**Network Security**

**Network Security**

Network Security is a security provided to a network from unauthorized access and risks. It is the duty of network administrator to adopt preventive measures to protect their network

OR

Network Security is protection of the access to files and directory in a computer Network against hacking misuse and unauthorized changes to the system

**Need for securing a network**

1. First is the security of the data information i.e. to protect the information from unauthorized access and loss
2. Second is computer security i.e. to protect data and to thwart hackers.

**Principle /Goals of network security**

1. Authentication
2. Confidentiality
3. Integrity
4. Availability
5. Non-Repudiation
6. Access Control

Authentication

*It is process of confirming a user or computer’s identity.*

Confidentiality

*Data confidentiality implies keeping data private. Data should be transfer from sender to receiver in encrypted form.*

Integrity

*Data ensures that data has not been modified in transit. Also, a data integrity solution might perform origin authentication to verify that traffic in originating from the source that should be sending it.*

Availability

*The availability of data is a measure of the data’s accessibility*

*Example – He could send improperly formatted data to a networked device, resulting in an unhandled exception error.*

Non – Replication

*After a message has been send and received, the sender and receiver should not be able to deny about the sending and receiving of the messages respectively.*

Access Control

*The term “access” involves writing, reading, executing and modifying. Thus access control determines and controls, who can access what. It regulates, which user has access to a resource.*

**Types of Attacks**

1. Passive Attack
2. Active Attack

Passive Attacks

The main goal of the passive attacks is just to gather information and not to do any alteration (Modification) to the message or harm the system resources.

In passive attack the sender and receiver remain unaware that the message contents have been read by other party.

Active Attack

In an active attack, an attacker (intruder) alters the original message or creates a fake message. This attack tries to affect the operation of system resources.

**Classification of Active Attacks**

1. Masquerade

*In such type of attack an unauthorized entity tries of gain more privileges that is authorized for. Masquerading is generally done by using stolen ID’s and password.*

1. Reply

*This active attack involves capturing or copy of the message send by the original sender and transmitting it later to bring about an unauthorized result.*

1. Modification of Messages

*This attack involves making certain modification to the captured message, or delaying or recording the message to cause an unauthorized effect.*

1. Denial of Services

*This attack prevents the normal functioning or proper management of communication facilities.*

*For example :- A network server can be overloaded by unwanted packages, thus resulting is performance degradation. DOS attack can interrupts and show down the services of a network.*

**Common types of Cyber Crimes**

1. Hacking

*A hacker is an unauthorized user who attempts to or gains to an information system. Hacking is an attack in to the privacy of data. Types of hackers are Black Hats Hacker, White Hats Hacker, Gray Hats Hacker, Phreakers.*

1. Cyber Stalking

*This crime involves use of internet to harass someone. The behavior includes false allegation, threats, etc.*

1. Spamming

*Spamming is sending of unsolicited bulk and commercial message over the internet.*

1. Phishing

*It is a criminally fraudulent process of acquiring sensitive information such as username, passwords and credit card details by disquishing as a trustworthy entity in an electronic communication*

1. Software Piracy

*It is an illegal reproduction and distribution of software for business or personal use. This is considered to be a type of violation of copyright and a violating of a license agreement.*

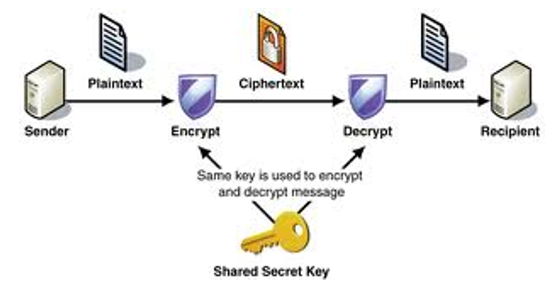
**Spoofing**

A person can pretend to be someone else. For example, a person can pretend to have the email address [jdoe@example.net](mailto:jdoe@example.net) or a computer can falsely identify itself as site called [www.example.net](http://www.example.net) .

**Types of encryption**

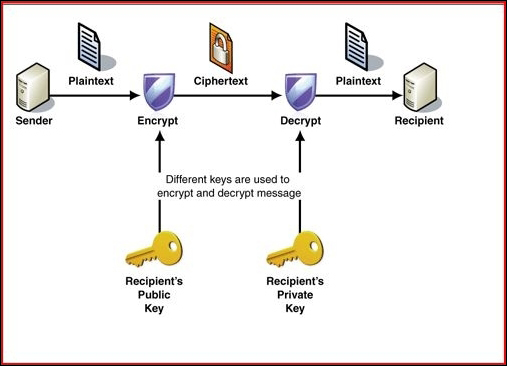
1. Symmetric Encryption

*With symmetric encryption cryptography, both the sender and recipient share a key is used to perform both encryption and decryption.*

**

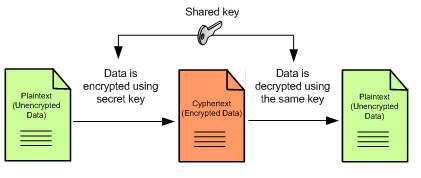
1. Asymmetric Encryption

*With asymmetric encryption cryptography (also known as public key cryptography), the sender encrypt data with one key and recipient uses a different key to decrypt cipher text. The encryption key and its matching decryption key are often refers to as a public / private key pair*

**

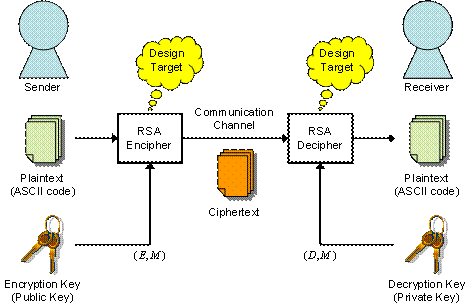
**DES (Data Encryption Standard)**

Data encryption standard is the block cipher which takes a fixed-length string of plain text bits and transforms through a series of complicated operation into another cipher text bit string of the same length.

**

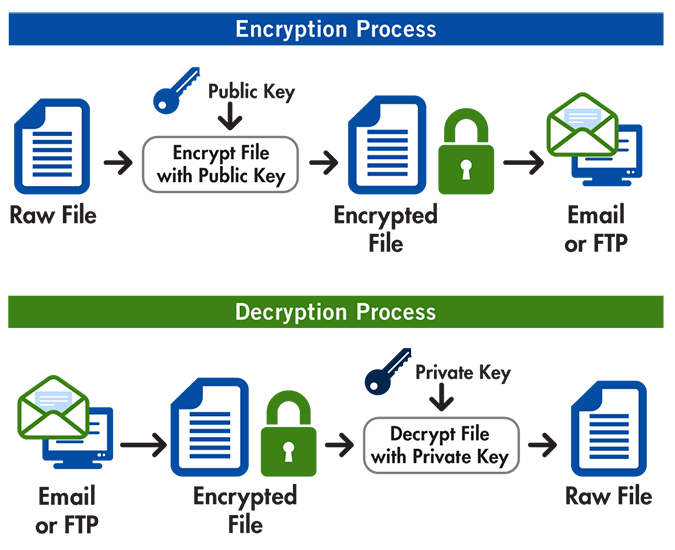
**RSA Encryption**

RSA encryption also is widely used such as for emails and files encryption system called PGP (Pretty Good Privacy). RSA use Asymmetric encryption



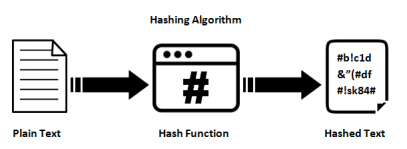
**PGP Encryption**

PGP is a popular program used to encrypt and decrypt email over the internet as well as authenticate message with digital signatures and encrypted stored files.



**Hashing**

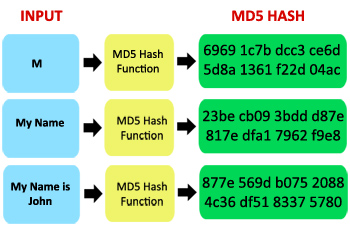
Hashing is kind of process, signature, function which is responsible for translating information into a cryptic values.



**MD5**

Message Digest Algorithm 5 take up a random data as an input and generate a fixed size hash value as the output.

The input data can be of any size, but output hash value size is always fixed.



**SSL Certificate**

It is a security protocol. SSL (Secure Socket Layer) is a standard security technology for establishing an encrypted link between a server and a client – typically a web server (website) and a browser; or a mail server and mail client (eg. Outlook).

**Secure Shell (SSH)**

Secure Shell is a program to log into another computer over a network to execute commands in a remote machine, and to move files from one machine to another.

It provides strong authentication and secure communication over insecure channels such as internet.

**Digital Signature**

The digital signature is a simply a procedure which generates the authenticity and integrity of messages and documents exchanged over the internet. The digital signature fulfills the following requirements: -

1. Authenticity
2. Non-repudiation
3. Integrity

**Digital Certificate**

The Digital Certificate similar to identification cards such as passwords and driving licenses. Identification cards are issued by recognized government authorities.

**What makes up a Digital Certificate**

Digital Certificate contains : -

1. The person’s name
2. An email Address
3. A serial number
4. A public key
5. An expiration date
6. A digital signature (Encryption)

**IPSEC Security features**

1. Authentication
2. Integrity
3. Confidentiality – conceals the message content through encryption

**Virus**

Virus is a program that can be broken into three functional parts

1. Replication – *some way to reproduce or duplicate itself*
2. Concealment – to facilitate replication, a virus must have one or more methods of masking (to hide) its existence.
3. Bomb -

The combination of these three attributes makes the collective program as virus

**Worm**

A computer was considered an application that could be replicated itself via a permanent or dialup network connection.

**Trogen Horses**

A Trogen Horse is an application which performs an activity that the user is unaware of this hidden application is what make a Trozan Horse.

Trogen Horse does not replicate or attack itself to other files. Trogen Horse had its bomb included from the original source code.

**Preventive Measures**

1. Access Control
2. Checksum
3. Process Monitoring

**Types of virus scanner**

1. On-demand
2. Memory Resident

**Heuristic Scanner**

A Heuristic Scanner does not compare code with a signature file as a virus scanner does. It uses a grading system to determine the probability that the program code being analyzed is a virus.

**VPN (Virtual Private Network)**

A VPN is a secure communication connection which is carried over an insecure public network.

VPN use advanced encryption and ‘tunneling’ technology to establish secure, end-to-end private network.

**Functions of VPN**

1. Authentication
2. Authorization
3. Confidentially
4. Data Integrity
5. Data Encryption

**Types of VPN**

1. Remote Access VPN

A remote access allows individual users to establish secure connection with a remote computer network.

A example of a company that needs a remote access VPN is a large firm with hundreds of sales people.

1. Site to Site VPN

A site-to-site VPN allows offices in multiple fixed locations to establish secure connection with each other over a public network Such as the internet. There are two types of site-to-site VPN

1. Intranet Based
2. Extranet Based

**Backup**

Keeping duplicate copy of your data has always been the best way to protect against disaster corruption or loss.

1. Tape Backup
2. Full Backup
3. Incremental Backup

Incremental backup copy to tape only files that have been recently added or changed

Sunday – full

Monday – from(Monday to Monday)

Tuesday – from(Tuesday to Tuesday)

1. Differential Backup

Sunday – full

Monday – from(Sunday to Monday)

Tuesday – from(Sunday to Tuesday)

**Offences and Penalities**

|  |  |  |  |
| --- | --- | --- | --- |
| **Cyber Crime** | **Brief Description** | **Relevant Section in IT Act** | **Punishments** |
| Cyber Stalking | Stealthily following a person, tracking his internet chats. | 43, 65, 66 | 3 years, or with fine up to 2 lakh |
| Intellectual Property Crimes | Source code Tampering, piracy, copyright infringement etc. | 65 | 3 years, or with fine up to 2 lakh |
| Cyber Terrorism | Protection against cyber terrorism | 69 | Imprisonment for a term, may extend to 7 years |
| Cyber Hacking | Destruction, deletion, alteration, etc in a computer resources | 66 | 3 years, or with fine up to 2 lakh |
| Phishing | Bank financial Frauds in Electronic Banking | 43, 65, 66 | 3 years, or with fine up to 2 lakh |
| Privacy | Unauthorized access to computer | 43, 66, 67, 69, 72 | 2 years, or with fine up to 1 lakh |

**Ways to Protect System from Hacking**

Here are seven simple, effective steps that network administrators can take to protect their systems.

* Implement a firewall
* Develop a corporate security policy
* Install anti-virus software
* Keep operating system up to date
* Don’t run unnecessary network services
* Conduct a vulnerability test
* Keep informed about network security

**Firewall**

A firewall is a hardware or software system that prevents unauthorized access to or from a network. It 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. All data entering or leaving the intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria. The criteria is normally the rules defined by the ALC (Access Control List) made by the administrator of the network.

A firewall sits at the junction point or gateway between the two networks.