ISSN: 2393-8528

IJICSE
Open Access

International Journal of Innovative Computer Science & Engineering (IJICSE)

Available Online at www.ijicse.in

Design and implementation of System and Wide Area Network Security

Ruchi Kumari[1], Lahar Singh Nishad[2]

[1]Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India

kumariruchi493@gmail.com

[2]Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India

laharsinghnishad@gmail.com

ABSTRACT

The root causes of information system security are that our information should be protected against unauthorized disclosure for legal and competitive reasons. All the information must be protected against accidental or illegal modification and must be available on time. Network security is the most important part of information security because it is responsible for securing all information passed via the network, and it is required to provide an acceptable level of protection for hardware and software. Poor security practices allow damage to our systems; we may be subject to criminal or civil legal proceeding. While good security can finally be seen as part of the market development strategy-consumers have expressed their concern over privacy and safety of data; Companies with strong security can furnish their investment to increase the pool of willing buyers and to increase their market share. In this paper we are describing how to protect our network and WAN network.

Key Words: Internet, TCP/IP, Security, Network Design, LAN, WAN, Encryption, VPN, IPSec.

INTRODUCTION:

Network Security means to protect network and data transmission over wired and wireless network. Internet is a network of networks that consists of millions of private, public, business and government networks of local to global scope that are linked by a broad array of electronic and optical networking technology. Network security is an important aspect for a wide variety of network application with increasing popularity of internet concerns about network security of personal computers, organizations and military have swiftly increased and therefore so much importance is being given to network security. The terms information security, computer security and information assurance are frequently used interchangeably, this fields are interrelated and share the common goals of protecting the availability of information, confidentiality and integrity. Protecting confidential information is a business requirement and many cases also in ethical and legal requirement. For the individual, information security has a significant effect on privacy, which is viewed very differently in different culture. As the more remote workers are added to business networks, the harder it becomes for IT to manage their connection back to head quarters. In order to ensure speedy and secure connections to branch offices, a WAN manager must strike a careful balance between WAN security and performance. This paper describes the WAN security to ensure the complete security of network. This would include physical security, network security and access control system. Physical security means keeping the network equipments safe from being physically damaged, tempered or stolen. Network security means keeping the information safe over the network while transmission. Access control system refers to control system that would allow user to access the information.

Network: A "network" has been defined as "any set of interlinking lines resembling a net, a network of roads and an interconnected system, a network of alliances". This definition suits our purpose well: a computer network is simply a system of interconnected computer.

The ISO/OSI Reference Model:

The International Standards Organization (ISO) Open System interconnect defines the seven layers of communication types, and the interfaces among them (See Fig.1). Each layer depends on the services provided by the layer below it. The OSI reference model is a hierarchical structure of seven layers that defines the requirements for communications between two computers. A system that implements protocol behavior consisting of a series of these layers is known as a 'protocol stack' or 'stack'. Protocol stacks can be

implemented either in hardware or software or the mixture of both.

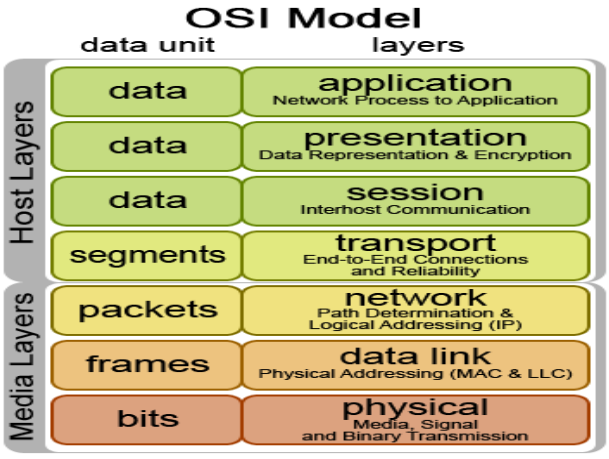


Figure 1: ISO/OSI reference Model

Only the lower layers are implemented in hardware, with the higher layers being implemented in software.

Security services and processes:

Network security services fundamentally for emerging internet applications characterized by real-time packet flows, large-scale multicasts and high-speed transmission such as customer database, web pages. Security services about risk management and implementing effective countermeasures.

Authentication:

Authentication is one of the important process of security to determine whether someone is, means who or what it is declared to be. It is completely done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially using an assigned or self-declared password.

Authorization:

Authorization is term for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. It is the process that governs the resources and operations that the authenticated client is permitted to access. Resources include files, databases, tables, rows, and so on, together with system-level resources such as registry keys and configuration data.

Auditing:

Auditing is one the important key for non-repudiation. Non repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

Confidentiality:

Confidentiality is a model designed to guide policies for information security within an organization. Confidentiality is a set of rules that limits access to information. It prevents sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. A good example is an account number or routing number when banking online. Data encryption is a common method of ensuring confidentiality.

Integrity:

Integrity of information means to protect information from being modified by unauthorized parties. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.

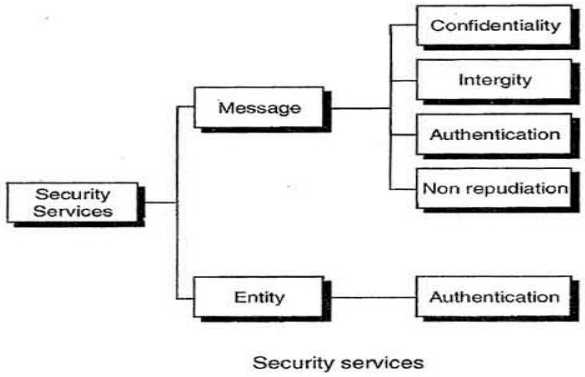


Figure 2: network security services

Availability:

From a security perspective availability of information refers to ensuring that legitimate parties are able to access the information when needed. These facets are an important step in designing any secure system (shown in fig2.). These techniques are applied to protect against internal and external network attacks.

Network security and protection

The main purpose of network security to prevents and monitors unauthorized access, misuse or denial of a computer network. It is the most vital component in information security because it is responsible for securing all information sent via computer. Following terms help in making correct decision regarding network security and prevention.

Attack Recognization: it recognize some common attacks, such as spoofing, Man-In-The-Middle attack, denial of service, buffer overflow etc. Encryption Technique: understand techniques to ensure confidentiality,

integrity, authenticity and no-repudiation of data transfer.

Network Security Architecture: configure a network with security appliances and software, such as placement of firewalls.

Access Control Lists (ACLs): Configure and audit routers and firewall to filter packets accurately and efficiently, dropping, passing or protecting packets based upon the IP or Port address.

Intrusion Detection/Prevention System (IDS/IPS): set and test rules to recognize and report attacks in a timely fashion.

Vulnerability Testing: Test all nodes to determine active application via scanning.

Security Planning: Prepare a security plan including security policies and procedure.

WAN PROTECTION:

All enterprises rely on WAN connections such as Frame Relay, ATM etc which provides more reliable and secure connection. WAN make the connections between all their branches secure, and all sending data reach in safe hands as recipient. It configure external network of any company protected and high level secured, the virtual private network 'VPN' is a good solution to organize a secure access to the internal network remotely. Internet protocol security 'IPSec' is configured with VPN to have more security to the network.

Virtual Private Network (VPN):

VPN is one of the most important solutions to viruses and hackers threats that make the network between companies and users secured. A virtual private network (VPN) is a network that uses a public communication infrastructure, like Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost. Three types of encryption protocols that Windows Servers use for secure communication: L2F, L2TP and PPTP.

Layer -2 Forwarding "L2F": L2F is a protocol that is designed to allow the tunneling of PPP frames between a NAS (network access server) and a VPN gateway device located at a central site. Remote access users connect to the NAS, and the PPP frames from the remote access user are then tunneled over the intervening network to the VPN gateway.

Point-to-Point Tunneling Protocol (PPTP)—PPTP is a protocol, developed by a consortium of vendors, including Microsoft and Ascend Communications. Like L2F, PPTP allows the tunneling of remote access client PPP frames between a NAS and a VPN gateway. PPTP uses a TCP connection for tunnel management and a modified version of Generic Routing Encapsulation (GRE) to encapsulate PPP frames for tunneled data. it provides a protected tunnel between PPTP enabled client "personnel computer" and a PPTP enabled server.

Layer 2 Tunneling Protocol versions 2 and 3 (L2TPv2/L2TPv3)—L2TP is an Internet Engineering Task Force (IETF) standard and combines the best features of L2F and PPTP. L2TP over IP networks uses User Datagram Protocol (UDP) and a series of L2TP messages for tunnel management. L2TP also uses UDP to send L2TP-encapsulated PPP frames as tunneled data. In a remote access environment, L2TP allows either tunneling of remote access client PPP frames via a NAS to a VPN gateway or tunneling of PPP frames directly from the remote access client to the VPN gateway.

IPSec:

The IPSec framework is a suite of IETF standards that provides for secure transmission of data over unsecured networks. It can also be used to securely tunnel data traffic between remote access or mobile users and a VPN gateway. IPSec protects against security vulnerabilities that are IP spoofing, Session hijacking and Traffic sniffing.

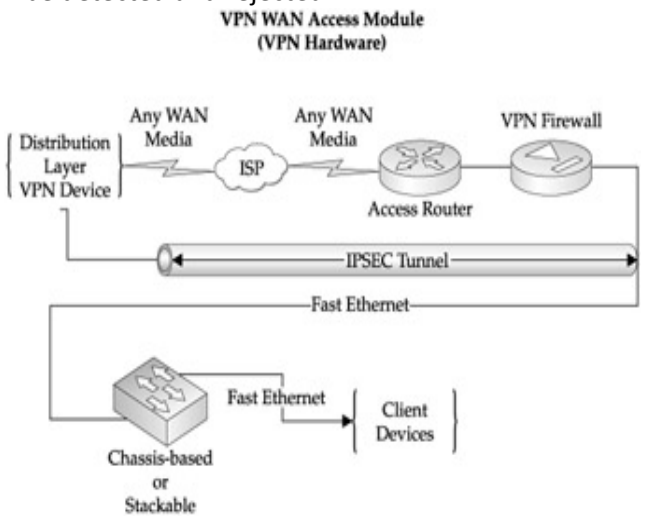
IPSec services:

Data transmission encryption: The sender host can encrypt packets prior to transmission.

Data integrity validation: The receiving host can authenticate each packet sent to ensure the original data that was transmitted was received.

Data source authentication: The sender host can mark packets, so the receiver can authenticate them.

Data state integrity: The sending and receiving hosts can mark packets, so any retransmission of the data stream can be detected and rejected.



IPSec implementations use a number of different security protocols to provide all above services. There are two IPSec packet protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). There are a number of service protocols, but the primary one is the Internet Key Exchange protocol (IKE).

Threats and Attacks on Router

While discussing about network security, Security of router can't be ignored. The three common factor used for network security are vulnerability, threats and attacks.

Vulnerability— A weakness that is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves.

Threats— The people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses.

Attacks— The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. The network devices under attack are the end devices, such as desktop and server.

There are three primary Vulnerabilities or weaknesses:

1. Technology weaknesses
2. Configuration weaknesses
3. Security policy weaknesses

Technical Weaknesses: Computer and network technologies have intrinsic security weaknesses. These include TCP/IP protocol weaknesses, which includes HTTP, FTP, SMTP insecure structure, operating system weaknesses it includes UNIX, Linux, Macintosh, Windows NT, 9x, 2K, XP and OS/2 operating systems all have security problems, and network equipment weaknesses Various types of network equipment, such as routers, firewalls, and switches, have security weaknesses.

Configuration Weaknesses: It is necessary to network administrator or network engineers to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate. Some common configuration weaknesses are unsecured user accounts, System account with easily guessed password, Misconfigured Internet Services, unsecured default settings within products etc.

Security Policy Weaknesses: Security Policy Weaknesses can create unforeseen security threats. The network may pose security risks to the network if users do not follow the security policy. Some common security policy weaknesses are lack of written security policies, lack of continuity, logical access controls not applied, software and hardware installation and changes do not follow policy etc.

There are four primary classes of threats for network security:

Unstructured threats: It consists of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company.

Structured threats: Structured threats come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses.

External threats: External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers.

Internal threats: Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network.

There are four classes of attacks:

Reconnaissance: It occurs when an adversary tries to know information about the network. It is the unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also known as information gathering.

Access: This attack occurs when someone tries to gain unauthorized access to a component, tries to gain unauthorized access to information on a component, or increases their privileges on a network component. Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information.

Denial of Service: Denial of service implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. This involves either crashing the system or slowing it down to the point that it is unusable.

Password Attacks: A password attack usually refers to repeated attempts to identify a user account, password, or both. These repeated attempts are called brute-force attacks. Password attacks are implemented using other methods, including Trojan horse programs, IP spoofing, and packet sniffers.

Solution to Router Attack

To enable security on router, password should be prompted because without password it acts as an open network.

If remote administrator is enabled, it allows anyone to view or change the router setting. So network security recommends remote administrator should be disabled.

Routers have their own firewall that can be enabled, enabling this feature as it helps add an extra layer of security for network.

Enabling of SSID allows that anyone looking for a wireless router, they can easily see your SSID, to make it more difficult to someone to find your network, disable the SSID feature. When you want to connect a new device to your network you have to manually enter your unique SSID.

The wireless MAC filter features allows a wireless device to connect to your router if the MAC address has been enter in the filter list. This can make connecting new devices to your network more difficult but improves the overall security of your wireless network.

Conclusion:

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. This module introduced the needs, trends and goals of network security. This paper describe the ISO/OSI model that is bone of networking which describe function of all layers and needs of security at network layer. We also describe security services and processes. We also throw a light on WAN protection using VPN, under VPN we also mention L2F, PPTP, L2TP, IPSec. This paper also includes discussion on threats and attacks on router with appropriate solution to how to protect wireless connection.

REFERENCES:

1. C. Karlof and D. Wagner., “Secure Routing in Wireless Sensor Networks: Attacks and Counter measures”, Sensor Network Protocols and Applications (SNPA'03), May 2003
2. H. Deng, W.Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, 2002, pp. 70 75.
3. P Papadimitratos, “SecureData Communications in Mobile Ad Hoc Networks” IEEE Journal On Selected Areas In Communications, vol. 24, No. 2, February 2006 pp 346 356
4. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, K. Nygard “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”
5. Akin T.," Hardening Cisco Routers," O’Reilly & Associates, 2002.
6. Kim J., Lee K., Lee C.," Design and Implementation of Integrated Security Engine for Secure Networking,"In Proceedings International Conference on Advnaced Communication Technology, 2004.
7. Q. Ali., and Alabady S., "Design and Implementation of A Secured Remotely Administrated Network,"In Proceedings International Arab Conference on Information Technology, ACIT'2007.
8. Munasinghe K. S. and Shahrestani S. A., “Evaluation of an IPSec VPN over a Wireless Infrastructure,” in Proceedings of the Australian Telecommunication Networks and Applications Conference (ATNAC 2004), pp. 315-320, December 2004a.
9. Munasinghe K. S. and Shahrestani S. A., “Analysis of Multiple Virtual Private Network Tunnels over Wireless LANs,” in Proceedings of the 3rdInternational Business Information Management Conference (IBIMA 2004), pp. 206-211, December 2004b.
10. Shimonski Robert J., Configuring Symantec Antivirus: enterprise edition. Lavoisier, 2003.
11. Shinder D., How the Windows Rights Management Service can Enhance the Security of your Documents. Published: Sep 23, 2003 Updated: Apr 06, 2005 Section: Articles. Windows 2003 Security. www.windowsecurity.com
12. Stallings W., Cryptography and Network Security, 4/E Prentice Hall, 2006.
13. Stinson D., Cryptography Theory and Practice, Third Edition last modified January 19, CRC Press, 2006.
14. SurfControl Instant Message Filter, Administrator's Guide Version 4.5 printed June 30, 2004. www.surfcontrol.com
15. SÜHEYLA K ZIN, Performance parameters of wireless virtual private network. Master Thesis, Middle East University. 2006.