotesitesoruserstogether.Insteadofusingadedicated, real-world connection such as leased line,a VPN uses"virtual"connectionsroutedthroughtheInternetfromthecompany'sprivatenetworktotheremotesiteoremployee.

VIII. CURRENTDEVELOPMENTSINNETWORK SECURITY

Thenetworksecurityfieldiscontinuingdownthesameroute.The same methodologies are being used with the additionof biometric identification. Biometrics provides a better methodof authentication than passwords. This might greatly reduce theunauthorized access of secure systems. The software aspect ofnetwork security is very dynamic. Constantly new firewalls andencryption schemes are being implemented. The research beingperformedassistinunderstandingcurrentdevelopmentandprojectingthe futuredevelopmentsofthefield.

1. HardwareDevelopments

Hardwaredevelopmentsarenotdevelopingrapidly.Biometric systems and smart cards are the only new hardwaretechnologiesthatarewidelyimpactingsecurity.Themostobvioususeofbiometricsfornetworksecurityisforsecureworkstation logons for a work station connected to a network.Each workstation requires some software support for biometricidentification of the user as well as, depending on the biometricbeing used, some hardware device. The cost of hardware devicesisonethingthatmayleadtothewidespreaduseofvoicebiometricsecurityidentification,especiallyamongcompaniesand organizations on a low budget. Hardware device such ascomputermicewithbuiltinthumbprintreaderswouldbethenextstep up.Thesedeviceswouldbemoreexpensivetoimplement on several computers, as each machine would requireitsownhardware device.

2. SoftwareDevelopments

Thesoftwareaspectofnetworksecurityisveryvast.Itincludes firewalls, antivirus, VPN, intrusion detection, and muchmore. The research development of all security software is notfeasible to study at this point. The goal is to obtain a view ofwhere the security software is heading based on emphasis beingplaced now.

IX. FUTURETRENDSINSECURITY

WhatisgoingtodrivetheInternetsecurityisthesetofapplications more than anything else. The future will possibly bethat the security is similar to an immune system. The immunesystemfightsoffattacksandbuildsitselftofighttougherenemies. Similarly, the network security will be able to functionasanimmune system.

The trend towards biometrics could have taken place a whileago,butitseemsthatitisn'tbeingactivelypursued.Manysecurity developments that are taking place are within the sameset of security technology that is being used today with someminoradjustments.

X. CONCLUSION

Network security is an important field that is increasinglygaining attention as the internet expands. The security threats andinternetprotocolwereanalyzedtodeterminethenecessarychangesinsecuritytechnology.Thesecuritytechnologyismostlysoftwarebased,butmany commonhardwaredevices are

used.The current development in network security is not veryimpressive.

Originally it was assumed that with the importance of thenetworksecurityfield,newapproachestosecurity,bothhardware and software, would be actively researched. It was asurprise to see most of the development taking place in the sametechnologies being currently used. Combined use of IPv6 andsecuritytoolssuchasfirewalls,intrusiondetection,andauthenticationmechanismswillproveeffectiveinguardingintellectual property for the near future. The network securityfield may have to evolve more rapidly to deal with the threatsfurther inthefuture.

REFERENCES

[1] Dowd,P.W.;McHenry,J.T.,"Networksecurity:it'stimetotakeitseriously,"Computer, vol.31,no.9, pp.24-28,Sep1998

[2] Kartalopoulos, S. V., "Differentiating Data Security and Network Security,"Communications,2008.ICC'08.IEEEInternationalConferenceon,pp.1469-1473,19-23May2008

[3] "Security Overview," www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.

[4] Molva, R., InstitutEurecom,"Internet Security Architecture," in ComputerNetworks&ISDNSystemsJournal, vol. 31,pp.787-804, April1999

[5] Sotillo, S., East Carolina University, "IPv6 security issues," August 2006,www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf.

[6] AndressJ.,"IPv6:thenextinternetprotocol,"April2005,www.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf.

[7] Warfield M., "Security Implications of IPv6," Internet Security SystemsWhitePaper,documents.iss.net/whitepapers/IPv6.pdf

[8] Adeyinka, O., "Internet Attack Methods and Internet Security Technology,"Modeling&Simulation,2008.AICMS08.SecondAsiaInternationalConferenceon,vol.,no.,pp.77-82,13-15May2008

[9] Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3,no.6,pp.68-72,Nov.-Dec.2005