NetworkSecurity:History,Importance,andFuture

[1]**SAGAR KUMAR BEBARTA,** *Gandhi Institute of Excellent Technocrats, Bhubaneswar, India*

[2]**RASMI RANJAN BALIARSINGH,** *Maharaja Institute of Technology,Bhubaneswar, Odisha, India*

ABSTRACT

Network security has become more important topersonalcomputerusers,organizations,andthemilitary. With the advent of the internet, securitybecame a major concern and the history of securityallows a better understanding of the emergence ofsecuritytechnology.Theinternetstructureitselfallowedformanysecuritythreatstooccur.Thearchitectureofthe internet,whenmodifiedcanreduce the possible attacks that can be sent acrossthe network. Knowing the attack methods, allowsfortheappropriatesecuritytoemerge.Manybusinesses secure themselves from the internet bymeansoffirewallsandencryptionmechanisms.Thebusinessescreatean"intranet"toremainconnectedtotheinternetbutsecuredfrompossiblethreats.

The entire field of network security is vast and in anevolutionarystage.Therangeofstudyencompassesabriefhistorydatingbacktointernet's beginnings and the current developmentinnetworksecurity.Inordertounderstandtheresearchbeingperformedtoday,backgroundknowledge of the internet, its vulnerabilities, attackmethodsthroughtheinternet,andsecuritytechnologyisimportantandthereforetheyarereviewed.

INTRODUCTION

The world is becoming more interconnected withtheadventoftheInternetandnewnetworkingtechnology. There is a large amount of personal,commercial, military, and government informationon networking infrastructures worldwide. Networksecurityisbecomingofgreatimportancebecause of intellectual property that can be easily acquiredthroughtheinternet.

Therearecurrentlytwofundamentallydifferentnetworks, data networks and synchronous networkcomprised of switches. The internet is considered adatanetwork.Sincethecurrentdatanetworkconsistsofcomputer-basedrouters,informationcanbeobtainedbyspecialprograms,suchas"Trojanhorses,"plantedintherouters.Thesynchronousnetworkthatconsistsofswitchesdoesnotbufferdataandthereforearenotthreatenedbyattackers.Thatiswhysecurityisemphasized in data networks, such as the internet,andothernetworksthatlink tothe internet.

The vast topic of network security is analyzed byresearchingthe following:

1. Historyofsecurityinnetworks
2. Internet architecture and vulnerablesecurityaspectsofthe Internet
3. Typesofinternetattacksandsecuritymethods
4. Securityfornetworkswithinternetaccess
5. Currentdevelopmentinnetworksecurityhardwareandsoftware

Basedonthisresearch,thefutureofnetworksecurityisforecasted.Newtrendsthatareemergingwillalsobeconsideredtounderstandwherenetwork securityisheading.

1. NetworkSecurity

System and network technology is a key technologyforawidevarietyofapplications.Securityiscrucial

to networksand applications. Although, networksecurityisacriticalrequirementinemergingnetworks,thereisasignificantlackofsecuritymethodsthatcanbeeasilyimplemented.

There exists a "communication gap" between thedevelopers of security technology and developersof networks. Network design is a well-developedprocessthatisbasedontheOpenSystems Interface (OSI) model. The OSI model has severaladvantageswhendesigningnetworks.Itoffersmodularity,flexibility,ease-of-use,andstandardizationofprotocols.Theprotocolsofdifferent layers can be easily combined to createstackswhichallowmodulardevelopment.Theimplementation of individual layers can be changedlater without making other adjustments, allowingflexibility in development. In contrast to networkdesign,securenetworkdesignisnotawell-developed process. There isn't a methodology tomanage the complexity of security requirements.Secure network design does not contain the sameadvantagesasnetwork design.

Whenconsideringnetworksecurity,itmustbeemphasizedthatthewholenetworkissecure.Networksecuritydoesnotonlyconcernthesecurityinthecomputersateachendofthecommunication chain. When transmitting data thecommunicationchannelshouldnotbevulnerabletoattack.Apossiblehackercouldtargetthecommunication channel, obtain the data, decrypt itand re-insert a false message. Securing the networkis just as important as securing the computers andencryptingthe message.

When developing a secure network, the followingneedtobe considered [1]:

1. Access – authorized users are provided themeanstocommunicatetoandfromaparticularnetwork
2. Confidentiality – Information in the networkremainsprivate
3. Authentication– Ensuretheusersofthenetworkarewhothey say theyare
4. Integrity– Ensurethemessagehasnotbeenmodifiedintransit
5. Non-repudiation– Ensuretheuserdoesnotrefutethatheusedthe network

Aneffectivenetworksecurityplanisdevelopedwith the understanding of security issues, potentialattackers, needed level of security, and factors thatmake a network vulnerable to attack [1]. The stepsinvolvedinunderstandingthecompositionofasecure network, internet or otherwise, is followedthroughoutthisresearchendeavor.

To lessen the vulnerability of the computer to thenetwork there are many products available. Thesetools are encryption, authentication mechanisms,intrusion-detection,securitymanagement andfirewalls.Businessesthroughouttheworldareusinga combinationofsomeofthesetools."Intranets" are both connected to the internet andreasonablyprotectedfromit.Theinternetarchitectureitselfleadstovulnerabilitiesinthenetwork. Understanding the security issues of theinternet greatly assists in developing new securitytechnologiesandapproachesfornetworkswithinternetaccessandinternetsecurityitself.

The types of attacks through the internet need toalsobestudiedtobeabletodetectandguardagainstthem.Intrusiondetectionsystemsareestablishedbasedonthetypesofattacksmostcommonlyused.Networkintrusions consistofpackets that are introduced to cause problems forthefollowingreasons:

- Toconsumeresourcesuselessly
- Tointerferewithanysystemresource'sintendedfunction
- Togainsystemknowledgethatcanbeexploitedinlater attacks

Thelastreasonforanetworkintrusionismostcommonly guarded against and considered by mostastheonlyintrusionmotive.Theotherreasonsmentionedneedtobe thwartedaswell.

Typical security currently exists on the computersconnectedtothenetwork.Securityprotocolss ometimesusuallyappearaspartofasinglelayerof the OSI network reference model. Current workis being performed in using a layered approach tosecure network design. The layers of the securitymodelcorrespondtotheOSImodellayers.Thisse curityapproachleadstoaneffectiveandefficientdesignw hichcircumventssomeofthecommonsecurity problems.

2. Differentiating Data Security andNetworkSecurity

Data security is the aspect of security that allows aclient's data to be transformed into unintelligibledatafortransmission.Evenifthisunintellig ibledata is intercepted, a key is needed to decode themessage. This method of security is effective to acertain degree. Strong cryptography in the past canbeeasilybrokentoday.Cryptographicmethodshavet ocontinuetoadvanceduetotheadvancementofthe hackersaswell.

When transferring ciphertext over a network, it ishelpful to have a secure network. This will allow fortheciphertexttobeprotected,sothatitislesslikelyform anypeopletoevenattempttobreakthecode.Asecurenetw orkwillalsopreventsomeonefrominsertingunauthorize dmessagesintothenetwork.Therefore,hardciphersaren eededaswellasattack-hardnetworks[2].

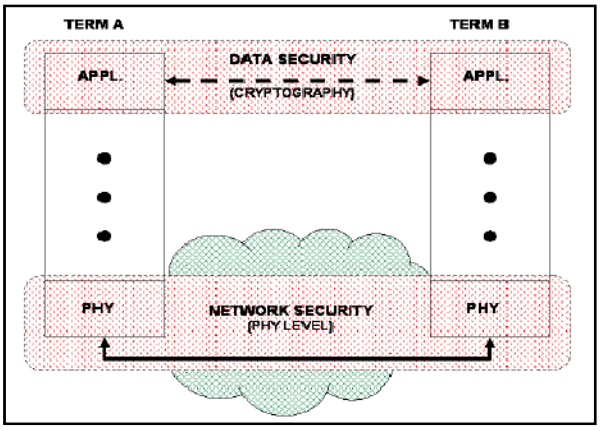

Figure 1: Based on the OSI model, data security and networksecurityhaveadifferentsecurityfunction[2].

Therelationshipofnetworksecurityanddatasecuritytoth eOSImodelisshowninFigure1.Itcan be seen that the cryptography occurs at theapplication layer; therefore the application writersare aware of its existence. The user can possiblychoosedifferentmethodsofdatasecurity.Netw orksecurityismostlycontainedwithinthephysical layer. Layers above the physical layer arealsousedtoaccomplishthenetworksecurityrequired[2].Authenticationisperformedonalayer above the physical layer. Network security inthe physical layer requires failure detection, attackdetectionmechanisms,andintelligentcountermea surestrategies[2].

HISTORYOFNETWORKSECURITY

Recent interest in security was fueled by the crimecommittedbyKevinMitnick.KevinMitnickcom mittedthelargestcomputer-relatedcrimein U.S.history[3].Thelosseswereeightymilliondollars in U.S. intellectual property and source codefromavarietyofcompanies[3].Sincethen,informati onsecuritycameintothespotlight.

Public networks are being relied upon to deliverfinancialandpersonalinformation.Duetotheevol utionofinformationthatismadeavailablethrough the internet, information security is alsorequired to evolve. Due to Kevin Mitnick's offense,companiesareemphasizingsecurityfortheintell ectual property. Internet has been a drivingforcefor data securityimprovement.

Internet protocols in the past were not developedtosecurethemselves.WiththeTCP/IPcom municationstack,securityprotocolsarenotimplemented .Thisleavestheinternetopentoattacks.Moderndevelop mentsintheinternetarchitecturehavemadecommunicati onmoresecure.

1. BriefHistoryofInternet

The birth of the interne takes place in 1969 whenAdvancedResearchProjectsAgencyNetwork(ARPANet) is commissioned by the department ofdefense(DOD)forresearchinnetworking.

The ARPANET is a success from the very beginning.Although originally designed to allow scientists toshare data and access remote computers, e-mailquickly becomes the most popular application. TheARPANET becomes a high-speed digital post officeas people use it to collaborate on research projectsanddiscusstopicsofvariousinterests.TheInterNetworking Working Group becomes the firstof several standards-setting entities to govern thegrowing network [10]. Vinton Cerf is elected thefirstchairmanoftheINWG,andlaterbecomesknownasa"FatheroftheInternet."[10]

In the 1980s, Bob Kahn and Vinton Cerf are keymembersofateamthatcreateTCP/IP,thecommon languageofallInternet computers. ForthefirsttimetheloosecollectionofnetworkswhichmadeuptheARPANETisseenasan"Internet", and the Internet as we know it today isborn. The mid-80s marks a boom in the personalcomputer and super-minicomputer industries. Thecombination of inexpensive desktop machines andpowerful,network-readyserversallowsmanycompanies to join the Internet for the first time.CorporationsbegintousetheInternettocommunicatewitheachotherandwiththeircustomers.

Inthe1990s,theinternetbegantobecomeavailable to the public. The World Wide Web wasborn.NetscapeandMicrosoftwerebothcompetingondevelopingabrowserfortheinternet.Internetcontinues togrowandsurfingthe internet has become equivalent to TV viewingformany users.

2. SecurityTimeline

Severalkeyeventscontributedtothebirthandevolution of computer and network security. Thetimelinecanbe startedasfar backasthe1930s.

Polish cryptographers created an enigma machinein1918thatconvertedplainmessagestoencryptedtext.In1930,AlanTuring,abrilliantmathematicianbrokethecodefortheEnigma.Securingcommunicationswasessentialin WorldWarII.

Inthe1960s,theterm“hacker”iscoinedbyacoupleofMassachusettsInstituteofTechnology(MIT) students. The Department of Defense beganthe ARPANet, which gains popularity as a conduitfortheelectronicexchangeofdataandinformation [3]. This paves the way for the creationof the carrier network known today as the Internet.Duringthe1970s,theTelnetprotocolwasdeveloped. This opened the door for public use ofdatanetworksthatwereoriginallyrestrictedtogovernment contractors and academic researchers[3].

During the 1980s, thehackers and crimes relatingto computers were beginning to emerge. The 414gangareraidedbyauthoritiesafteranine-daycrackingspreewheretheybreakintotop-secretsystems.TheComputerFraudandAbuseActof1986 was created because of Ian Murphy’s crime ofstealinginformationfrommilitarycomputers.Agraduate student, Robert Morris, was convicted forunleashingtheMorrisWormtoover6,000vulnerablecomputersconnectedtotheInternet.Based on concerns that the Morris Worm ordealcouldbereplicated,theComputerEmergencyResponseTeam(CERT)wascreatedtoalertcomputerusersofnetwork securityissues.

Inthe1990s,Internetbecamepublicandthesecurityconcernsincreasedtremendously.Approximately 950 million people use the internettodayworldwide[3].Onanyday,thereareapproximately225majorincidencesofasecurity

breach[3].Thesesecuritybreachescouldalsoresultinmonetarylossesofalargedegree.Investment in proper security should be a priorityforlargeorganizationsaswellascommonusers.

INTERNET ARCHITECTURE ANDVULNERABLESECURITYASPECTS

Fear of security breaches on the Internet is causingorganizations to use protected private networks orintranets [4]. The Internet Engineering Task Force(IETF)hasintroducedsecuritymechanismsatvariouslayersoftheInternetProtocolSuite[4].Thesesecuritymechanismsallowforthelogicalprotection of data units that are transferred acrossthenetwork.

The security architecture of the internet protocol,knownasIPSecurity,isastandardizationofinternet security. IP security, IPsec, covers the newgenerationofIP(IPv6)aswellasthecurrentversion (IPv4). Although new techniques, such asIPsec, have been developed to overcome internet'sbest-knowndeficiencies,theyseemtobeinsufficient[5].Figure2showsavisualrepresentationofhowIPsecisimplementedtoprovidesecure communications.

IPSecisapoint-to-pointprotocol,onesideencrypts, the other decrypts and both sides sharekeyorkeys.IPSeccanbeusedintwomodes,namelytransport mode andtunnelmodes.

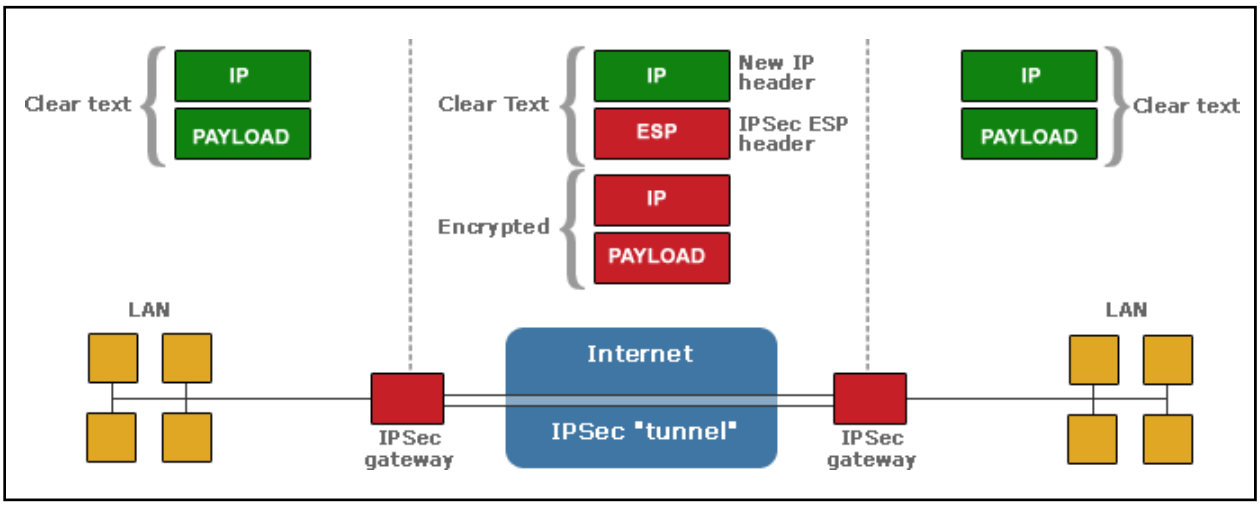

Figure 2:IPseccontainsagatewayandatunnelinordertosecurecommunications.[17]

ThecurrentversionandnewversionoftheInternetProtocolareanalyzedtodeterminethesecurity implications. Although security may existwithintheprotocol,certainattackscannotbeguardedagainst.Theseattacksareanalyzedtodetermine other security mechanisms that may benecessary.

1. IPv4andIPv6Architectures

IPv4wasdesignin1980toreplacetheNCPprotocol on the ARPANET. The IPv4 displayed manylimitations after two decades [6]. The IPv6 protocolwasdesignedwithIPv4'sshortcomingsinmind. IPv6isnotasupersetoftheIPv4protocol;insteaditisanew design.

The internet protocol's design is so vast and cannotbe covered fully. The main parts of the architecturerelatingtosecurityarediscussedindetail.

1.1 IPv4Architecture

Theprotocolcontainsacoupleaspectswhichcaused problems with its use. These problems donot all relate to security. They are mentioned togainacomprehensiveunderstandingoftheinternet protocol and its shortcomings.The causesofproblemswiththeprotocol are:

1. AddressSpace
2. Routing
3. Configuration
4. Security
5. QualityofService

The IPv4 architecture has an address that is 32 bitswide[6].Thislimitsthemaximumnumberofcomputers that can be connected to the internet.The 32 bit address provides for a maximum of twobillions computers to be connected to the internet.Theproblemofexceedingthatnumberwasnotforeseen when the protocol was created. The smalladdress space of the IPv4 facilitates malicious codedistribution[5].

Routing is a problem for this protocol because therouting tables are constantly increasing in size. Themaximumtheoreticalsizeoftheglobalroutingtables was 2.1 millionentries [6]. Methods havebeen adopted to reduce the number of entries inthe routing table. This is helpful for a short periodof time, but drastic change needs to be made toaddressthisproblem.

The TCP/IP-based networking of IPv4 requires thatthe user supplies some data in order to configure anetwork.SomeoftheinformationrequiredistheIP address, routing gateway address, subnet mask,and DNS server. The simplicity of configuring thenetwork is not evident in the IPv4 protocol. Theusercanrequestappropriatenetworkconfigurationfromacentralserver[6].Thiseases configurationhasslesfortheuserbutnotthenetwork'sadministrators.

ThelackofembeddedsecuritywithintheIPv4protocol has led to the many attacks seen today.Mechanisms to secure IPv4 do exist, but there areno requirements for their use [6]. IPsec is a specificmechanismusedtosecuretheprotocol.IPsecsecuresthepacketpayloadsbymeansofcryptography.IPsecprovidestheservicesofconfidentiality,integrity,andauthentication[6].This form of protection does not account for theskilledhackerwhomaybeabletobreaktheencryption methodandobtainthe key.

When internet was created, the quality of service(QoS)wasstandardizedaccordingtotheinformationthatwastransferredacrossthenetwork. The original transfer of information wasmostly text-based. As the internet expanded andtechnology evolved, other forms of communicationbegan to be transmitted across the internet. Thequality of service for streaming videos and musicaremuchdifferentthanthestandardtext.Theprotocoldoesnothavethefunctionalityofdynamic QoS that changes based on the type ofdatabeingcommunicated[6].

1.2 IPv6Architecture

WhenIPv6wasbeingdeveloped,emphasiswasplaced on aspects of the IPv4 protocol that neededtobeimproved.Thedevelopmenteffortswereplacedinthe followingareas:

1. Routingandaddressing
2. Multi-protocolarchitecture
3. Securityarchitecture
4. Trafficcontrol

The IPv6 protocol's address space was extended bysupporting128bitaddresses.With128bitaddresses,theprotocolcansupportupto
3.4 * (10)^38 machines. The address bits are usedless efficiently in this protocol because it simplifiesaddressingconfiguration.

TheIPv6routingsystemismoreefficientandenablessmallerglobalroutingtables.Thehostconfigurationisalsosimplified.Hostscanautomaticallyconfigurethemselves.Thisnewdesign allows ease of configuration for the user aswellasnetwork administrator.

The security architecture of the IPv6 protocol is ofgreat interest. IPsec is embedded within the IPv6protocol. IPsec functionality is the same for IPv4and IPv6. The only difference is that IPv6 can utilizethesecuritymechanismalongtheentireroute[6].

The quality of service problem is handled with IPv6.The internet protocol allows for special handling ofcertainpacketswithahigherqualityofservice.

From a high-level view, the major benefits of IPv6are its scalability and increased security. IPv6 alsooffers other interesting features that are beyondthescope ofthispaper.

It must be emphasized that after researching IPv6and its security features, it is not necessarily moresecure than IPv4. The approach to security is onlyslightlybetter,notaradicalimprovement.

2. AttacksthroughtheCurrentInternet ProtocolIPv4

There are four main computer security attributes.They were mentioned before in a slightly differentform,butarerestatedforconvenienceandemphasis.Thesesecurityattributesareconfidentiality,integrity,privacy,andavailability.

Confidentiality and integrity still hold to the samedefinition. Availability means the computer assetscan be accessed by authorized people [8]. Privacy isthe right to protect personal secrets [8]. Variousattackmethodsrelatetothesefoursecurityattributes. Table 1 shows the attack methods andsolutions.

Table1:AttackMethodsandSecurityTechnology[8]

Computer Security attributes	Attack Methods	Technology for Internet Security
Confidentiality	Eavesdropping, HIacking, Phishing, DoS and IP Spoofing	IDS, Firewall, Cryptographic Systems, IPSec and SSL
Integrity	Viruses, Worms, Trojans, Eavesdropping, DoS and IP Spoofing.	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Privacy	Email bombing, Spamming, Hacking, DoS and Cookies	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Availability	DoS, Email bombing, Spamming and Systems Boot Record Infectors	IDS, Anti-Malware Software and Firewall.

Commonattackmethodsandthesecuritytechnology will be briefly discussed. Not all of themethodsinthetableabovearediscussed.Thecurrenttechnologyfordealingwithattacksisunderstoodinordertocomprehendthecurrentresearchdevelopmentsinsecurityhardwareandsoftware.

2.1 CommonInternetAttackMethods

Commoninternetattacksmethodsarebrokendownintocategories.Someattacksgainsystemknowledgeorpersonalinformation,suchaseavesdroppingandphishing.Attackscanalsointerfere with the system's intended function, suchas viruses, worms and trojans. The other form ofattackiswhenthesystem'sresourcesareconsumes uselessly, these can be caused by denialofservice(DoS)attack.Otherformsofnetworkintrusionsalsoexist,suchaslandattacks,smurfattacks,andteardropattacks.TheseattacksarenotaswellknownasDoS attacks,buttheyareused in some form or another even if they aren'tmentionedby name.

2.1.1 Eavesdropping

Interceptionofcommunicationsbyanunauthorized party is called eavesdropping. Passiveeavesdroppingiswhenthepersononlysecretlylistens to the networked messages. On the otherhand,activeeavesdropping is when theintruderlistensandinsertssomethingintothecommunicationstream.Thiscanleadtothemessagesbeingdistorted.Sensitiveinformationcanbe stolenthisway [8].

2.1.2 Viruses

Viruses are self-replication programs that use filesto infect and propagate [8]. Once a file is opened,theviruswillactivatewithinthe system.

2.1.3 Worms

A worm is similar to a virus because they both areself-replicating, but the worm does not require afile to allow it to propagate [8]. There are two maintypes of worms, mass-mailing worms and network-aware worms. Mass mailing worms use email as ameans to infect other computers. Network-awarewormsareamajorproblemfortheInternet.Anetwork-aware worm selects a target and once theworm accesses the target host, it can infect it bymeansofaTrojanor otherwise.

2.1.4 Trojans

Trojans appear to be benign programs to the user,butwillactuallyhavesomemaliciouspurpose.Trojans usually carry some payload such as a virus[8].

2.1.5 Phishing

Phishingisanattempttoobtainconfidentialinformationfromanindividual,group,ororganization[9].Phisherstrickusersintodisclosing personal data, such as credit card numbers, onlinebankingcredentials,andothersensitiveinformation.

2.1.6 IPSpoofingAttacks

Spoofingmeanstohavetheaddressofthecomputer mirror the address of a trusted computerinordertogainaccesstoothercomputers.Theidentityoftheintruderishiddenbydifferentmeans making detection and prevention difficult.WiththecurrentIPprotocoltechnology,IP-spoofedpackets cannotbe eliminated[8].

2.1.7 DenialofService

DenialofServiceisanattackwhenthesystemreceivingtoomanyrequestscannotreturncommunicationwiththerequestors[9].Thesystemthenconsumesresources waitingforthehandshaketocomplete.Eventually,thesystemcannot respond to any more requests rendering itwithoutservice.

2.2 TechnologyforInternetSecurity

Internet threats will continue to be a major issue intheglobalworldaslongasinformationisaccessibleandtransferredacrosstheInternet.Different defense and detection mechanisms weredevelopedtodeal withthese attacks.

2.2.1 Cryptographicsystems

Cryptography is a useful and widely used tool insecurity engineering today. It involved the use ofcodesandcipherstotransforminformationintounintelligibledata.

2.2.2 Firewall

A firewall is a typical border control mechanism orperimeter defense. The purpose of a firewall is toblocktrafficfromtheoutside,butitcouldalsobe

used to block traffic from theinside. A firewall isthefrontlinedefensemechanismagainstintruders.Itisa systemdesignedtopreventunauthorized access to or from a private network.Firewallscanbeimplementedinbothhardware andsoftware, or acombinationofboth[8].

2.2.3 IntrusionDetectionSystems

An Intrusion Detection System (IDS) is an additionalprotection measure that helps ward off computerintrusions.IDSsystemscanbesoftwareandhar dwaredevicesusedtodetectanattack.IDSproductsareus edtomonitorconnectionindeterminingwhetherattacksa rebeenlaunched.SomeIDSsystemsjustmonitorandalert ofanattack,whereasotherstry toblockthe attack.

2.2.4 Anti-MalwareSoftwareandscanners

Viruses, worms and Trojan horses are all examplesof malicious software, or Malware for short. Specialso-calledanti-Malwaretoolsareusedtodetectthe mandcure aninfectedsystem.

2.2.5 SecureSocketLayer(SSL)

The Secure Socket Layer (SSL) is a suite of protocolsthat is a standard way to achieve a good level ofsecurity between a web browser and a website. SSLis designed to create a secure channel, or tunnel,betweenawebbrowserandthewebserver,sothat any information exchanged is protected withinthe secured tunnel. SSL provides authentication ofclientstoserverthroughtheuseofcertificates.Clients present a certificate to the server to provetheiridentity.

3. SecurityIssuesofIPProtocolIPv6

From a security point of view, IPv6 is a considerableadvancementovertheIPv4internetprotoco l.DespitetheIPv6'sgreatsecuritymechanisms,itstillcon tinuestobevulnerabletothreats.Some areasoftheIPv6protocolstillposeapotentialsecurityissu e.

The new internet protocol does not protect againstmisconfiguredservers,poorlydesignedapplicati ons,or poorly protected sites.

The possible security problems emerge due to thefollowing[5]:

1. Headermanipulationissues
2. Floodingissues
3. Mobilityissues

Header manipulation issues arise due to the IPsec'sembeddedfunctionality[7].Extensionheadersd eter some common sources of attacks because ofheadermanipulation.Theproblemisthatextensionhea dersneedtobeprocessedbyallstacks,andthiscanleadtoal ongchainofextension headers. The large number of extensionheaderscanoverwhelmacertainnodeandisafo rm of attack if it is deliberate. Spoofing continuestobe asecurity threatonIPv6protocol.

A type of attack called port scanning occurs when awholesectionofanetworkisscannedtofindpotentialtar getswithopenservices[5].Theaddress space of the IPv6 protocol is large but theprotocolisstillnotinvulnerabletothistypeofattack.

Mobility is a new feature that is incorporated intotheinternetprotocolIPv6.Thefeaturerequiresspecia l security measures. Network administratorsneedto beawareofthesesecurityneedswhenusingIPv6's mobility feature.

SECURITYINDIFFERENTNETWORKS

The businesses today use combinations of firewalls,encryption,andauthenticationmechanismsto create"intranets"thatareconnectedtotheinternetbutprot ectedfrom itatthe sametime.

Intranet is a private computer network that usesinternetprotocols.Intranetsdifferfrom"Extranets"i nthattheformeraregenerallyrestricted to employees of the organization whileextranets can generally be accessed by customers,suppliers,or otherapprovedparties.

There does not necessarily have to be any accessfromtheorganization'sinternalnetworktotheInte rnet itself. When such access is provided it isusuallythroughagatewaywithafirewall,alongwith user authentication, encryption of messages,and often makes use of virtual privatenetworks(VPNs).

Although intranets can be set up quickly to sharedatainacontrolledenvironment,thatdataisstillatris kunlessthereistightsecurity.Thedisadvantage of a closed intranet is that vital datamight not get into the hands of those who need it.Intranetshaveaplacewithinagencies.Butforbroaderd atasharing,itmightbebettertokeepthenetworks open,withthesesafeguards:

1. Firewallsthatdetectandreportintrusionattempt s
2. Sophisticatedviruscheckingatthefirewall
3. Enforcedrulesforemployeeopeningofe-mailat tachments
4. Encryptionforallconnectionsanddatatransfers
5. Authentication by synchronized, timedpasswordsorsecurity certificates

It was mentioned that if the intranet wanted accessto the internet, virtual private networks are oftenused. Intranets that exist across multiple locationsgenerally run over separate leased lines or a newerapproach of VPN can be utilized. VPN is a privatenetworkthatusesapublicnetwork(usuallytheInte rnet) to connect remote sites or users together.Instead of using a dedicated, real-world connectionsuchasleasedline,aVPNuses"virtual"conne ctions routed through the Internet from thecompany'sprivatenetworktotheremotesiteor employee. Figure 3 is a graphical representation ofanorganization andVPN network.

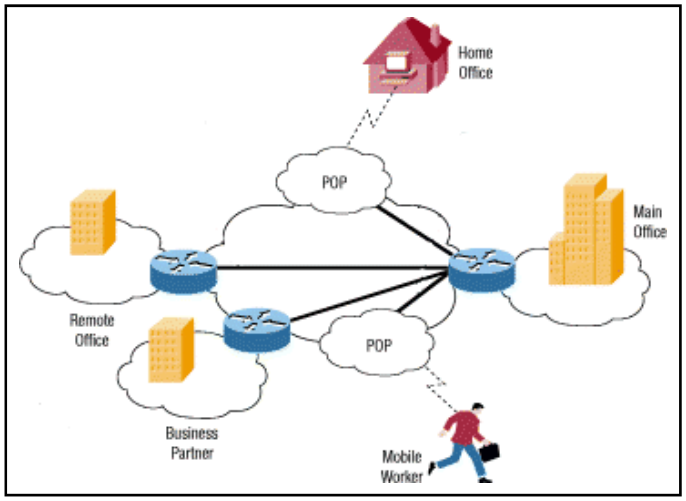

Figure 3: A typical VPN might have a main LAN at the corporateheadquarters of a company, other LANs at remote offices orfacilitiesandindividualusersconnectingfromoutinthefield.[14]

CURRENT DEVELOPMENTS IN NETWORKSECURITY

The network security field is continuing down thesameroute.Thesamemethodologiesarebeingused with the addition of biometric identification.Biometricsprovidesabettermethodofaut hentication than passwords. This might greatlyreduce the unauthorized access of secure systems.New technology such as the smart card is surfacinginresearchonnetworksecurity.Thesoftwareas pectofnetworksecurityisverydynamic.Constantly new firewalls and encryption schemesarebeingimplemented.

Theresearchbeingperformedassistsinunderstanding current development and projectingthefuture developmentsofthe field.

1. HardwareDevelopments

Hardwaredevelopmentsarenotdevelopingrapidly. Biometric systems and smart cards are theonlynewhardwaretechnologiesthatarewidelyimpac ting security.

The most obvious use of biometrics for networksecurityisforsecureworkstationlogonsforaworkstationconnectedtoanetwork.Eachworkstationrequiressomesoftwaresupportforbiometricidentificationoftheuseraswellas,dependingonthebiometricbeingused,somehardware device. The cost of hardware devices isone thing that may lead to the widespread use ofvoicebiometricsecurityidentification,especiallyamongcompaniesandorganizationsonalowbudget.
Hardware device such as computer micewith built in thumbprint readers would be the nextstep up. These devices would be more expensive toimplement on several computers, as each machinewouldrequireitsownhardwaredevice.Abiometric mouse, with the software to support it, isavailablefromaround$120intheU.S.Theadvantage of voice recognition software is that itcanbecentralized,thusreducingthecostofimplementation per machine. At top of the range acentralizedvoicebiometricpackagecancostupto $50,000 but may be able to manage the secure log-inofupto5000machines.

The main use of Biometric network security will betoreplacethecurrentpasswordsystem.Maintaining password security can be a major taskfor even asmall organization. Passwords havetobe changed every few months and people forgettheirpasswordorlockthemselvesoutofthesystem byincorrectlyenteringtheirpasswordrepeatedly. Very often people write their passworddown and keep it near their computer. This is ofcoursecompletelyunderminesanyeffortatnetworksecurity.Biometricscanreplacethissecurityidentification method.Theuseofbiometricidentificationstopsthisproblemandwhile it may be expensive to set up at first, thesedevices save on administration and user assistancecosts.

Smart cards are usually a credit-card-sized digitalelectronicmedia.Thecarditselfisdesignedtostore encryptionkeysandotherinformationusedinauthenticationandotheridentificationprocesses.Themainideabehindsmartcardsisto provide undeniable proof of a user's identity. Smartcards can be used for everything from logging in tothenetworktoprovidingsecureWebcommunicationsandsecuree-mailtransactions.

Itmayseemthatsmartcardsarenothingmorethan a repository for storing passwords. Obviously,someonecaneasilystealasmartcardfromsomeoneelse.Fortunately,therearesafetyfeatures built into smart cards to prevent someonefromusingastolencard.Smartcardsrequireanyonewhoisusingthemtoenterapersonalidentificationnumber(PIN)beforethey'llbegranted any levelof access into thesystem. ThePINissimilar tothePIN usedbyATMmachines.

When a user inserts the smart card into the cardreader, the smart card prompts the user for a PIN.ThisPINwasassignedtotheuserbytheadministrator at the time the administrator issuedthe card to the user. Because the PIN is short andpurely numeric, the user should have no troubleremembering it and therefore would be unlikely towritethe PINdown.

But the interesting thing is what happens when theuser inputs the PIN. The PIN is verified from insidethesmartcard.BecausethePINisnevertransmitted across the network, there's absolutelynodangerofitbeingintercepted.Themainbenefit, though, is that the PIN is useless withoutthesmartcard,andthesmartcardisuselesswithoutthe PIN.

There are other security issues of the smart card.Thesmartcardiscost-effectivebutnotassecureasthe biometric identificationdevices.

2. SoftwareDevelopments

Thesoftwareaspectofnetworksecurityisveryvast. It includes firewalls, antivirus, vpn, intrusiondetection,andmuchmore.Theresearchdevelopment of all security software is not feasibletostudyatthispoint.Thegoalistoobtainaview

of where the security software is heading based onemphasisbeingplacednow.

Theimprovementofthestandardsecuritysoftware still remains the same. When new virusesemerge,theantivirusisupdatedtobeabletoguarda gainstthosethreats.Thisprocessisthesame for firewalls and intrusion detection systems.Manyresearchpapersthathavebeenskimmedw ere based on analyzing attack patterns in order tocreatesmarter securitysoftware.

As the security hardware transitions to biometrics,thesoftwarealsoneedstobeabletousetheinfo rmationappropriately.Currentresearchisbeing performed on security software using neuralnetworks. The objective of the research is to useneuralnetworksforthefacialrecognitionsoftware.

Many small and complex devices can be connectedtotheinternet.Mostofthecurrentsecurityalgo rithms are computational intensive and requiresubstantialprocessingpower.Thispower,howev er,isnotavailableinsmalldeviceslikesensors. Therefore, there is a need for designinglight-weightsecurityalgorithms.Researchint hisareaiscurrently beingperformed.

FUTURETRENDSINSECURITY

What is going to drive the Internet security is theset of applications more than anything else. Thefuture will possibly be that the security is similar toan immune system. The immune system fights offattacks and builds itself to fight tougher enemies.Similarly,thenetworksecuritywillbeabletofun ctionas animmunesystem.

Thetrendtowardsbiometricscouldhavetakenplace a while ago, but it seems that it isn't beingactively pursued. Many security developments thatare taking place are within the same set of securitytechnologythatisbeingusedtodaywithsomemin oradjustments.

CONCLUSION

Networksecurityisanimportantfieldthatisincreasingly gainingattentionastheinternetexpands. The security threats and internet protocolwere analyzed to determine the necessary securitytechnology.Thesecuritytechnologyismostlyso ftwarebased,butmanycommonhardwaredevicesareuse d.Thecurrentdevelopmentinnetworksecurityisnotvery impressive.

Originally it was assumed that with the importanceof the network security field, new approaches tosecurity,bothhardwareandsoftware,wouldbeactively researched. It was a surprise to see most ofthedevelopmenttakingplaceinthesametechnologies being currently used. The embeddedsecurityofthenewinternetprotocolIPv6mayp rovide many benefits to internet users. Althoughsomesecurityissueswereobserved,theIPv6int ernetprotocolseemstoevademanyofthecurrent popular attacks. Combined use of IPv6 andsecurity tools such as firewalls, intrusion detection,and authentication mechanisms will prove effectiveinguardingintellectualpropertyforthenearfutu re.Thenetworksecurityfieldmayhavetoevolve more rapidly to deal with the threats furtherinthe future.

REFERENCES

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

[2] Kartalopoulos, S. V., "Differentiating Data Securityand Network Security," *Communications, 2008. ICC '08.IEEE International Conference on*, pp.1469-1473, 19-23May2008

[3] "SecurityOverview,"www.redhat.com/docs/manu als/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.

[4] Molva, R., InstitutEurecom,"Internet SecurityArchitecture,"in*ComputerNetworks&ISDNSys temsJournal*,vol.31,pp.787-804,April1999

[5] Sotillo, S., East Carolina University, "IPv6 securityissues," August 2006,www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf.
[6] Andress J., "IPv6: the next internet protocol," April2005, www.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf.
[7] Warfield M., "Security Implications of IPv6," *InternetSecurity Systems White Paper*,documents.iss.net/whitepapers/IPv6.pdf
[8] Adeyinka, O., "Internet Attack Methods and InternetSecurity Technology," *Modeling & Simulation, 2008.AICMS 08. Second Asia International Conference on*,vol.,no., pp.77-82,13-15May2008
[9] Marin,G.A.,"Networksecuritybasics,"*Security&Privacy,IEEE*,vol.3,no.6,pp.68-72,Nov.-Dec.2005
[10] "Internet History Timeline,"www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.htm.
[11] Landwehr,C.E.;Goldschlag,D.M.,"Securityissuesin networks with Internet access," *Proceedings of theIEEE*,vol.85, no.12, pp.2034-2051,Dec1997
[12] "Intranet." *Wikipedia, The Free Encyclopedia*. 23Jun 2008, 10:43 UTC. Wikimedia Foundation, Inc. 2 Jul2008 <http://en.wikipedia.org/w/index.php?title=Intranet&oldid=221174244>.
[13] "Virtual private network." *Wikipedia, The FreeEncyclopedia*. 30 Jun 2008, 19:32 UTC. WikimediaFoundation,Inc. 2Jul2008 <http://en.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=222715612>.
[14] Tyson, J., "How Virtual private networks work,"http://www.howstuffworks.com/vpn.htm.
[15] Al-Salqan, Y.Y., "Future trends in Internet security,"*Distributed Computing Systems, 1997., Proceedings ofthe Sixth IEEE Computer Society Workshop on FutureTrendsof*, vol.,no.,pp.216-217,29-31Oct1997
[16] Curtin, M. "Introduction to Network Security,"http://www.interhack.net/pubs/network-security.
[17] "Improving Security,"http://www.cert.org/tech_tips,2006.
[18] Serpanos, D.N.; Voyiatzis, A.G., "Secure networkdesign:Alayeredapproach,"*AutonomousDecentralizedSystem, 2002. The 2nd International Workshop on*, vol.,no.,pp. 95-100,6-7Nov.2002
[19] Ohta, T.; Chikaraishi, T., "Network security model,"*Networks, 1993. International Conference onInformation Engineering '93. 'Communications andNetworks for the Year 2000', Proceedings of IEEESingapore International Conference on* , vol.2, no.,pp.507-511vol.2,6-11Sep1993