ISSN (e): **2250 – 3005** || *Volume, 07* || *Issue, 05*|| *May – 2017* ||
International Journal of Computational Engineering Research (IJCER)

Review of Computer Network Security System

[1]sujit Kumar, [2]rasmiprava Biswal
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India
Indus College of Engineering, Bhubaneswar, Odisha, India

ABSTRACT
Network security has become more important to personal computer users, organizations, and the military.
Withtheadventoftheinternet,securitybecameamajorconcernandthehistoryofsecurityallowsabetterun derstanding of the emergence of security technology. The internet structure itself allowed for many securitythreats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sentacross the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businessessecure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an"intranet" to remain connected to the internet but secured from possible threats. The entire field of networksecurity is vast and in an evolutionary stage. The range of study encompasses a brief history dating back tointernet's beginnings and the current development in network security. In order to understand the research beingperformed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet,and securitytechnologyisimportantandtherefore theyare reviewed.
Keywords: Mitigation,Cryptography,Network,Security

1.0 PREAMBLE

The world is becoming more interconnected with the advent of the Internet and new networking technology.Thereisalargeamountofpersonal,commercial,military,andgovernmentinformationonnetworkinginfrast ructuresworldwide. Network security is becoming of great importance because of intellectual propertythatcanbe easilyacquiredthroughthe internet.
There are currently two fundamentally different networks, data networks and synchronous networkcomprised of switches. The internet is considered a data network. Since the current data network consists ofcomputer basedrouters, information can be obtainedby special programs, such as"Trojan horses," plantedinthe routers. The synchronous network that consists of switches does not buffer data and therefore are notthreatened by attackers. That is why security is emphasized in data networks, such as the internet, and othernetworksthatlinktotheinternet.Thevasttopicofnetworksecurityisanalyzedbyresearchingthefollowing:

1. Historyof securityinnetworks
2. InternetarchitectureandvulnerablesecurityaspectsoftheInternet
3. Typesofinternetattacksandsecuritymethods
4. Securityfornetworkswithinternetaccess
5. Currentdevelopmentinnetworksecurityhardwareandsoftware

Basedonthisresearch,thefutureofnetworksecurityisforecasted.Newtrendsthatareemergingwillalso be considered tounderstandwhere networksecurityisheading.

1.1 INTERNETARCHITECTUREANDVULNERABLESECURITYASPECTS

Fear of security breaches on the Internet is causing organizations to use protected private networks or intranets.The Internet Engineering Task Force (IETF) has introduced security mechanisms at various layers of the
InternetProtocolSuite.Thesesecuritymechanismsallowforthelogicalprotectionofdataunitsthataretransferredacross the network. The security architecture of the internet protocol, known as IP Security, is a standardizationof internet security. IP security, IPsec, covers the new generation of IP (IPv6) as well as the current version(IPv4). Although new techniques, such as IPsec, have been developed to overcome internet's bestknowndeficiencies, theyseemtobeinsufficient.

1.2 IPv4andIPv6Architectures

IPv4 was design in 1980 to replace the NCP protocol on the ARPANET. The IPv4 displayed many limitationsaftertwodecades.TheIPv6protocolwasdesignedwithIPv4'sshortcomingsinmind.IPv6isnotasupersetofth e IPv4 protocol; instead it is a new design. The internet protocol's design is so vast and cannot be covered fully.Themainpartsofthe architecturerelatingto securityarediscussedindetail.

1.2.1 IPv4Architecture

The protocol contains a couple aspects which caused problems with its use. These problems do not all relate tosecurity.Theyarementionedtogainacomprehensiveunderstandingoftheinternetprotocolanditsshortcomings. The causesofproblemswiththeprotocol are:

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

The IPv4architecture has an address that is32bitswide.This limits themaximumnumberofcomputers that can be connected to the internet. The 32 bit address provides for a maximum of two billionscomputers to be connected to the internet. The problem of exceeding that number was not foreseen when theprotocol was created. The small address space of the IPv4 facilitates malicious code distribution. Routing is aproblem for this protocol because the routing tables are constantly increasing in size. The maximum theoreticalsize of the global routing tables was 2.1 million entries [6]. Methods have been adopted to reduce the number ofentries in the routing table. This is helpful for a short period of time, but drastic change needs to be made toaddressthisproblem.

The TCP/IP based networking of IPv4 requires that the user supplies some data in order to configure anetwork. Some of the information required is the IP address, routing gateway address, subnet mask, and DNSserver. The simplicity of configuring the network is not evident in the IPv4 protocol. The user can requestappropriate network configuration from a central server. This eases configuration hassles for the user but not thenetwork'sadministrators.

ThelackofembeddedsecuritywithintheIPv4protocolhasledtothe manyattacksseentoday.

Mechanisms to secure IPv4 do exist, but there are no requirements for their use. IPsec is a specificmechanism used to secure the protocol. IPsec secures the packet payloads by means of cryptography. IPsecprovidestheservicesofconfidentiality,integrity, andauthentication.

Thisform ofprotectiondoesnotaccountfortheskilledhackerwhomay beabletobreaktheencryption method and obtain the key. When internet was created, the quality of service (QoS) was standardizedaccording to the information that was transferred across the network. The original transfer of information wasmostly text based. As the internet expanded and technology evolved, other forms of communication began to betransmitted across the internet. The quality of service for streaming videos and music are much different than thestandardtext.TheprotocoldoesnothavethefunctionalityofdynamicQoSthatchangesbasedonthetypeofdatabeingc ommunicated.

1.3 AIM ANDOBJECTIVES

Sincetheevolutionof attackis endless,thisthesisgivesan overview of the best practices in reviewingtheknown attacksandrecommendationonhowto prevent reoccurrenceattacks.

The objectives of this work are to reveal and define the concept of attack and threat to computer network, tohighlight different mitigating techniques used to circumvent threats and attacks, to illustrate the procedure toimplement the best security practices, and to extend the practices of an outsider trying to gain access into thenetworktothenetworkengineer.

2.1 REVIEWOFPREVIOUSWORKS

Network attacks have been discovered to be as varied as the system that they attempt to penetrate. Attacks areknown to either be intentional or unintentional and technically competent intruders have been interested intargetingtheprotocolsused forsecurecommunicationbetweennetworkingdevices. (Reed2003).This reviewaddresses howhighlysophisticatedintrudersarepenetratinginternetnetworksdespitehighlevels of security. But as the intruders increase, the network experts are deriving many techniques in preventingattackersfromaccessingcompanynetworks.

2.2 CATEGORIESOFSECURITYTHREATS

Security threat can be categorized into four parts and these categories are theways or forms through whichthreatscanbe carriedout onanetwork.

i. UNSTRUCTUREDTHREATS

Unstructured security threat is the kind of threat created by an inexperienced person trying to gain access to

anetwork. They commonly use common hacking tools, like shell scripts, and password crackers. A good securitysolutionshouldeasilythwartthiskindofattack.Inotherwords,thesekindsofhackerscouldnotbeunderestimated because theycancauseseriousdamage tonetwork.

ii. STRUCTUREDTHREATS

Unlike unstructured threats, structured threat hackers are well experienced and highly sophisticated. They usesophisticated hacking tools to penetrate networks and they can break into government or business computers toextract information. On certain occasions, structured threats are carried out by organized criminal gangs orindustrycompetitors.

iii. EXTERNALTHREATS

Some unauthorized people outside the company who do not have access to the company's computer system ornetwork could cause external threat. They usually break into company's network via the Internet or server. Bothexperienced and inexperiencedhackerscouldposeexternalthreats.

iv. INTERNALTHREATS

This kind of threat could be by a disgruntled employeewho has authorized access to the company's network.Likeexternalthreats,thedamagethatcouldbecausedbysuchahackerdependsontheexpertiseofthe hacker.

2.3 PHYSICALINSTALLATIONATTACK

Physical installation attacks, as the name implies originate from some basic threats that we can see with own eyebutmight not be prevented.

Firstly, hardware threat is a common example of a physical installation attack; this could be due to theold age of a particular system, and as a result of that, it start acting erratically and damage some data before ittotally dies. Environmental threat, as discussed previously, can be caused by natural phenomena, such as extremeweather temperatures, earthquakes, and storms. Furthermore, electrical threat can cause extensive damage to anetwork. This kind of threat is common in countries where the power supply is always interrupted unexpectedly.Examples of this type of threat are: blackout (unexpected interruption of power supply), brownout (insufficientsupply of power voltage) and noise (unconditioned power). Maintenance threat could also cause problem

tonetwork.Examplesofmaintenancethreatsarepoorcabling,poorcablelabelling,electrostaticdischarge,andlackofcriticalspare parts.

2.4 DEVICECOMMUNICATIONATTACK

Technically competent hackers have been able to fashion a structured attack targeted at communication protocols.The OSI model has seven layers that are used for communication between networking devices, which are withvulnerabilitiesthatcanbecontrolled.Basically,higherlayerscannotbesecuredwhilethelowerlayersarealsonot being secured, yet in recent years there has been limited attention to insecurities at the physical layer or datalink layer despite changes in network operational practice that include developments like nation-wide layer twonetworksandnational and regional optical networks.

Currently known threats at lower levels of the OSI stack include ARP spoofing, MITM (man-in-themiddle) attacks at layer two, and physical layer attacks such as passive optical taps or the interception ofwireless network signals by attackers. While these attacks are well known, little research is currently focused onaddressingthose concerns.

3.0 MITIGATIONSOFNETWORKTHREATSAND ATTACKS

Due to the unfortunate case of numerous threats and attacks that have befallen the networking industry, itbecomes imperative tofindways ofmitigating each of the attacks. Chaptertwoabove described the varioustypes of threat facing network security, Chapter three and four discuss the solutions for the threats mentioned inthepreviouschapters.

3.1 HARDWARETHREATMITIGATION

As a result of fault from physical installation, planning of physical security to limit damage or theft of equipmentduring the process of installing hardware is very important. Few of the many ways that this action could bemonitored or controlled is by making sure that no unauthorized access from the doors, ceiling, raised floor,windows, ducts or vents, monitoring and control closet entry with electronic logs, use of security cameras, and ifpossible,electronicaccess control shouldbeusedandsecurity systems shouldlog all entry attempts andcontrolled bysecuritypersonnel.

PhysicalsecurityisdiscussedindetailinChapterfourofthisthesis.

3.2 ENVIRONMENTAL THREATMITIGATION

The first stage of every attack has been from lack of environmental control, which brings about limiting damagebycreatingaproperoperatingenvironmentthrough:Temperaturecontrol,humiditycontrolandpositiveairflow.

3.3 ELECTRICALTHREATMITIGATION

Loss of power can also be an opportunity for intruders to break into a controlled network, which could beprevented or controlled in many ways few of which are mentioned here; Electrical threat could be limited byensuringuninterruptedpowersupplyfornetworkdevices,byfollowingapreventativemaintenanceplandesigned for the purpose, andbyperformingremote alarmingandmonitoring.

3.4 MAINTENANCE-RELATEDTHREATMITIGATION

Maintenance has always been a vital operation, for any organization that uses hardware. Maintenance relatedthreatscanbe limitedby:

- Usingneatcableruns
- Labelingcriticalcablesandcomponents
- Using(electrostaticdischarge)ESDprocedures
- Stockingcriticalspares
- Controllingaccesstoconsole ports

Console should neither be left connected nor logged into any console port, and ensure logging off administrativeinterfaces before leaving. A locked room should not be relied upon as the major protection for devices. No roomis totally secured,andif intruders get in a securedroom,there is nothing stoppingthem from making aconnectiontothe consoleportofa router ora switch.

3.5 PACKETSNIFFERATTACKMITIGATION

Thefollowingarethetoolsthatcanbeusedtocontrolpacketsnifferattacks;

Authentication: For defense against packet sniffers, the use of strong authentication should be the firstmitigation option. Strong authentication is a technique of authenticating users that cannot be circumvented easily.One Time Passwords (OTPs) are a clear example of strong authentication. A onetime password is a securitymechanismthat makesuseofamobiledeviceingeneratingpasswordeachtimeanapplicationrequestsforit.

Switched Infrastructure: This technique counters the use of packet sniffers in a network environment.Forinstance,ifanorganizationdeploysalayer-2switchedEthernet,accessbyintruderscanonlybegainedtothe traffic flow of the connected port. Obviously a switched infrastructure does not totally eradicate the threat ofpacketsniffers, buttheireffectivenessisreducedconsiderably.

Anti-Sniffer Tools: Certainly, there would always be a solution for every threat, anti-sniffer is asoftware and hardware, designed for detection of the use of sniffers on a network, and can be implemented onnetworks.

Cryptography: A communication channel is cryptographically secure when the only data a packetsniffer detects is a cipher text (a random string of bits) and not the original message. Cisco deploys network-levelcryptography based on IP Security (IPsec), IP security is a standard security method for networking devices incommunicatingprivatelythroughthe useofInternet Protocol(IP).(CANS2011)

Secure Sockets Layer (SSL) and Secure Shell Protocol (SSH) are also cryptographic protocols fornetwork management.

Fundamentaltosecurityindistributedsystemsistheuseofcryptographictechniques.Thebasicideaof applying these techniques is simple. Consider a sender S wanting to transmit message m to a receiver R. Toprotect the message against security threats, the sender first **encrypts** it into an unintelligible message m′, andsubsequentlysendsm′toR. R, inturn,must**decrypt** thereceivedmessageintoitsoriginalformm.

3.6 PORTSCANANDPINGSWEEPATTACKMITIGATION

The prevention of port scans and ping sweeps seems to be difficult without compromising network capabilities.However, the use of intrusion prevention systems at network and host levels is an advisable way of mitigatingany damages. Ping sweeps can be stopped if ICMP (internet control message protocol) echo as well as echo-replyare turnedoffonedge routers.

Network-based intrusion prevention systems (IPSs) which compare incoming traffic to signatures intheir databaseand host-based intrusion prevention systems (HIPS) can usually notify an administrator when areconnaissanceattackisunderway.

Discoveringstealthscansrequireskernellevelwork.

3.7 ACCESSATTACKSMITIGATION

Thefollowingaremitigationtechniquesforpasswordattacks:

1) Usersshouldnotbeallowedtousethesamepasswordsonmultiplesystems.
2) Accountsshouldbedisabledafterdetectingacertainamountofunsuccessfulloginattempts.
3) Theuseofordinarytextpasswordsshouldnotbeallowed.
4) Useofstrongpasswords(e.g.,Use"mY8!Rthd8y@"ratherthanmybirthday)

3.8 TRUSTEXPLOITATIONATTACKMITIGATION

Trust exploitation-based attacks can be mitigated by means of tight constraints on the level of trust withinnetworks.Theoutsidesystemsofafirewallshouldnotbefullytrustedbytheinside Systemsofthefirewall,in other words trust should be limited to specific protocols where possible, and should also be validated by anotherparametersotherthananIPaddress.

3.9 MAN-IN-THE-MIDDLEATTACKMITIGATION

Cryptography (encryption) is the only effective mitigation technique for Man-in-the-middle attacks. Man-in-the-middleattackmitigation canbeachievedby theencryption of trafficin an IP-Security tunnel.With thisEncryption method, intrudersor hackerscanseeonlyciphertext. (Mattsson2006)

4.0 CHANNELSOFSECURINGACOMPUTERNETWORK

4.1 PHYSICALSECURITY

Information security professionals have long focused on virtual risks, but at some point all things virtual becomephysical. It is that crossing point—where physical infrastructure and systems provide an access point to thevirtualworld--thatthelinkbetweenphysicalthreatsandvirtualthreatsaremostapparent (Lindstrom2003).
Many physical threats should be factored into a security program which includes; theft, human error, sabotage,and environmental disruption.

4.1.1 VideoSurveillanceandIP

Video surveillance and IP are modern technologies devices used in different part of the world toward protectingenterprises from the physical threat against their network as well as computing equipment. The attributes of thissolutioninclude:

- **Secure:** The computer architecture of a video surveillance renders the security of transmission byencrypting communications for protection against captured data or inserted into the information stream.Additionally, tamper resistivity on sensors can be deployed with a protective casing. Finally, the abilitytodistributeandadministersensorsoffersredundancytoprotectagainstfocusedattackonthesensor.
- **SolidState:**Movingpartsdonotexistonthesensors.Movingpartsareherebysusceptibletomechanicalandphysicaldamage,whichrequiressitevisitsforrepair.Bydevelopingthedigitalpotentialities of the system, the system was able to eradicate the need for mechanical features wherebythelikelihoodoffailure isreduced.
- **IP Connectivity:** Separate physical cabling for CCTV functions is required for existing monitoringsystems. Video surveillance uses the same technology it protects by incorporating it into the typical IPnetwork which allows sensors to be positioned anywhere the network protects its components. Inaddition, iteradicatesthenecessityfor duplicatecabling usingvariouswiretypes.
- **Multi-sensor collectors:** In keeping along with the "human senses" framework of threat monitoring,NetBotz provides the ability to gather data from multiple sensors in order to combine information into asingleplace.
- **Intelligentanalysissoftware:** The more software grows intelligent, the more quickly individualsrespond to threats. As technology produces the ability to aggregate data from various places, a level ofanalysis complexity is created which is best resolved through analytical software. Finally, this createseffectiveand efficientapproachto theneedsofidentifyingattacksand reactingto it.
- **Simple Network Management Protocol (SNMP) Aggregator:** Some capabilities are associated with aphysical threat monitoring system and works with the IP network with its ability to also collect SNMP(Simple Network Management Protocol) data and also passes the data along at appropriate times. (Pete,L.2003)

4.2 USAGEOFSYSTEMCONTROL

Once an operating system is installed on a computer, some simple steps should be taken immediately afterinstallation:

i. Defaultusernamesandpasswordsshouldbechangedimmediately.
ii. Access tosystem resourcesshouldberestricted,sothatonlytheauthorizedindividualscanhaveaccessto the resources.
iii. Anyunnecessaryapplicationandservicesshouldbeturnedoffanduninstalled,ifpossible.
iv. Systemshouldnotbeleftonorun-lockedwhilenotonsight.
v. UsersshouldsubscribeandalwayscheckSubscribeandalwayscheckforpatchesandupdatetoinstallfromsoftw

are andHardware vendors.

4.2.1 SECUREDPASSWORD

Thepracticeofthefollowingtechniquescangiveacompanyrestofmindconcerningpasswords:

i. Usersshouldnotbeallowedtohavethesamepasswordonmultiplesystems.

ii. Accountsshouldbedisabledafteracertainnumberofunsuccessfullogins.Thispracticepreventscontinuouspaswordattempts.

iii. A plain-text passwords should be avoided. The use of either an OTP (One Time Password) or encryptedpassword isrecommended.

iv. The use of strong passwords or passphrase is highly recommended. Strong passwords should be at leasteight characters long anduppercaseletters,lowercaseletters,symbolsorspecial characters,andnumbers should be used in passwords. Many systems provide strong password support and can alsorestricta usertousingofonlystrongpasswords.

4.2.2 SECURITYSOFTWARE

To protect against known viruses, host antivirus software should be installed. Antivirus software detects mostviruses and Trojan horse applications. It also prevents viruses from spreading in the network. Antivirus softwaredoesitsprotectionintwoways:

1. Filescanningbycomparingtheircontentswithknownvirusesinavirusdefinitiondatabaseordictionary.
2. Suspicious processes that run on a host and indicate infection are monitored. This monitoring mayincludeport monitoring, data captures, andothermethods.

5.1 SUMMARY

Flourishing in today's economy, service providers should provide open and easily accessible communicationsservices, which will enable their end users to contact anyone in the world. The same open and freely scalablecommunication architecture offers limitless communications services to end users and also sets a very attractivetargettohackers whowouldabusethatopencommunicationaccessfortheirown financial benefits.

A security implementation of an organization, irrespective of its size, should consider all forms ofaccess and intrusion on network hardware both physically and remotely, such as environmentalmonitoring,using video surveillance and IP, securing remote access using AAA (TACACS+) and deploying of firewalls anddemilitarized zone (DMZ).

Because security is a long-term issue, service providers need a security strategy and staff that is welleducatedinthatstrategy. To thatend, thisthesisdiscussed the tools and practices that areindispensabletonetworkoperators in securing theirnetworks against denial ofservice(DoS)attacksand other commonsecuritythreats. Finally, serviceproviderscanturnthosenecessary securityprotectionsintoprofitablemanagedsecurityservicesfortheirenterprisecustomers.

5.2 CONCLUSION

Because security is a long-term issue, service providers need to develop a security strategy. A good place to startis to educate staff on best practices. When implementing a security plan, it is important to begin by implementingthe most obvious protections first and by deploying equipment that is capable of the most advanced protections,deploying equipment capable of providing privileged-EXEC authentication and a higher level of scalability thanline-level, suchasAAA Services.

Other straightforward steps include: protection of servers and routers by using onetime passwords andallowing only authorized users to get to routers, by applying authorization systems based on TACACS+ orRADIUS. Administrators can also implement a mechanism to manage incoming traffic, which can include DoSattacks against the control processors of routers. In general, operators should turn off unused and unneededservices, evenwhenthismayentailturningofffeaturesonservers.

Finally, the increase in physical infrastructure as well as its growing implication to an organization hascreated the necessity to physically protect the systems themselves, not only from cyber-attacks, but also from thephysical attacks that can be perpetrated against them. Implementing policy-based security also brings manyadvantages to the security arsenal, because it automates the implementation of the security philosophy andlessens the chance of user error in protecting the network. When implementing security policy, it is necessary tokeep in mind that mechanisms such as DMZ, IPSec- VPNs, firewalls and intrusion detection and preventiontechniquesthataresocriticaltosecuringnetworkinfrastructurecanbeturnedintomanagedsecurityservicesthatcouldbe soldto enterprise customers.

REFERENCES

[1]. Adeyinka,O.,"InternetAttackMethodsandInternetSecurityTechnology,"Modeling &Simulation,2008.
[2]. AICMS08.SecondAsiaInternational Conferenceon,vol.,no.,pp.7782,1315May2008
[3]. AlSalqan,Y.Y.,"FuturetrendsinInternetsecurity,"DistributedComputingSystems,1997.,ProceedingsoftheSixthIEEEComputer

SocietyWorkshop onFutureTrendsof, vol.,no.,pp.216217,2931Oct1997
[4]. AndressJ.,"IPv6:thenextinternetprotocol," April2005,www.usenix.com/publications/login/200504/pdfs/andress0504.pdf.
[5]. Bidou,R.2000.Denialofserviceattacks.Retrieved:May102012.Availableat:http://www.docstoc.com/docs/85149779/Denial-of-Service-AttacksCiscoSecurity.2005.SecuringCisco Network Devices. (v 1.0 ed.) Available at: http://www.scribd.com/doc/985242/Securin g-Cisco-Network-Devices-SND-v1-0
[6]. Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24 28,Sep1998
[7]. Hill,J.2001.AnAnalysisoftheRADIUSAuthenticationProtocol.Retrieved:April162012.Available at:http://www.untruth.org/~josh/security/radius/radius-auth.html
[8]. Kartalopoulos,S.V.,"DifferentiatingDataSecurityandNetworkSecurity,"Communications,2008.ICC'08.IEEE InternationalConferenceon, pp.14691473,1923May2008
[9]. Landwehr,C.E.;Goldschlag,D.M.,"SecurityissuesinnetworkswithInternetaccess,"ProceedingsoftheIEEE,vol.85, no.12,pp.20342051,Dec 1997
[10]. Lin,D.;Tsudik,G.;Wang,X.CryptologyandNetworkSecurity,inProceedingsof10thInternationalConferenceon Cryptologyand NetworkSecurity: Sanya,China,2011, [p3]
[11]. Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3, no.6, pp. 68 72, Nov. Dec. 2005Mattsson,U.T. October 03, 2006. BestPractice for Enterprise Database Encryption Solutions. Retrieved:May5,
[12]. 2012.Availableat:http://papers.ssrn.com/sol3/papers.cfm?abstract_id=934271
[13]. MITKerberosTeamSecurityContact.TheNetworkAuthenticationProtocol.Retrieved:January27,2012.
[14]. Available at:http://web.mit.edu/kerberos/contact.html
[15]. Molva, R., InstitutEurecom,"Internet Security Architecture," in Computer Networks & ISDN Systems Journal,vol. 31, pp.787804,April 1999
[16]. Orbit-ComputerSolutions.2012.Threatstophysicalandnetworkinfrastructure.Retrieved:May52012.Availableat:,http://www.orbit-computersolutions.com/Threats-to-Physical-and-NetworkInfrastructure.php
[17]. Paul,A.May132003.ImplementingsecureaccesstoCiscodevicesusingTACACS+andSSH.Retrieved,February28,2012.
[18]. Availableat:http://www.sans.org/reading_room/whitepapers/networkdevs/implementingsecureaccess-cisco-devices-tacacs-plusssh_1041
[19]. Pete,L.June2003.TheEmergenceofthePhysicalThreatNo.2-3P.O.Box152,Malvern,PA19355:SpireSecurity, LLC.
[20]. Availableat:http://netbotz.com/library/Physical_Threat_Security.pdf
[21]. ReedD.November21,2003.NetworkModeltoInformationSecurity.Retrieved:Availableat:http://www.sans.org/reading_room/whitepapers/protocols/applying-osilayer-networkmodel- information-security_1309
[22]. Sotillo,S.,EastCarolinaUniversity,"IPv6securityissues,"August2006,www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf
[23]. Tyson,J.,"HowVirtualprivatenetworkswork,"http://www.howstuffworks.com/vpn.htm
[24]. WarfieldM.,"SecurityImplicationsofIPv6,"InternetSecuritySystemsWhitePaper,documents.iss.net/whitepapers/IPv6.pdf