International Journal of Information Technology and Knowledge Management
January-June 2011, Volume 4, No. 1, pp. 133-137

COMPARATIVE ANALYSIS OF DATA SECURITY TECHNIQUES IN NETWORK ENVIRONMENT

Kanwaljit Singh[1] & Tejpreet Singh[2]

In the network, data are transformed in form of packets to transfer from one place to another for the communication. To make the communication successful and effective, data should remain protective at sender and receiver end. Various attacks and vulnerable actions are performed by the hackers and attackers to affect the data. In the seven layer network environment, various attacks are fired at different layers. To make the network most fired proof, various network securities are implemented. In this paper we discuss about the OSI layers, vulnerable attacks and security techniques, and a comparative analysis of network security techniques is done against the vulnerable attacks to make the data on network error free and through analysis to find the best security techniques. This paper will be beneficial for the Information Technology professionals who are responsible for implementing the security on organizational network for data communication.

1. Introduction

In the network environment the data move from one location to another through a particular path using hardware and software tools like switches, routers, gateways, protocols, etc. The media used to transfer data can be either the wire-oriented or the wireless. An IP (Internet Protocol) address is a unique code that each computer has that identifies the machine these packets are being sent from. IP addresses can be used to identify where a computer is connecting from. A proper technique or system is used to transfer the data from source to destination. The data has to pass through the seven layers of source-end from physical layer to application layer. And after passing through the physical layer the data is transferred into the network. And at the destination end again the data is passed through the seven layers from physical to application layer.

The seven layers are Physical layer, Data-link layer, Network layer, Transport layer, Session layer, Presentation layer and Application layer. Starting from the application layer at one station, proceeding to the bottom layer over the channel to the next station and back up the hierarchy. Each layer performs different functions. The Physical layer deals with the physical properties of the network, such as voltage levels, cable types, and interface pins. The Data Link layer transmits and receives packets of information reliably across a uniform physical network. The Data-link layer provides error control and flow control of data. To make the communication active among two computers, MAC address role comes into play. MAC addressing information resides on OSI model layer-2.

The Network layer handles the data routing and forwarding. The Network layer routes data through various physical networks while travelling to a known host. Routers are the machines that decide how to send information from one logical network to another. The Network layer principle is knowing that routers make decisions based on OSI layer-3 information. The Transport layer manages end-to-end transmission control and error control. Transport layer ensures the reliable arrival of messages and provides error checking mechanism and data flow controls. The Session layer establishes, manages and terminates the communication period of data sending and receiving of two communicating end points. The Presentation layer translates the data i.e. the layer ensures that the communications passing through are in appropriate form for the recipient. And the Application layer defines the standards for interaction at the user or application program level, such as provides the GUI to communicate between user and PC/ Sever.

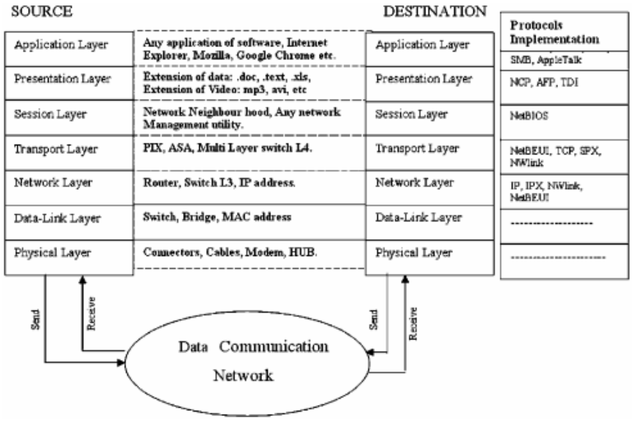
In the network the data flow in the form of packets. The packet is divided into two parts; 'source address and destination address' and 'encrypted data and identification number'. Every organization has the database or networks that store or transfer the data according to the requirements. For example, in banking sector the data is stored in form of currency figures and have its own private network, a software organization store its data in the form of high level or low level programs, etc. The data can be either in rest or in moving state, i.e. either stored in database (server) or transferred from source to destination via some network. Network security is a top-priority issue in data communication networks. As communication networks are growing rapidly, security issues have pushed to the forefront of concern for end users, administrators and equipment

[1]Amritsar College of Engg & Tech, Amritsar

[2]Khalsa College of Engg & Tech, Amritsar

Email: [1]waliakanwal@hotmail.com, [2]tejricky@gmail.com

suppliers. If we talk about security two major entities get highlighted; network vulnerability and network attacks.


SOURCE
DESTINATION
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data-Link Layer
Physical Layer
Any application of software, Internet Explorer, Mozilla, Google Chrome etc.
Extension of data: .doc, .text, .xls, Extension of Video: mp3, avi, etc
Network Neighbour hood, Any network Management utility.
PIX, ASA, Multi Layer switch L4.
Router, Switch L3, IP address.
Switch, Bridge, MAC address
Connectors, Cables, Modem, HUB.
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data-Link Layer
Physical Layer
Protocols Implementation
SMB, AppleTalk
NCP, AFP, TDI
NetBIOS
NetBEUI, TCP, SPX, NWlink
IP, IPX, NWlink, NetBEUI

Send
Receive
Send
Receive
Data Communication Network

Fig 1: Flow of Data through Seven Layers (Tools and Protocols Implemented in Each Layer)

2. VULNERABILITIES

Vulnerabilities and attacks increases due to the grant permitted at different levels to access the network. The grant is permitted to the remote user or to the business partner or supplier, etc. to access the site. In this paper the vulnerabilities and the attacks are defined according to the layer.

Today's network engineer has no choice but to be security-conscious and the security engineer has no choice but to understand the network he is taken to secure. The Internet connection is all it takes to exploit a well known vulnerability and a computer doesn't check for a user's intent when logging them on. Majority of the vulnerabilities display themselves as application vulnerabilities, which are closer to user application. The Application layer vulnerabilities are the Denial of Service (DoS), Buffer Overflow and Malicious Attacks i.e. attacks on the network by the viruses or worms or humans. These applications send the username or password in such a way that, if anyone senses the network traffic, can easily access the username and password and gain the unauthorized network access. Presentation layer vulnerabilities include poor handling of inputs that can crash the application or surrender of control to execute arbitrary instructions. Some of the examples of presentation vulnerabilities are buffer overflows. The program execution can be redirected into completely unintended areas due to these vulnerabilities. Session layer establish the connection using the port number and the sequence number. The vulnerabilities are easily exploited in session layer, as it is very easy for the hacker to guess the port numbers as they are of standard and the sequence number can be guessed in predictable way and the malicious attack rate increases. The transport layer manages the end-to-end transmission. The different vulnerabilities occur in transport layer are standard port number, Denial of Services and spoofing. The next layer is network layer; this layer is responsible for routing and forwarding of data. One of the biggest vulnerability is that there is no certain path between the source to the destination that make their data safe. Other vulnerabilities are attacks on routers like password attack, malicious attacks, buffer attack, denial of services and IP spoofing. Data-link layer deals with physical and logical connections of the packet on the network and also the error control. Data link layer work with the help of two sub layers; Media Access Control (MAC) and Logic Link Control (LLC) that are connected via a protocol, Address Resolution Protocol (ARP). The various vulnerabilities arises in data-link layer are ARP vulnerabilities i.e. ARP has no means for authentication or validation, ARP spoofing, MAC flooding. And the last is the physical layer that deals with the physical communication between two communicators. The vulnerabilities that arise in this layer are loss of power, physical theft of data or hardware, unauthorized change in the environment by removing resources, or by disconnecting physical data-links.

Table 1
A Two-dimensional Matrix Representation between Layers and Vulnerabilities

Vulnerabilities Layers	DoS	Malicious Attacks	Buffer Overflow	Spoofing	ARP	Physical Damage
Physical Layer	√					√
Data-Link Layer	√		√	√	√	
Network Layer	√	√	√	√		
Transport Layer	√			√		
Session Layer		√		√		
Presentation Layer			√			
Application Layer	√	√	√	√		

The major vulnerabilities that create the obstacle in the network are Spoofing, Buffer Overflow, Denial of Services, Malicious attacks, ARP and Physical damage. If these vulnerabilities are plug out from the network the communication become more efficient and safe.

1. Denial of Services (DoS): The hacker can play violently with your computer without penetrating into your computer. DoS intensifies the network and putting high computational load on the target system by sending many connection requests to a target system which increase the volume of data on network and by spoofing the source MAC

address of the access point, the receipt has no way of telling if the requests are legitimate or illegitimate and process them, which results in degradation of the network.

2. Spoofing and Hijacking: Hijacking is one step ahead to spoofing. Hijacking fakes someone's identity in order to take over the connection that is already established.

   Spoofing is a technique that forwards the packets to a computer with a source address indicating that the packets are coming from trusted computer.

3. Malicious Attacks: The set of programs that enter into the network by breaking its firewall and taking the advantage of someone's computer. The malicious attacks are generated by virus, worms, etc. Malicious attacks reduce the functionality of the target computer.

4. ARP: Address Resolution Protocol. ARP is a protocol that allows a source computer to ask other computer if they know the MAC address of the machine it wants to speak with. The function of ARP is the mapping between IP address and MAC address on local network. MAC addressing information resides on OSI model layer-2. By altering the MAC information one can effectively exploiting the Data Link Layer. This is known as ARP Cache Poisoning.

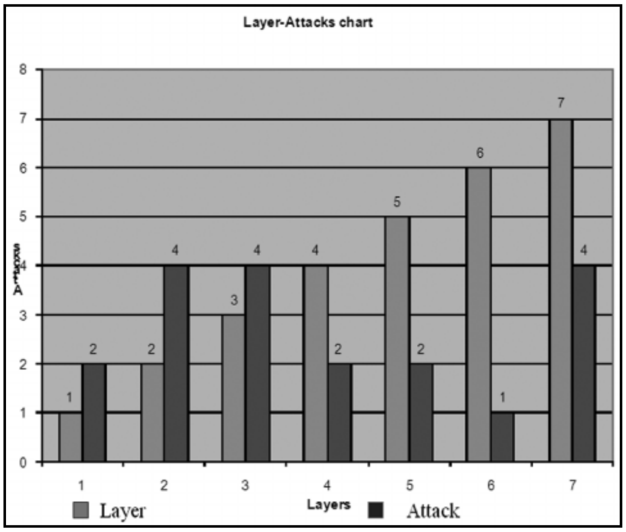


Fig. 2: A Layer-Vulnerabilities or Attacks Relation Chart

5. Buffer Overflow: Buffers are data storage areas, which generally hold a pre-defined amount of finite data. A buffer overflow occurs when a program attempts to store data into a buffer, and the data is larger than the size of the buffer. During buffer overflow the extra data can overflow into adjacent memory locations, corrupting valid data and possibly changing the execution path and instructions. The ability to exploit a buffer overflow allows one possibly inject arbitrary code into the execution path. This arbitrary code could allow remote system level access, giving unauthorized access to not only malicious hackers, but also to replicating malware.

From fig-2 one can easily analyse the possibility of attack on data communication network layers.

3. SECURITY TECHNIQUES

Network security is a technique that reduces the possibility of the vulnerable attacks on the network. The security product is said to be effective if it prevents the network from the maximum possible threats. Various respondents use different security techniques to prevent the network from the vulnerabilities. One has to choose the most apparent technique(s) that is (are) most effective against the intrusions. The table (Tab-2) represents the various security techniques used against the attacking vulnerabilities.

Table 2
Two Dimensional Matrix Representations between Vulnerabilities and Security Techniques

Vulnerabilities → ↓ Security Techniques	DoS	Malicious Attack	Buffer Overflow	Spoofing	ARP	Physical Damage
Firewall	√	√	√	√	√	
IPS	√	√	√			
IDS	√	√				
NAC	√	√				
Hardening	√	√		√	√	
Physical Security	√					√

Firewall

A firewall is a combination of software and hardware devices that filters the information coming through the network to network to block unwanted traffic. The firewall is designed to protect the information and to prevent from intruders. The network will turned into a relay machine to send out flood of spasm or DoS attack. The technologies used by firewall to overcome the DoS are as follow:

(a) Network Address Translation (NAT to prevent crackers from seeing our network address). The NAT technology translated the IP address of the network to different IP address for the Internet.

(b) Stateful Packet Inspection (SPI provide high degree of security) SPI inspects the packets of information coming into the network to make sure they correspond to an outgoing request and are not an attack from a cracker.

(c) Proxy Server: With proxy, all traffic from the Internet is sent to the proxy, the third party watching the transmission only see the proxy not the actual network.

Advanced firewall programs give network extra protection through cookie control, spyware control, adware control and software application control. The firewall that keeps on informing all the conversations the network has on the Internet so that network can be in control. All the above technologies help the firewall to prevent the network from the Denial of Service, Malicious attacks, buffer overflow, and ARP vulnerabilities. Entrance filtering, a technique which verifies that packets are coming from a legitimate source, is also an invaluable tool to safeguard against attacks enabled through IP spoofing.

Hardening

Hardening is the process of identifying and fixing vulnerabilities on a system or network by evaluating network's security hardware, software and processes and then making the appropriate adjustments to strengthen them. With sufficient time for research and development, additional work on core network protocols can be used to harden the network and devices against the malicious attacks.

Route and packet filtering at network is an easy way to decrease vulnerabilities at the base level. If these two best practices are widely adopted, there would be a significant decrease in Denial of service attackers which use forged and unexpected source IP addresses. The route and packet filtering help to prevent spoofing of traffic via the injection of false routing control message. Switch hardening offers protection against ARP attacks. IOS has a command called Set Port Security. Enabling this feature will restrict the switch such that only one (default) MAC address is allowed per physical port. This command allows one to configure the action that will take place upon a hardware address change. By limiting the number of hardware address per unit, a host cannot change his hardware address or try to map multiple MAC addresses to route traffic out one port. This will not analyse the MAC/IP table and take action during changes.

IDS: Intrusion Detection System

Intrusion Detection System (IDS) is a type of security management system for computers and networks. An IDS gathers and analyzes information from various areas within a network to identify possible security breaches, which include both intrusions and misuse. In IDS the sensors are located in the network borders. The sensors capture all network traffic and analyse the content of individual packet for malicious traffic.

The recognizing pattern matching attack methods is the oldest method in IDS. It involves identifying an intrusion just by examining a packet and recognizing within a series of bytes, a sequence which corresponds to a specific signature. This method is used as a supplement to filters on IP addresses, destination used by connections and source and destination ports. By filtering the requests the denial of service vulnerability can be overcome and the networks will response to the required requests.

IPS: Intrusion Prevention System

An Intrusion prevention system is a network security device that monitors network activities for malicious or unwanted behavior and can react in real-time, to block or prevent those activities. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) monitors network traffic. IPS is new generation of IDS. IPS drops the offering packets and then potentially blocks the entire data flow form the suspected hacker. If the traffic that triggered the false positive alert of a customer order, the customer will not wait around for long as his entire session is torn down and all subsequent attempts to reconnect to network are blocked by the well meaning IPS. This will overcome the problem of denial of service.

IPS operate inline to monitor all network traffic for malicious attacks. The blocking of packets overcome the problem of buffer overflow and malicious attacks.

Network Access Control (NAC)

Network Access Control (NAC) is an approach to computer network security that attempts to merge endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.

The threat of malicious code is greater in the networked machine space. The NAC technology prevents split tunneling i.e two or more applications to be communicating simultaneously, while the network connection is going on. Preventing split tunneling creates illusion of safety.

Physical Security

Locking the server room, switch box help the network authorities to protect the server and the switch from the network tangling. Latch guards should be installed to prevent prying the door open with a crow bar. Hallway cameras are also a good deterrents for un-wanted visitors. Physical access could also allow a hacker to add accounts to the server. Those accounts could be used to access the server remotely and launch a DoS attack. The hard locks with maximum pins and the hidden cameras will prevent the hackers to access the servers to operate with the data and network tools and applications. These physical security tools prevent the network from the denial of service vulnerability

4. CONCLUSION

The first phase of the paper clarifies that all the seven layers with appropriate protocols are helpful for flow of data from source IP address to destination IP address on the network. The second phase discuss about the layer-vulnerability interaction. Each layer is attacked by various vulnerabilities to generate the obstacles in data flow. The vulnerabilities attack jointly or individually on network to destroy the authenticity of the data and damage the network. On analysis it was found that among the seven layers, the layers that deeply affected by the vulnerable attacks are data link layer, network layer and application layer. The other layers are also get affected but in less proportionate Among the various vulnerabilities discussed above, denial of service and spoofing are the most prominent that makes the network weaker. The third phase illustrates the security techniques that may be implemented to overcome the attacks. To secure the passive or transit data and to strengthen the network, analysis has been done on security techniques and it is found that firewall is the strongest security technique that makes the network strong and data authenticated. The paper concludes that, by collaborating the most effective security techniques, a strong bond can be generated that will protect the network and the data from the vulnerable attacks.

Bibliography

[1] The Book “Computer and Communication Networks” by Nader F. Mir.

[2] Damon Reed, “Applying the OSI Seven Layer Network Model to Information Security”, SANS GIAC GSEC Practical Assignment Version 1.4b, 2002.

[3] Glenn Surman, “Understanding Security using the OSI Model”, GSEC Practical Version 1.3, 2002.

[4] Eric Chien and Péter Ször, Virus Bulletin Conference, September 2002, “Blended Attacks Exploits, Vulnerabilities and Buffer-overflow Techniques in Computer Viruses”.

[5] Intrusion Prevention System (2004).

[6] Robert Wagner, Jeff Bryner, CISSP, GCIH-Gold, GCFA-Gold, “Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks”, SANS Institute 2008.

[7] Jake Shores, “Network Hardening”.

[8] Lingyu Wang, Steven Noel, Sushil Jajodia, “Minimum-Cost Network Hardening Using Attack Graphs”, Science Direct, Computer Communications, 29(2006) USA.

[9] David W Chadwick, “Network Firewall Technologies” IS Institute, University of Salford, Salford, England.

[10] Stuart Compton “Denial of Service Attacks and Mitigation”, GAWN Gold Certification, SANS Institute 2008.

[11] Charles H Scott Jr, “Auditing and Securing Multifunction Devices”, GSEC Gold Certification, SANS Institute 2007.

[12] Renaud Bidou, “How to Test IPS” RADWARE.

[13] Erik Rodriquez, “Physical Network Security”.

[14] Sophia J. Carter, “Ways to Prevent IP Spoofing”, eHow Contributor, 2009.

[15] Pete Lindstrom, “Intrusion Prevention System (IPS): Next Generation Firewals”, Research Report, Spire Security, 2004.

[16] Joel Snyder, “NAC Deployment A Five Step Methodology”, OPUS ONE, 2007.

[17] CISCO Systems, “A Begineer’s Guide to Network Security” CISCO Systems, 2001.