Chapter 1

INTRODUCTION

Network and Information security continue to be one of the area that require more attention and improvement in the Information Technology world. This area has become profit making bussiness for hackers. At the same time businesses and many other activities in our everyday lives are becoming more and more dependent on Information Technology. This chapter attempts to give a systematic view of system security requirements and the potential means to satisfy them.

1.1 Network Security Fundamentals

Over the time attackers have become more sophisticated in the methodologies they use to intrude into networks. Securing information is the prime concern today for any network. A security property describes a desired feature of a system with regard to certain types of attacks. Security properties such as confidentiality, integrity, availability, authentication and non-repudiation are the core qualities of any information system. Various security mechanisms can be used to enforce these security properties.

1.1.1 Security Parameters

From Wikipedia, the free encyclopedia: In computer and computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Internet Engineering Task Force(IETF) defines attack in RFC 2828 as:

an assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

According to W. Stallings, Network Security Essentials — Applications and Standards, Prentice-Hall, Englewood, the normal information flow from source to destination and several categories of attacks that target it are shown in Figure 1A.

Interruption: The attacker targets the source or the communication channel and prevents information from reaching its intended destination by modification of data, overloading the link so that the information gets dropped because of congestion or cut the wire. An asset of the systems (hardware or software) gets destroyed or becomes unavailable. Interruption attempt to perform denial-of-service (DOS) attack.

Interception: An unauthorized/authorized party gains access to the information by eavesdropping into the communication channel (e.g., wiretapping).

Modification: The information is not only intercepted, but modified by an unauthorized party while in transit from the source to the destination. By tampering with the information, it is actively altered (e.g., modifying message content).

Fabrication: An attacker inserts counterfeit objects into the system without having the sender doing anything. When a previously intercepted object is inserted, this processes is called replaying.When the attacker pretends to be the legitimate source and inserts his desired information, the attack is called masquerading (e.g., replay an authentication message, add records to a file).

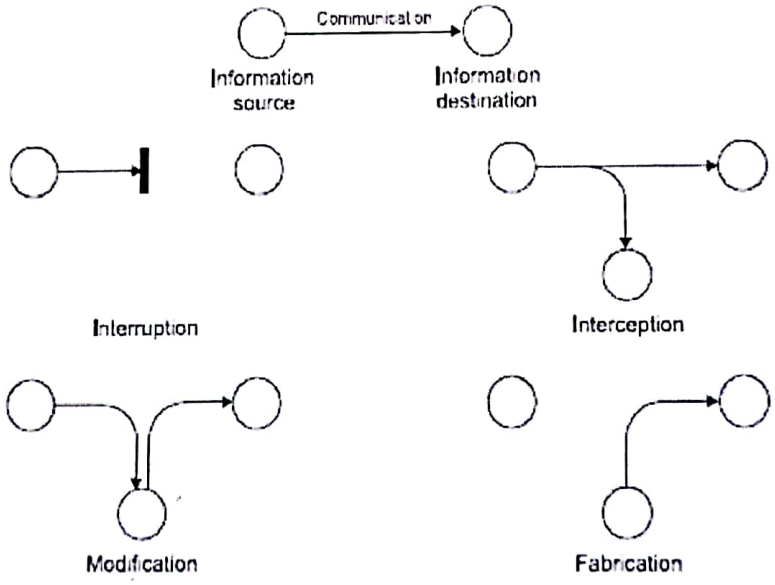

Figure 1A Categories of attacks.

Some of the security parameters are given below:

Integrity: Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people. Thus Integrity refers to methods of ensuring that data is real, accurate and safeguarded from unauthorized user modification. Events like storage erosion, error and intentional data or system damage by employees or hackers can create data changes, hence access control must be provided by access control mechanism of operating systes or data base security etc. Some data might include cryptographic checksums, for verification of integrity. Backups must be available to restore the affected data to its correct state.

Availability is best ensured by rigorously maintaining all hardware, and operating systems environment so that the systems can be accessed by all the users 24/7 hours. For this you can provide adequate communication bandwidth Redundancy, failover, RAID, high-availability clusters and disaster recovery and proxy servers to guard against downtime and firewalls to avoid the denial-of-service (DoS) attacks and network intrusions.

Confidentiality Confidentiality refers to limiting access to information on a resource to authorized people. An attacker that exploits a weakness in a product to access non-public information is compromising the confidentiality of that product. To ensure confidentiality of data you can use User IDs and passwords , Data encryption, two-factor authentication, biometric verification and security tokens, key fobs or soft tokens for access control. The extremely sensitive data can be stored on air gapped computers, disconnected storage devices or, hard copy form only.

Examples: A weakness in a web site that enables a visitor to read a file that should not be read would constitute an security vulnerability. However, a weakness that revealed the physical location of a file would not constitute a vulnerability — although such a weakness could be useful for reconnaissance purposes, and could be used in conjunction with a bona fide vulnerability to compromise files, it would not by itself enable an attacker to compromise data, and thus it would not constitute a security vulnerability.

Non-repudiation Non repudiation is the concept of ensuring that a contract agreed by two users over Internet cannot be later denied by any one of them. This property describes the mechanism that prevents either sender or receiver from denying a transmitted message. Non-repudiation provides assurance of communication and delivery to the clients and server both.

As you can observe, integrity, availability, and confidentiality are the three main goals for security. If one or more of these three elements lacks, there is a security vulnerability. A single security vulnerability can compromise one or all these elements at the same time. For instance, an information disclosure vulnerability would compromise the confidentiality of a product, while a remote code execution vulnerability would compromise its integrity, availability, and confidentiality.

1.1.2 Attack Detection, Avoidance, Prevention, Deterrence, Reaction and Recovery

The different measures that can be initiated to counter the attacks on the security properties are: Attack Prevention, Attack Avoidance and Attack Detection.

Typically attacks are actions aimed to compromise the confidentiality, integrity, and/or availability of a computer or computer network..

Attack Detection: Detection of an attack is the process of monitoring and analyzing the events occurring in a computer system in order to detect signs of security problems. The several dissimilar systems provide unique functions and mechanisms for attack detection with the aim to detect, filter, or prevent system from attack to provide data security and ensure continuity of services provided by a network.

Broadly detection system can be categories in two categories: (i) Host-based (ii) Network-based detection system. Host-based attacks target a computer machine and try to gain access to privileged services or resources on that machine. Network-based attacks make it difficult for legitimate users to access various network services by deliberately occupying or sabotaging network resources and services. According to the detection principle, the attack detection may divide into Signature-based Detection and Anomaly Detection/Signature-based Detection technique looks for patterns and signatures of already known attacks in the network traffic. For example anti-virus software- quick heal secure browse. Active attacks configured automatically, block suspected attacks without any intervention required by an operator. It has the advantage of providing real-time corrective action in response to an attack. Passive system only alerts the operator against attacks and potential vulnerabilities.

Detecting an attack is important for two causes; first the system must recover from the damage caused by the attack and second, it allows the system to take measures to prevent similar attacks in future with the help of intrusion detection systems.

Attack Avoidance: it aims to make the source not viable by an attacker even though the attacker is able to illegally access that resource. An example of security mechanism for attack avoidance is the use of cryptography. Encrypting data renders the data useless to the attacker, thus, avoiding possible threat or application of antivirus for blocking the traffic or firewall to filter the traffic.

Attack Prevention: As like the name it aims to prevent the system from attacks by blocking. To block an attack it is must for a system that system has a complete knowledge of all possible attacks in advance, which is always not possible because of frequently generation of new types of attacks. Firewall is a best example of attack prevention system.

Attack Deterrence: it refer to influence an assailant not to initiate an attack by increasing the perceived risk of negative consequences for the attacker. However. It cover a burly permissible system to help attack anticipation but requires strong evidence against the attacker in case an attack was launched. The digital forensic can be used for this purpose. Various forensic software such as Encase, FTK, ProDiscover etc and hardware tools such as forensic workstations, write blocker etc can be used for computer forensic. You can use network tools such as RegMon, Process Explorer. FileMon, PS tools, Kknoppix Std Tools for network forensic.

Attack Reaction and Recovery: Once an attack is detected, the system must react to an attack and perform the recovery mechanisms as defined in the security policy.

1.1.3 Security Practices

For providing maximum protection against intrusions, organizations employ different security practices. Some of them are described below:

Use Security Software The most important thing you can do to keep your computer safe is to install and maintain security softwares such as an Identity Finder, a tool to help you search for, protection of personal information stored on your computer, file shares, or external media.

Maintain Latest Software and Updates Keep your software updated by applying the latest service packs and patches. The best way to maintain third-party software is to install the Secunia Personal Software Inspector. This will alert you when your current software applications are out of date or require a security update.

Frequently Backup Important Data Back up your data frequently. This protects your data in the event of an operating system crash, hardware failure, or virus attack. UITS recommends saving files in multiple places using two different forms of media (e.g., Cloud Storage, On course Resources, or USB flash drive).

1.2 Vulnerability and Attacks

Security vulnerability is a weakness in a system that could allow an attacker to compromise the integrity, availability, or confidentiality of that system. Security vulnerabilities can be defined as the existence of a weakness, design or implementation error that can lead to an unexpected, undesirable behavior of system. This may lead to compromising security of networks, application or protocol.

Vulnerabilities can be classified as follows:

Design Vulnerability: If the weakness is inherent in the design of the software then these kind of vulnerabilities are difficult to detect and eliminate. A example of these kind of vulnerabilities is TCP/IP protocol stack. The security requirements were not taken into consideration while designing the TCP/IP suite. Many protocols of this stack does not have authentication mechanisms which is the cause of many attacks on Internet.

Implementation Vulnerability: These vulnerabilities are introduced in the hardware or software of the system during Implementation phase. Example of this kind of vulnerability is buffer overflow problem. This causes the system memory to be overwritten breaking down complete system.

Configuration or operational Vulnerabilities: These type of vulnerabilities occur because of misconfiguration or keeping the default configuration on by system administrator. This may result in attacker entering the system as default user or using privileges of system. Disabling unwanted services, allowing weak passwords, not setting authorization permissions are all vulnerabilities of misconfiguration.

1.2.1 Attacks

Anderson defined an intrusion attempt or a threat to be the potential possibility of a deliberate unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable. Headyet al. definition about intrusion says, an intrusion is any set of actions that attempt to comprise the integrity, confidentiality or availability of a resource.

A passive attack is one that can take place by eavesdropping. An active attack is one that requires interaction, such as injecting something into the data stream or change, delete, reroute, add, forge or divert data. The four classes of attacks, namely Interruption, Interception, Modification and Fabrication violate the various security properties of a computer system.

An attack consists of following components.

1. Attack tools: Tools used for performing an attack.
2. Vulnerability: weakness in the system which is to be exploited.
3. security event: after performing attack changes happening in the system.
4. Result of an attack: outcome of an attack. For example modification or deletion of a file.

Attack Models: Attack models can be categorized into two categories: traditional attacks and distributed attacks. Further the traditional model can be classified as one-to-one and one-to-many types. The distributed attacks models can be classified as many-to-one or many-to-many models. Attack leads to violations of the security policies of a computer system, such as unauthorized access to private information, malicious break-in into a computer system, or rendering a system unreliable or unusable.

Attack classification is shown in figure 1.1:

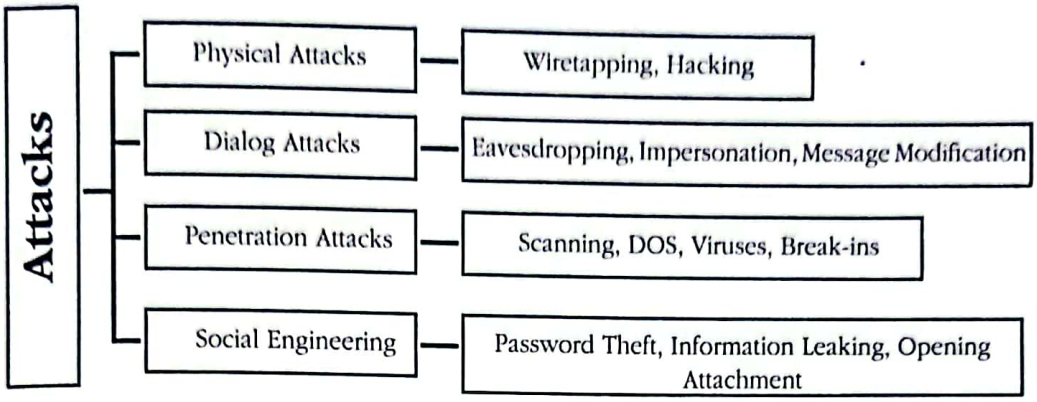

Figure 1.1 Attack Classification

Generally, attacks can be categorized into following types:

1. Passive Attacks: It is aimed at gaining access to penetrate the system without compromising IT resources.
2. Active Attacks: It is aimed at results in an unauthorized state change of T resources.

Attacks are also idendentified by the source cateategory, namely those performed from internal systems (local network), the Internet or from remote dial-in sources. Now, let us see what types of attacks and abuses are detectable (sometimes hardly detectable) by tools to put them in the ad-hoc categorization as below:

Authentication and Authorization Attack(unauthorized access)

- Password cracking and access violation,
- Trojanhorses,
- Stealing information, for example disclosure of proprietary information,
- Taking advantage of system weaknesses to gain access to resources or privileges

Modification Attacks (Unauthorized modification of resources)

- Spoofing of identity example is to get system administrator rights,
- Information modification and deletion
- Unauthorized transmission and creation of data, for example arranging a database ofstolencreditcard numbers on a government computer (e.g. the spectacular theft of several thousand numbers of credit cards in 1999),
- Unauthorized configuration changes to systems and network.

Availability Attacks (Denial of Service (DoS)

- Flooding – compromising a system by sending huge amount so fuseless information to lock out legitimate traffic and deny services:
- Pingflood(Smurf) – a large number of ICMP packets sent to a broadcast address,
- Sendmailflood - flooding with hundreds of thousands of messages in a short period of time; also POP and SMTP relaying,
- SYN flood – initiating huge amounts of TCP requests and not completing handshakes as required by the protocol,
- Distributed Denial of Service (DDoS); coming from a multiple source,

1.3 Defense Mechanisms

There are different types of devices and mechanisms within the security environment to provide a layered approach of defense so that if an attacker is able to bypass one layer, another layer stands in the way to protect the network. Two of the most popular and significant tools used to secure networks are firewalls and intrusion detection systems. The rudimentary functionality of a firewall is to screen network traffic for the purpose of preventing unauthorized access between computer networks.

In this section, we will examine the various types of firewalls and intrusion detection systems, as well as understand the classification of these technologies. This section describes the importance of intrusion detection and prevention, and why they must be a part of every network security administrator's defense plan.

1.3.1 Access Control

Network Access Control (NAC), known as network admission control, is a method of bolstering the security of a proprietary network by restricting the availability of network resources to endpoint devices that comply with a defined security policy.

A traditional network access server (NAS) is a server that performs authentication and authorization functions for potential users by verifying logon information. In addition to these functions, NAC restricts the data that each particular user can access, as well as implementing anti-threat applications such as firewalls, antivirus software and spyware-detection programs. NAC also regulates and restricts the things individual subscribers can do once they are connected. Several major networking and IT vendors have introduced NAC products.

1.3.2 Authentication

Network Level Authentication is a technology used in Remote Desktop Services (RDP Server) or Remote Desktop Connection (RDP Client) that requires the connecting user

to authenticate themselves before a session is established with the server. Originally, if you opened an RDP (remote desktop) session to a server it would load the login screen from the server for you. This would use up resources on the server, and was a potential area for denial of service attacks.

1.3.3 Network Security Devices

To protect the network from the flood of attacks many security devices are designed and being used. Some of the devices are described in detail below:

1.3.3.1 Firewall

A firewall is a software program or device that monitors, and sometimes controls, all transmissions between an organization's internal network and the Internet. A firewall is typically deployed on the network's edge to prevent inappropriate access to data behind the firewall. The firewall ensures that all communication in both directions conforms to an organization's security policy. Firewall technologies are configurable. You can limit communication by direction, IP address, protocol, ports, or numerous other combinations. If you have access to the firewall, you can configure it to enable the ports, protocols, and addresses. In some cases, however, your organization's security policy may prevent optimal streaming. For example, firewalls configured to only allow TCP traffic may cause the user to see frequent buffering of clips. User experience of the presentation is compromised; greater latency and startup times affect the time needed to view the clip, and delivery of the clip requires more total bandwidth.

Typical architecture of firewall is show in figure 1.2 below:

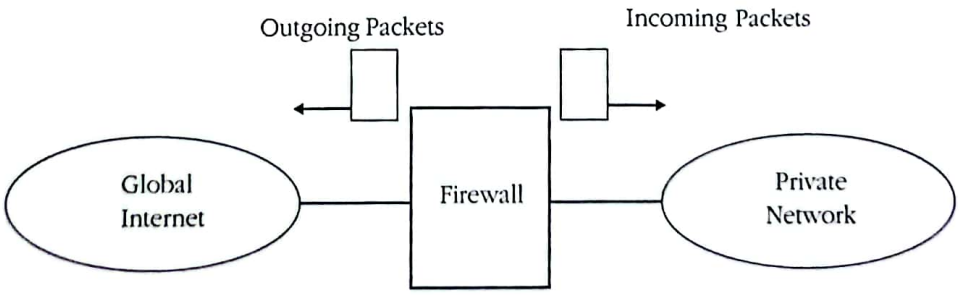

Figure 1.2 Firewall

1.4 Categories of Firewall

There are two categories of Firewall namely hardware firewall and software firewall

1.4.1 Hardware Firewalls

Hardware firewalls can be purchased as a stand-alone product but more recently hardware firewalls are typically found in broadband routers, and should be considered an