Network Security:

Network Security is the protection of Information and systems and hardware that use, store, and transmit that information.

Network Security encompasses those steps that are taken to ensure the confidentiality, integrity, and availability of data or resources

Network Security and its growth are driven by various factors

- Internet Connectivity is 24/7 and is Worldwide.
- Increase in Cyber Crime.
- Proliferation (Increase) of Threats.
- Impact on Business and Individuals
- Sophistication (complexity) of Threats.
- Legislation (law) and Liabilities (legally responsible)

Impact On Business:

Decrease in Productivity

Loss of Sales Revenue

Release of Unauthorized sensitive data

- Threat of Trade secrets or formulas
- Compromise of Reputation and trust
- Threat to environmental and safety systems
- Loss of time

Information Security Goal:

Confidentiality

_ Prevent the disclosure of sensitive information from unauthorized people, resources, and Processes.

Integrity

_ The protection of system information or processes from intentional or accidental modification.

Availability

_ The assurance that systems and data are accessible by authorized users when needed.

Security Catagories:

Information Security

- Protecting Information from Intruders who could possibly harm the state of Information.
- Information in encrypted form is most widely used form of security.

Network Security

- Protecting Information from Intruders during its transmission.
- Protecting Network Services From Intruders is Very Critical and difficult to maintain.

Computer Security

- Protecting system from malicious software, network attacks.
- Generic name for the collection of tools designed to protect data and to prevent hackers
- Keep up a system running.

Internet Security

Measure to protect data during their transmission over a collection of interconnected networks.

Security Attacks => Exploitation of Vulnerability.

Types of Security Attacks.

Passive Attacks
Active Attacks

Vulnerability:

- A network vulnerability is a weakness in a system, technology, product or policy
- Several organizations track, organize and test these vulnerabilities
- Each vulnerability is given an ID and can be reviewed by network security professionals over the Internet.
- The Common Vulnerability Exposure (CVE) list also publishes ways to prevent the vulnerability from being attacked

Security Attack Categorization:

Interruption

This is an attack on availability.

Example : Cutting of a communication line.

Interception

This is an attack on confidentiality.

Example : Wiretapping to capture data in a network.

Modification

This is an attack of Integrity

Example : Changing values in a data file.

Fabrication

This is an attack on authenticity

Example : Insertion of fake messages in a network.

Malicious Program :

- ➢ Most sophisticated type of Threat.
- ➢ Exploits Vulnerabilities by the use of Programs.
- ➢ Categories => According to Replicative behaviour

- ➢ Replicative (Virus, Worm, Zombie)
- ➢ Non Replicative (Trapdoors, Trojan horse)
- ➢ Categories => According to Need of Host Machine
- ➢ Need Host Program (Trapdoors, Logic bombs, Trojan horse)
- ➢ Independent (Zombie)

Virus:

“A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.“

Trojans:

“A Computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Program.”

Logic Bombs:

“A logic bomb is a piece of code that is written intentionally into a software system that will set off a malicious function when specified conditions are met.”

Trojans that activate on certain dates are often called “**Time Bombs”.**

Zombie:

“A bot is a type of malware which allows an attacker to gain complete control over the affected computer. Computers that are infected with a bot are generally referred to as 'zombies’ “.

“Networks of Zombie Computers are referred as Botnets”

Security Services :

Authentication

Assurance that the communicating entity is the one claimed

Access Control

Prevention of the unauthorized use of a resource

Data Confidentiality

Protection of data from unauthorized disclosure

Data Integrity

Service to ensure Integrity (originality) of transmitted message.

Non-Repudiation

Ensuring the denial of receipt and transmission

Interruption

This is an attack on availability.

_ Example : Cutting of a communication line.

Interception

This is an attack on confidentiality.

Example : Wiretapping to capture data in a network.

Modification

This is an attack of Integrity

Example : Changing values in a data file.

Fabrication

This is an attack on authenticity
Example : Insertion of fake messages in a network.

Fundamental Security objectives:

- Four fundamental objectives of Info Security
    - Confidentiality - Protection from unauthorized persons
    - Integrity - consistency of data; no unauthorized creation, alteration or destruction
    - Availability - ensuring access to legitimate users
    - Legitimate use - ensuring appropriate use by authorized users

Client server Security Problems:

- Physical security holes
    - Individual giving unauthorized access to computer
- Software security holes
    - Badly written programs

- Inconsistent usage holes
    - System administrator assembles a combination of hardware and software that is seriously flawed.

Protection Mechanism:

- Trust based security
    - Trust everyone
- Security through obscurity
    - Don’t let others to know about it
- Password schemes
- Biometric systems

Emerging client server Security Threat:

- Threat to client
    - Software agents and malicious code threat
        - Software agent resembles a more traditional virus. It is an executable program that has the ability to move from machine to machine and invoke itself without external influence.
        - Malicious code
            - Virus
            - Trojan horse
            - Worm

Threat to server

- Server security is as important as network security because servers often hold a great deal of an organization's vital information. If a server is compromised, all of its contents may become available for the cracker to steal or manipulate
- Threats to sever consists of unauthorized modification of server data, unauthorized eavesdropping or modification of incoming data packets and compromise of a server system by exploiting bugs in the server software.

- eavesdropping (monitoring packet sent over the network) , DOS (denial of service), packet replay (recording and retransmission of message packet in the network) and modification

Access Controls:

- Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment.

- Access control systems perform authorization identification, authentication, access approval, and accountability of entities through login credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys.

- There are two main types of access control: physical and logical.

- Physical access control limits access to campuses, buildings, rooms and physical IT assets.

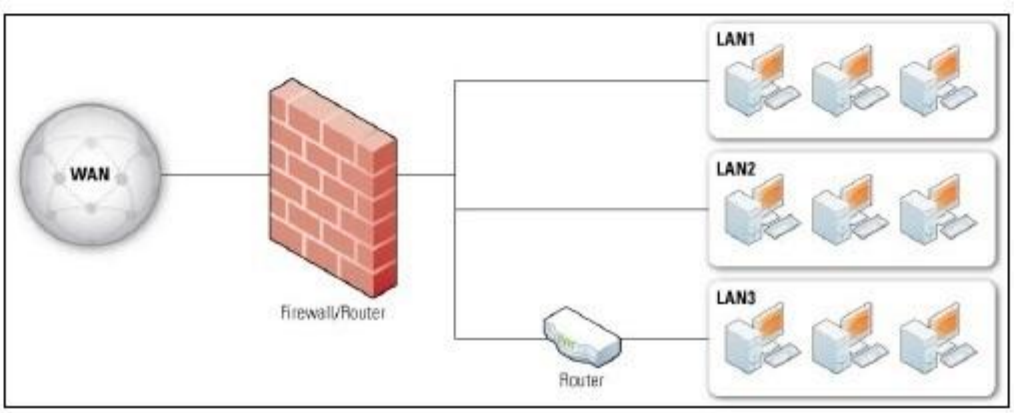
- Logical access limits connections to computer networks, system files and data.

FIREWALL:

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Generally, firewalls are configured to protect against unauthenticated interactive logins from the outside world. This helps prevent hackers from logging into machines on your network. More sophisticated firewalls block traffic from the outside to the inside, but permit users on the inside to communicate a little more freely with the outside.

Firewalls provide an important logging and auditing function; often, they provide summaries to the administrator about what type/volume of traffic has been processed through it. This is an important benefit: Providing this block point can serve the same purpose on your network as an armed guard does for your physical premises.



Simple Routed Network with Firewall Device

Source: National Institute of Standards and Technology

http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

Catagories of Firewall:

Hardware firewalls can be purchased as a stand-alone product but are also typically found in broadband routers, and should be considered an important part of your system and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

Software firewalls are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer.

Types of fire wall:

Network layer firewalls

Network layer firewalls generally make their decisions based on the source address, destination address and ports in individual IP packets. A simplerouter is the traditional network layer firewall, since it is not able to make particularly complicated decisions about what a packet is actually talking to or where it actually came from.

One important distinction many network layer firewalls possess is that they route traffic directly through them, which means in order to use one, you either need to have a validly assigned IP address block or a private Internet address block. Network layer firewalls tend to be very fast and almost transparent to their users.

Application layer firewalls

Application layer firewalls are hosts that run proxy servers, which permit no traffic directly between networks, and they perform elaborate logging and examination of traffic passing through them. Since proxy applications are simply software running on the firewall, it is a good place to do logging and access control. Application layer firewalls can be used as network address translators, since traffic goes in one side and out the other after having passed through an application that effectively masks the origin of the initiating connection.

However, run-of-the-mill network firewalls can't properly defend applications. As Michael Cobb explains, application layer firewalls offer Layer 7 securityon a more granular level, and may even help organizations get more out of existing network devices.

In some cases, having an application in the way may impact performance and make the firewall less transparent. Older application layer firewalls that are still in use are not particularly transparent to end users and may require some user training. However, more modern application layer firewalls are often totally transparent. Application layer firewalls tend to provide more detailed audit reports and tend to enforce more conservative security models than network layer firewalls.

Future firewalls will likely combine some characteristics of network layer firewalls and application layer firewalls. It is likely that network layer firewalls will become increasingly aware of the information going through them, and application layer firewalls have already become more transparent. The end result will be kind of a fast packet-screening system that logs and checks data as it passes through.

Proxy firewalls

Proxy firewalls offer more security than other types of firewalls, but at the expense of speed and functionality, as they can limit which applications the network supports.

Why are they more secure? Unlike stateful firewalls or application layer firewalls, which allow or block network packets from passing to and from a protected network, traffic does not flow through a proxy. Instead, computers establish a connection to the proxy, which serves as an intermediary, and initiate a new network connection on behalf of the request. This prevents direct connections between systems on either side of the firewall and makes it harder for an attacker to discover where the network is, because they don't receive packets created directly by their target system.

Proxy firewalls also provide comprehensive, protocol-aware security analysis for the protocols they support. This allows them to make better security decisions than products that focus purely on packet header information.

Firewall Security Policies:

- Administration with the responsibility of designing,specifying and implementing or overseeing the installation of a fire wall must address a number of management issue before installation.
- Managers must be clear about the security policies of the organization for examaple whether their companys firewall is in place to to deny all services except interneto rnet connection or to provide a metered and auditied method of regulating access to the internet in a nonthreatening manner.
- Managers must be aware of the level of monitoring ,redundancy and control in the functioning of the firewalls.

- Managers must make a checklist of what firewalls should monitor,permit and deny.
- Firewall policies must be realistic reflection of the level of security in the entire network.
- Finally managers need to keep in mind that firewalls are not always impenetrable.

Transaction Security:

- Transaction security has become a high profile concern because of the increase number of merchants trying to do commerce online.
- Consumer confidence in the reliability and protection of business transactions against third party threats must be enhanced before electronic commerce can succeed.
- Unsure of security consumers are unwilling to provide credit card payment information over the internet.
- In order to allay consumer consumer fear and protect to confidential data on public network companies are starting to pay greater attention to transaction privacy , authentication and anonymity
- Transaction privacy,confidentiality and integrity are the main barriers to the widespread acceptance of electronic commerce.
- The five internet security requirements are
    a. Privacy : the ablity to control who see or cannot see information and under what terms.
    b. Authenticity: The ability to know the identies of communication parties.
    c. Integrity: The assurance that stored or transmitted information is unaltered.
    d. Availability: The ability to know when information and communication services will or will not be available.
    e. Blocking: The ability to block unwanted information or intrusions.

Types OF online transaction:

The type of transaction depends on the type of data or content being sent across the network . the different catagories of data are

a. Public data : no security restrictions and read by any one
b. Copyright data: copyrighted but no secrete

c. Confidential data: content is secrete but the existence of the data is not secrete.

d. Secrete data: secrete data and must be keep confidential

Requirements for transaction Security:

- Transaction Confidentiality
  -
- Transaction integrity
  - The assurance that stored or transmitted information is unaltered
- Transaction privacy
  - The ability to control who sees information and under what terms

Encryption:

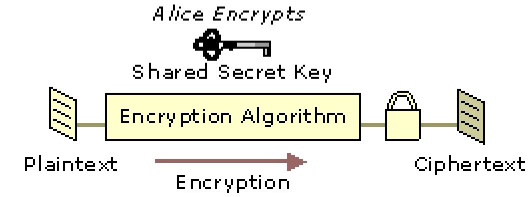
Encryption is the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties.

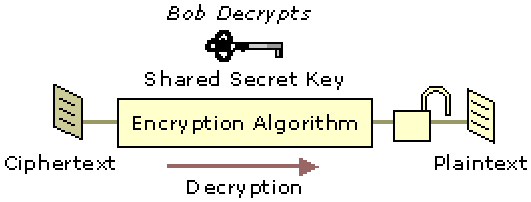
The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the Internet or other computer networks. Modern encryption algorithms play a vital role in the security assurance of IT systems and communications as they can provide not only confidentiality, but also the following key elements of security:

- Authentication: the origin of a message can be verified.
- Integrity: proof that the contents of a message have not been changed since it was sent.
- Non-repudiation: the sender of a message cannot deny sending the message.

Symmetric Encryption

- Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.



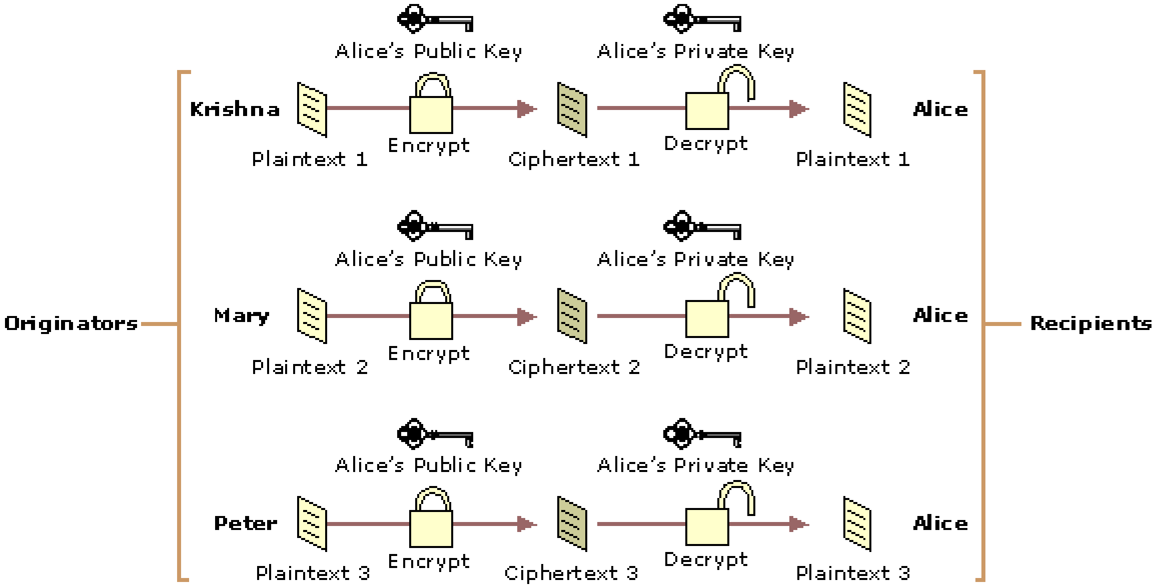


Asymmetric Encryption

- The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.

  Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

  This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

- 
Alice's Public Key
Alice's Private Key
Krishna
Plaintext 1
Encrypt
Ciphertext 1
Decrypt
Plaintext 1
Alice
Alice's Public Key
Alice's Private Key
Originators
Mary
Plaintext 2
Encrypt
Ciphertext 2
Decrypt
Plaintext 2
Alice
Recipients
Alice's Public Key
Alice's Private Key
Peter
Plaintext 3
Encrypt
Ciphertext 3
Decrypt
Plaintext 3
Alice