NETWORK SECURITY

ABSTRACT

Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Network Security is a broad topic that covers a multitude of sins (an act that causes strong disapproval). Network security has become more important to personal computer users, organizations and the military. With the phenomenal growth in the Internet, network security has become an integral part of computer and information security. In order to come up with measures that make networks more secure, it is important to learn about the vulnerabilities that could exist in a computer network and then have an understanding of the typical attacks that have been carried out in such networks. The main motive behind this paper is to study the threats to network security and the measures or techniques we should follow to protect our network.

Keywords: Resources, Authorization, Security, Communications, Server, Network.

INTRODUCTION

Network security is a mechanism to protect data or message from going into the hands of malicious people. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. Network security is typically handled by a network administrator or system administrator who implements the security policy, network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access and also ensure that employees have adequate access to the network and resources to work.

A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network. Network security is an organization's strategy and provisions for ensuring

the security of its assets and of all network traffic. Network security is manifested in an implementation of security policy hardware, and software. Network security is crucial requirement in emerging networks.

Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment. While developing a secure network, the following need to be

a) Access: authorized users are provided the means to communicate to and from a particular network.
b) Confidentiality: It means that the content of message when transmitted across a network must remain confidential i.e only the intended receiver and no one else should be able to read the message.
c) Authentication: It is the identification and assurance of the origin of information. The receiver needs to be sure of senders identity i.e. the receiver has to make sure that the actual sender is the same as he claims to be.
d) Integrity: It means that the data must reach its destination without any modification i.e. exactly as it was sent.
e) Non-Repudiation: it means that the sender must not be able to deny sending a message that was actually sent.

NETWORK SECURITY CONCEPTS

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' also used (e.g., a fingerprint or retinal scan). Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wire shark traffic and may be logged for audit purposes and for later high-level analysis. Communication between two hosts using a network may be encrypted to maintain privacy.

BASIC SECURITY ASSUMPTIONS

Several new assumptions have to be made about computer networks because of their evolution over the years:

- Modern networks are very large, very interconnected, and run both ubiquitous protocols (such as IP) and proprietary protocols. Therefore, they are often open to access, and a potential attacker can with relative ease attach to, or remotely access, such networks. Widespread IP internetworking increases the probability that more attacks will be carried out over large, heavily interconnected networks, such as the Internet.
- Computer systems and applications that are attached to these networks are becoming increasingly complex. In terms of security, it becomes more difficult to analyze, secure, and properly test the security of the computer systems and applications; it is even more so when virtualization is involved. When these systems and their applications are attached to large networks, the risk to computing dramatically increases.

OBJECTIVES

a) To examine the threats to Network Security.
b) To examine the techniques which are essential to ensure network security.

RESEARCH METHODOLOGY

The methodology adopted for this paper is based on secondary data only. So, we have taken reference from journals, research papers, reference books, magazines and internet.

THREATS TO NETWORK SECURITY

a) **Malware:** Malware is short for "malicious software." Wikipedia describes_malware as a term used to mean a "variety of forms of hostile, intrusive, or annoying software or program code." Malware could be computer viruses, worms, Trojan horses, dishonest spyware, and malicious rootkits—all of which are defined below.
b) **Computer virus:** A computer virus is a small piece of software that can spread from one infected computer to another. The virus could corrupt, steal, or delete data on your computer—even erasing everything on your hard drive. A virus could also use other programs like your email program to spread itself to other computers.
c) **Rogue security software:** Have you ever seen a pop-up window that advertises a security update or alert? It appears legitimate and asks you to click on a link to install the "update" or "remove" unwanted malicious software that it has apparently detected. This could be rogue security software designed to lure people into clicking and downloading malicious software. Microsoft has a useful webpage that describes rogue security software and how you can protect yourself.

d) **Trojan horse:** Users can infect their computers with Trojan horse software simply by downloading an application they thought was legitimate but was in fact malicious. Once inside your computer, a Trojan horse can do anything from record your passwords by logging keystrokes (known as a keystroke logger) to hijacking your webcam to watch and record your every move.

e) **Malicious spyware:** Malicious spyware is used to describe the Trojan application that was created by cybercriminals to spy on their victims. An example would be keylogger software that records a victim's every keystroke on his or her keyboard. The recorded information is periodically sent back to the originating cybercriminal over the Internet. Keylogging software is widely available and is marketed to parents or businesses that want to monitor their kids' or employees' Internet usage.

f) **Computer worm:** A computer worm is a software program that can copy itself from one computer to another, without human interaction. Worms can replicate in great volume and with great speed. For example, a worm can send copies of itself to every contact in your email address book and then send itself to all the contacts in your contacts' address books. Because of their speed of infection, worms often gain notoriety overnight infecting computers across the globe as quickly as victims around the world switch them on and open their email.

g) **Botnet:** A botnet is a group of computers connected to the Internet that have been compromised by a hacker using a computer virus or Trojan horse. An individual computer in the group is known as a "zombie" computer. This could include distributing spam to the email contact addresses on each zombie computer, for example. If the botnet is sufficiently big in number, it could be used to access a targeted website simultaneously in what's known as a denial-of-service (DoS) attack. The goal of a DoS attack is to bring down a web server by overloading it with access requests. Popular websites such as Google and Twitter have been victims of DoS attacks.

h) **Spam:** Spam in the security context is primarily used to describe email spam — unwanted messages in your email inbox. Spam, or electronic junk mail, is a nuisance as it can clutter your mailbox as well as potentially take up space on your mail server. Unwanted junk mail advertising items you don't care for is harmless, relatively speaking. However, spam messages can contain links that when clicked on could go to a website that installs malicious software onto your computer.

i) **Phishing:** Phishing scams are fraudulent attempts by cybercriminals to obtain private information. Phishing scams often appear in the guise of email messages designed to appear as though they are from legitimate sources. For example, the message would try to lure you into giving your personal information by pretending that your bank or email service provider is updating its website and that you must click on the link in the email to verify your account information and password details.

j) **Rootkit:** A rootkit is a collection of tools that are used to obtain administrator-level access to a computer or a network of computers. A rootkit could be installed on your computer by a cybercriminal exploiting a vulnerability or security hole in a legitimate application on your PC and may contain spyware that monitors and records keystrokes. Rootkits gained notoriety when, in 2005, a security blogger discovered

that a copy-protection tool inside music CDs from Sony BMG Music Entertainment was secretly installing a rootkit when users copied the CD onto their computers.

k) **Masquerading:** Masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. The attempt may come from within an organization, for example, from an employee; or from an outside user through some connection to the public network.

TECHNIQUES OF NETWORK SECURITY

a) CRYPTOGRAPHY

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Until modern times, cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible text (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext.

A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the ciphertext. Formally, a "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible ciphertext, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important both formally and in actual practice, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

There are two kinds of cryptosystems: symmetric and asymmetric. In symmetric systems the same key (the secret key) is used to encrypt and decrypt a message. Data manipulation in symmetric systems is faster than asymmetric systems as they generally use shorter key lengths. Asymmetric systems use a public key to encrypt a message and a private key to decrypt it. Use of asymmetric systems enhances the security of communication. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share

the same key (or, less commonly, in which their keys are different, but related in an easily computable way). Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others.

A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each ciphertext exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all consistent and secret. The difficulty of securely establishing a secret key between two communicating parties, when a secure channel does not already exist between them, also presents a chicken-and-egg problem which is a considerable practical obstacle for cryptography users in the real world.

b) FIREWALL

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls are a software appliance running on general purpose hardware or hardware-based firewall computer appliances that filter traffic between two or more networks. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine. Firewall appliances may also offer other functionality to the internal network they protect such as acting as a DHCP or VPN server for that network.

Packet filters act by inspecting the "packets" which are transferred between computers on the Internet. If a packet does not match the packet filter's set of filtering rules, the packet filter will drop (silently discard) the packet or reject it (discard it, and send "error responses" to the source). Conversely, if the packet matches one or more of the programmed filters, the packet is allowed to pass. This type of packet filtering pays no attention to whether a packet is part of an existing stream of traffic (i.e. it stores no information on connection "state"). Instead, it filters each packet based only on information contained in the packet itself (most commonly using a combination of the packet's source and destination address, its protocol, and, for TCP and UDP traffic, the port number). TCP and UDP protocols constitute most communication over the Internet, and because TCP and UDP traffic by convention uses well known ports for particular types of traffic, a "stateless" packet filter can distinguish between, and thus control, those types of traffic (such as web browsing, remote printing, email transmission, file transfer), unless the machines on each side of the packet filter are both using the same non-standard ports.

c) DIGITAL SIGNATURES

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity). Digital signatures are a standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering. Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. Digital signatures employ asymmetric cryptography.

In many instances they provide a layer of validation and security to messages sent through a non secure channel: Properly implemented, a digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital seals and signatures are equivalent to handwritten signatures and stamped seals. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid.

d) VIRTUAL PRIVATE NETWORKS

There are two types of IP addresses: public and private. A public IP address is globally unique and only one machine connected to the public Internet can have a public IP address. Private IP addresses are one of the solutions to reduce the exhaustion of IP address space. A private IP address has to be unique only within the set of networks of a particular organization. Larger organizations have sites at different locations in the world. The hosts in the different sites of the organization may be identified with a unique private IP address. But the same set of private IP addresses can be used in the networks of different organizations. Hence, a packet with a private IP address as the destination IP address cannot be used to route packets from one site to another site of an organization through the public Internet. The virtual private network (VPN) technology uses IP-in-IP tunneling to encrypt and encapsulate the IP datagram that has the private IP addresses of the two end hosts with another IP header that has the source and destination IP addresses as the public IP address of the gateway routers for these two private networks. Each organization is required to have one or more gateway routers with a public IP address in order to facilitate communication over the public Internet. As the original IP datagram is encrypted, no intermediate forwarding host in the public Internet can look at the contents of the message.

CONCLUSION

Network security is an important field that is increasingly gaining attention as the internet expands. The crux behind network security is to ensure access to the network and its data for authorized hosts/users and deny access to unauthorized hosts/users. A secure network needs to have tamper-proof communication media and resilient protocol mechanisms that can avoid or reduce the chances of an attack. Hence, it has become a design requirement that in addition to authenticating the application users, it is also essential to authenticate the networks and hosts from which the application users are communicating in the Internet. The network security field may have to evolve more rapidly to deal with the threats further in the future.

REFERENCES

Cryptography and Network Security: Principles and Practice" by William Stallings

Data Communications and Networking (McGraw-Hill Forouzan Networking)

National Institute of Standards and Technology, Advanced Encryption Standard

Network Security: The Complete Reference

R. Anderson, and M. Roe. A5, 1994.

W. Stallings, Cryptography and Network Security: Principles and Practice, Second edition, Prentice Hall, 1999.