Output of the verification is compared signature component 'r' of the values match if said signature is valid because only the sender processing its private key can generate valid signature for the document.

Wide Lam Protocol

→ It is a computer network authentication protocol that allows 2 parties to verify each other identity

→ It uses a trusted key Distribution centre (KDC) & symmetric key cryptography to negotiate b/w the parties.

→ variants: Symmetric key & public key

→ Susceptible to various security flaws

→ Inefficient compared to alternative authentication protocols.

→ ~~It works~~

Fermat's Theorem

Statement: If p is prime no. & a is an integer such that a is not divisible by p then

$$a^{p-1} = 1 \pmod{p}$$

Explanation: This theorem is a fundamental result in modular arithmetic.

→ It states that raising any integer a to the power p-1 will leave remainder of 1 when divided by p provided a and p are coprime.

eg $a = 3, \quad p = 7$

$3^{7-1} = 3^6 = 729$

$729 \bmod 7 = 1$

729 when divided by 7 gives remainder = 1

Application: often used in cryptography, especially in modular arithmetic computations

Euler's Theorem

It states that for any integer 'a' and for any positive integer 'n' such that 'a' is coprime to 'n' & $\phi(n)$ is the no. of positive integers ($\leq n$) that are coprime to n then

$$a^{\phi(n)} = 1 \bmod (n)$$

$\phi(n)$ = Euler's totient Function.

$$= n\left(1-\frac{1}{n}\right)\left(1-\frac{1}{y}\right)\left(1-\frac{1}{z}\right)$$

$$n = x^p y^{q_2 r}$$

eg Use Euler's remainder theorem to find the remainder when 2^{70} is divided by 15.

Δ

$$a^{\phi(n)} = 1 \bmod n$$

$a = 2$, ~~$\phi(n) = 70$~~, $n = 15$

$$n = x^p y^{q_2 r} = 3 * 5$$

$\phi(n) = n\left(1-\frac{1}{4}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$= 15\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$\phi(n) = 15\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 8$

Now, $2^8 = 256$

on dividing 2^{70} by 15

$2^{70} = (2^8)^8 \cdot 2^6 = 1^8 \cdot 64 = 4 \bmod 15$

Remainder is 4.

15 | 64 | 4
60
4

Q. Explain Pretty Good Privacy

Ans It is an encryption software program designed to ensure confidentiality, integrity and authenticity of virtual communications & information.

→ It based on a combination of symmetric encryption, public key cryptography and hashing

Following services are offered by PGP:-

1) Authentication - means something that is validate something as true or real.

→ To login into some sites we give our account name and password, that is an authentication verification procedure.

→ In emails, authentication has to be checked as there are some people who spoof the emails or some spams which causes lot of inconvenience → By signing messages with sender's private key, it offers recipient with a means to verify the authenticity of verbal exchange.

Confidentiality - In emails, only the sender and receiver should be able to read the message. , that means the contents have to be kept secret from every other person except the 2.

→ Confidentiality facilitated via encryption protect content material of messages from unauthorized access.

Steps on ~~Sender Side~~ taken by PGP to create secure email

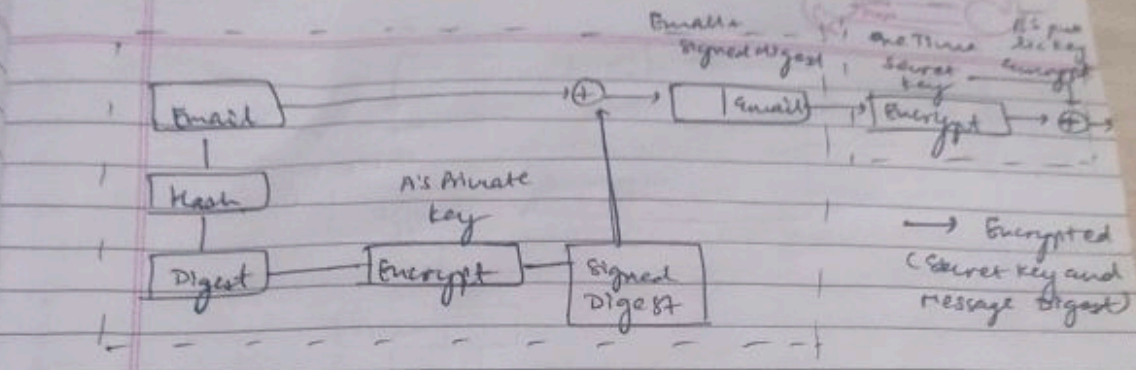
① email msg is hashed using hashing function to create a digest.

② The digest is then encrypted to form signed digest by using sender's private key and then it is added to the original email msg.

③ Original msg & signed digest are encrypted by using one time secret key created by sender.

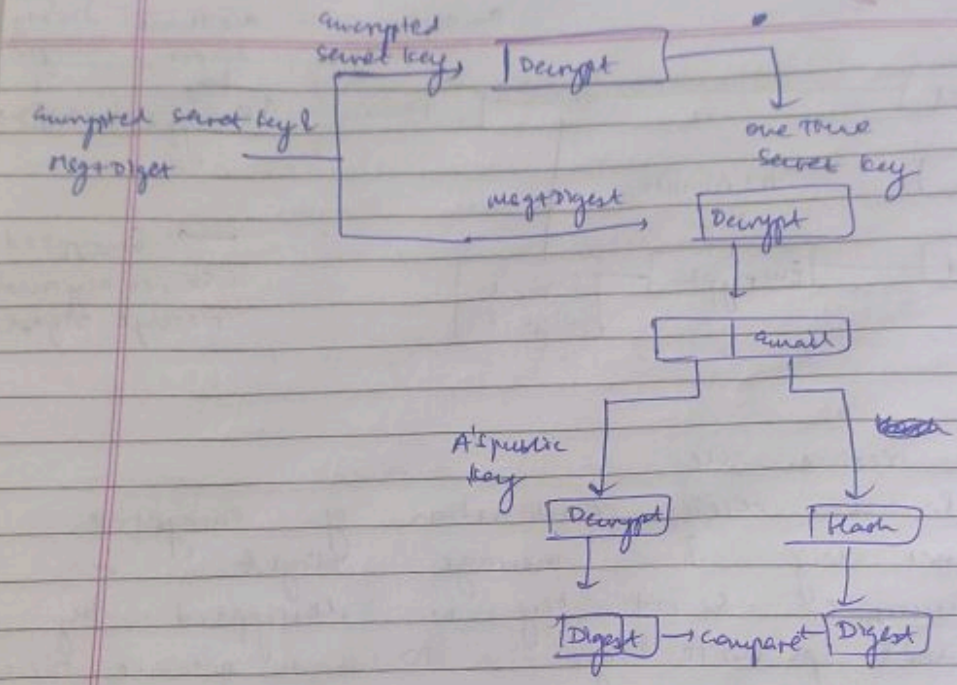
④ The secret key is encrypted by using receiver's public key.

⑤ Both the encrypted secret key & encrypted combination of msg and digest are sent together.



At receiver side

1. Receiver receive combination of encrypted secret key & message digest.
2. Encrypted secret key is decrypted by receiver's private key to get one time secret key.
3. Secret key is then used to decrypt the combination of msg & digest
4. The digest is decrypted by using sender's public key and signed msg is hashed using hash func. to create a digest.
5. Both the digests are compared if both are then are equal means all the aspects of security are preserved.



Kerberos

.) Draw its name from greek mythology where 3 headed dog safeguard entry of gate.

.) Similarly, Kerberos services is supposed to have 3 components - authentication, accounting, audit. It is intented to protect network gate of an organization

.) Out of the 3 components, authentication is primarily implemented and ∴ Kerberos is mainly treated as an authentication service.

.) Developed at MIT.

.) In Kerberos, AS authenticates users and servers

Thus, users upon authentication can utilize services of server or server can provide services to authenticated users.

- Kerberos, though a complex protocol, relies on symmetric encryption instead of asymmetric encryption.
- It treat user and system used by user differently.
- User authentication is not considered system authentication because of the following
  (i) A user may pretend as another user while functioning from a system
  (ii) Impersonating a system is possible by changing MAC or IP address.
  (iii) Eavesdropping of msgs to exchanged b/w system and server is possible.
- Kerberos consider distributed client/server environment where users prove their identity to server by entering correct password and then invoke desired service.
- Servers system also prove their identity to ~~server~~ ~~by entering~~ correct password communicating clients.
- It imposes following requirements :-
  → It should be secure enough such that finding info for impersonation is not possible
  → Kerberos system should be highly reliable such that upon failure of Kerberos server, another backup server may be used.
  → Highly scalable at large no. of

→ no. of clients and servers can participate
→ Based on Needham and Schroeder protocol
→ Both users and servers trust kerberos for mutual authentication.
→ It is also used as a KDC for distributing keys securely to users.
→ ARCHITECTURE

① KDC :- trusted 3rd party who shares secret key with all users.
→ This helps in reducing no. of shared keys.
→ Otherwise for N user communication keys, required are of the order O(N²)
i.e for 6 users $6(6-1) = 15$ keys are required whereas using KDC only 6 keys are required.
→ 2 components:

~~Session Key~~:

AS: play role of KDC. All users register with AS who keep a database of user identities and their corresponding passwords. Main functionality of AS is to verify users via passwords and provide session key to be used ahead b/w user & TGS. It also provide ticket granting ticket to user.

TGS :- issues service granting tickets & session key to the user upon request. Service granting tickets are used to request service from real server while session key is used to protect session b/w user & server.

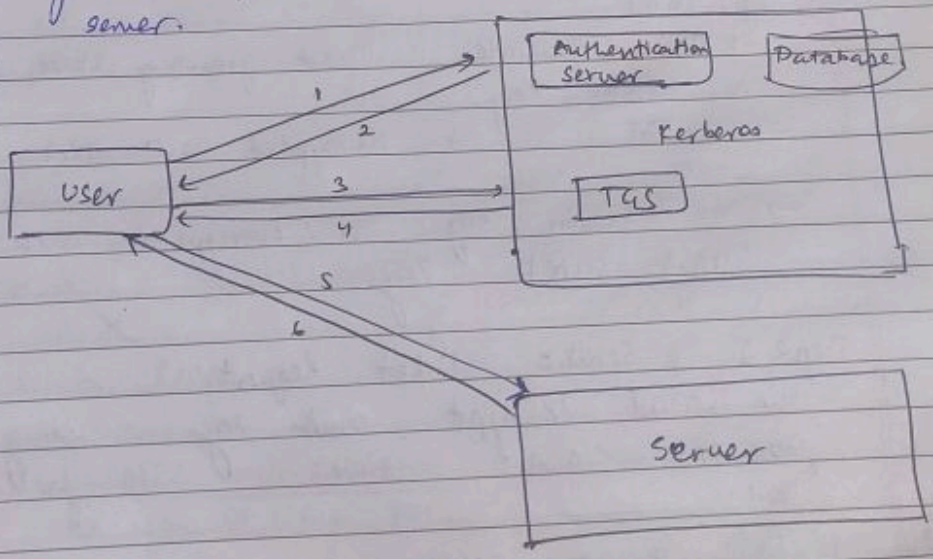
In case user wants to contact more than 1 server for different services, he has to contact TGS more than once for different tickets for diff services.

Real Server: provides actual services like Print, FTP, file, etc. to the users.

Kerberos uses 2 kinds of tickets -

1) Ticket granting Ticket provided by AS to user for request and authentication at TGS

2) Service granting Ticket :- provided by TGS to user for request and authentication at real server.



(2) Client : User or Device requesting access to a service

1) Runs Kerberos client software to interact with the KDC.

Database : A secure database within KDC that store user and service credentials.

Server : Host who services the client wants to access. Validate client using service granting tickets issued by TGS

Certification Mechanism

Step 1: Initial authentication

1. Client sends plaintext authentication request to AS.
2. AS verify client's credentials in the KDC database.
3. If valid:
   → AS generate Ticket granting Ticket & a session Key
   → TGT is encrypted with TGS secret Key.
   → Session key is encrypted with client secret Key

Step 2 : Service Ticket Request

1. The client decrypt session key using its password and store TGT for future use.
2. To ~~access~~ access a service, client sends TGT, a request for service ticket.
3. TGS decrypt TGT using its secret key and validate the request
4. If valid:

SET, Web security, 802.11 services, IKE

→ TGS issues service granting ticket & session key to the users upon request.

Step 3: Accessing the service

1. Client sends service granting ticket to and an authenticator to the service server.
2. The SS:
   → decrypts service ticket using its secrete key
   → validate authenticator using session key
3. If valid, SS grant access to the requested service.

Authenticator: A timestamp encrypted with the session key used by client to prove its identity

Advantages

1. Prevent Password Transmission - reducing risk of interception
2. Mutual authentication : preventing impersonation attack
3. Session Based - Do not re enter password every time.
4. Centralized authentication - Centralized control and management by KDC
5. Scalability - scalable for large company with many users.

Challenges & limitation

1) Single point of failure - KDC is critical, if compromised the entire network fails.
2) Time Synchronization - If used out of sync, authentication fails.
3) Initial Trust - Password weak, security at risk.

IP Security Policy

Determined primarily by the interaction of 2 databases:

(i) Security Association Database (SAD)
(ii) Security Policy Database (SPD)

Security Association - One way logical connection blw sender and Receiver that ~~offer~~ provide security services to the traffic carried on it. It is a set of shared security attributes blw 2 nlw entities that enable secure communication SA include following information:

(i) Security parameters: a specific set of security parameters that are related to a type of traffic.
(ii) IP addresses: of the communicating parties.
iii) Security Parameter Index (SPI): unique identifier A bit string, SPI enable receiving system to select SA. 32 bit no. that uniquely identify

SPI remains same as the packets need to travel SA.

SA for a connected device in computer nw. It is determined during SA negotiation on the hosts. It is placed in IPsec header (on by GSP) so that receiver SAD may identify SA for this packet from SPD.

- It is a table that stores information on SAs for IPsec security services.
- SA is a one way connection b/w 2 entities that provides security services to a flow traffic carried on it.
- SAD entries define how a specific communication session is protected, including encryption and authentication mechanisms.

Contents of SAD entry:

(i) SPI:
(ii) IP sec Protocol: Specify whether the SA uses AH or Encapsulating Security Payload.
(iii) Encryption Algorithm: Details of the cryptographic algorithm (eg: AES)
(iv) keys: encryption & authentication keys used for securing traffic
v) Lifetime: Specify for how long SA is valid.
vi) Sequence NOs: Protect against replay attacks.
vii) mode: Specify whether SA operates in transport or tunnel mode.

SAD:- set of SA's put together in a DB termed as SAD. It is basically a matrix with each row having single SA.
2 Types: Inbound, Outbound SAD.

SA kept in SAD is uniquely identified by
(i) SPI (ii) Dest. address - of DA of the host (public router system) firewall (router). Thus, SA's are unique per DA
(iii) Protocol - IPsec Protocols = AH or ESP

Security Policy Database Description

- Higher level database that specifies how and what security services applied to IP packets.
- It differentiates b/w traffic that is to be IPsec protected and traffic that is allowed to bypass IPsec.
- It determines how to handle traffic
- SPD entries are rules that map traffic flows to security actions.

contents

(i) Selectors: Match criteria for traffic including SIP & DIP, protocol (eg. TCP, UDP, ICMP), port nos

(ii) Actions: Specifies how to handle matched traffic
Protect - Apply an SA for encryption, & authentication, or both.
Bypass - allow traffic to pass without security
Discard: block traffic entirely.

(iii) Priority determine order of rule evaluation.

- SP in IPsec implies the type of security to be applied to the IP packet upon arrival or departure
- SP is kept in a SP Database
- Each entry in SPD is indexed based upon selectors: SA, DA, Name, Protocol, Source Port, Dest. Port.

Web Security

SSL :- concerned with providing security services to application that uses TCP as its underlying protocol and hence runs b/w TCP & Application. Its internet standard version : TLS.
∴ Protocol is commonly referred as SSL/TLS

SET :- Secure electronic Transaction.
It is used for securing credit card transactions.

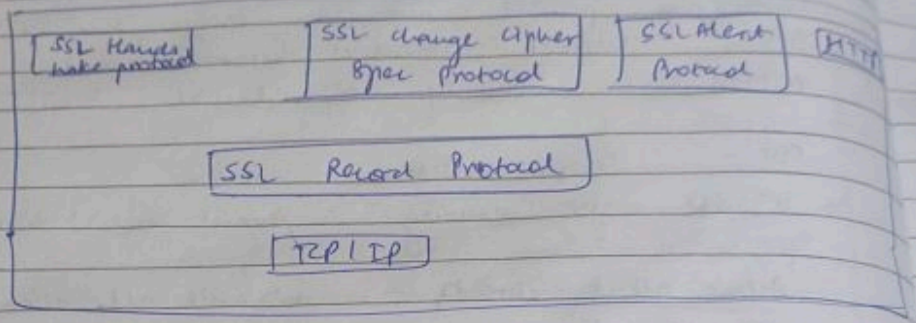
Active attack threats :- Website alteration, msg alteration b/w client and server, user impersonation, etc.

Passive attack threats :- Eavesdropping on web traffic, restricted website information leakage.

SSL :- one of the most popular web security mechanisms

- Implemented as a TL security service.
- Originally developed by Netscape.
- Its version 3 (SSLV3) was designed by taking public and industry input.
- It uses TCP to provide reliable end to end services
- It does not use represent a single protocol but various protocols at 2 layers
- 3 higher level protocols that manage SSL exchanges exists as a part of SSL :-

Handshake Protocol, Change cipher spec Protocol, Alert Protocol.



SSL Protocol Stack

(iii) SSL Handshake Protocol :- is used b/w client and server before sending any data for the following purposes:-

(i) Server and client authentication to each other
(ii) Negotiation b/w client and server for deciding encryption & MAC algorithms.
(iii) Negotiation of cryptographic keys to be used for encryption & MAC calculations.
(iv) Protocol msg has 3 fields: Type (1B), length (3B), content (≥0)

(i) SSL change cipher spec protocol : simplest among the three SSL specific protocols utilizing SSL Record Protocol.

→ It has a single msg having single byte which is initialized to 1.

→ Main intention is to update cipher suite of the connection.

SSL Alert Protocol It is meant for conveying alerts to the peers. Alert msgs are compressed and encrypted in accordance with the current connection state

→ The Alert Protocol msg has 2 Bytes. First byte indicate level of alert i.e it conveys severity the message.

→ 2nd Byte is used to indicate specific alert via codes.

SET

Secure Electronic Transaction

- Provides Security Specifications describing set of security protocols and formats for credit card transactions over the Internet
- Provide 3 services: secure communication trust and privacy
- As many parties are involved during communication, SET uses secure communication channel b/w them for securing data exchange.
- It uses X.509v3 DC for providing trust.
- It provides information to only trusted parties involved in the transaction for enhancing privacy

Key Features:

① Information Confidentiality: In SET, DES symmetric encryption is used to protect purchasing info. from access by others.

→ Cardholder Account and other details.

(ii) Payment information
(iii) Cardholder's credit card no.

Data integrity: For protecting the payment info. sent from the cardholders to the merchants by any alterations, SET use either RSA or SHA-1

Cardholder account authentication: SET enables merchants to verify that a cardholder is a legitimate user of a valid cr. no. SET uses X.509 v3 DC with RSA signature for this purpose.

Merchant authentication: SET enables cardholders to verify that merchant has a financial relationship with a financial institution allowing it to accept payment cards.

Same point.

Dual Signature

→ One of the major requir. of SET is that customer's order info should not be visible to the bank and payment info (customer's credit card no) should not be visible to merchant.

→ For this requirement, SET introduce concept of dual signature.

- DS is used to OR 2 messages of 2 different recipients. (Bank & Merchant)
- Message corresponding to order info. is sent to the merchant and msg corresponding to payment info is sent to the bank.

The following are ensured -

(i) Bank remains unaware of details of customer's OI. & merchant of remains unaware of details of PI.

(ii) Customer privacy is enhanced by keeping OI & PI separate.

(iii) OI & PI are linked to each other and hence can be used under dispute cases.

Calculating DS :-

Process of purchasing goods and services is initiated by the customer who takes individual hashes of PI & OI, concatenates them and takes hash of the resultant. Final hash is encrypted with customer's private key and this finally encrypted hash is formed as DS

$$DS = E_{K_c}\left[H\left(H(PI) \| H(OI)\right)\right]$$

Needham Schroeder Protocol

Symmetric Protocol

(Alice) Bob

A initiates communication to B. S is server trusted by both parties.

Protocol can be specified as follows:

(i) $A \rightarrow S : A, B, N_A$

Alice send msg to the server identifying herself and Bob, telling server that she wants to communicate with Bob

(ii) $S \rightarrow A : \langle N_A, K_{AB}, B, \langle K_{AB}, A \rangle_{K_{BS}} \rangle_{K_{AS}}$

Server generate K_{AB} (symmetric generated Key which will be the session key of the session (b/w A and B) and sends back to Alice a copy ~~under~~ encrypted under K_{AS} for Alice to forward to Bob and also a copy for Alice.

Nonce assures Alice that the message is fresh and the server is replying to that particular message and the inclusion of Bob's name tells Alice ~~[illegible]~~ who she is to share the key with

(iii) $A \rightarrow B : \langle K_{AB}, A \rangle_{K_{BS}}$

Alice forward key to Bob who decrypt it using the keys he shares with the server thus authenticating the data

(iv) $B \rightarrow A : \langle N_B \rangle_{K_{AB}}$

B send A a nonce encrypted under K_{AB} to show that he has the key

A → B : $\langle K_{AB} \cdot Y \rangle_{K_B}$

A perform a simple encryption operation on nonce re-encrypts it and sends it back verifying that B is still alive and holds the key.

Denning improvement

Denning identified a vulnerability in NS symmetric key protocol, specifically related to replay attacks. If an attacker records old msg K_{AB}, then he can replay msg $\langle K_{AB}, A \rangle_{K_B}$ to Bob who will accept it, being unable to tell that the key is not fresh.

Improvement: Introduce timestamp in the protocol to ensure freshness of the msgs.

•) Server include Timestamp in its response and TS is checked by both parties.

This ensures that even if attacker replay old msgs they will be rejected due to expired TS.

Kehn's Improvement

ensure mutual authentication enhance NS protocol to against replay and man in the middle attacks. and protecting

key changes :- include an explicit MAC msg authentication code a to validate each ste

$\langle N_A, K_{AB} \rangle_B$

A → B:

a

IPSec (srPdf)

- IP sec provides authentication and confidentiality to the packets at network layer.
- IPSec is useful as security provided at higher layers i.e application & transport layer are not apparent in few cases :-
  (1) PGP & S/MIME provides security only to Email applications and not to all client/server applications. Thus, IPSec is useful to such applications.
- IPSec can be implemented in firewall or routers. It can also be implemented in the end systems.

Benefits of IPSec

- It analyse all the incoming traffic to an organization from outside world and can filter the undesired ones.
- IPSec protect routing mechanisms providing associations b/w routers such as that an attacker can't cause harm to any routing mechanism.

Malicious Programs

① Backdoor – an unauthorized entry point in any software module that is known to the person who created it.

② Logic Bombs – condition based malicious activity by a code

③ Trojan Horse – is a program that allow hackers to gain remote access to a target system.

→ It is mainly used for debugging and testing purpose.
→ During debugging and testing, it sometimes becomes essential to avoid unnecessary authentications.
→ It may also happen that authentication procedure goes wrong.
→ Under all cases, backdoor proves to be an effective measures.
→ It provides entry into the system without going through the normal authorization or hashing the security checks.
→ It recognize user ID or sequence of inputs.
→ Thus, backdoor provides a secret entry by someone who is aware of it.

6/10/3

Logic Bombs is a software threat that is embedded into some other legitimate program and have remain unnoticed.

→ It gets activated upon meeting some conditions like presence or absence of certain files, a particular user who is running the application.

→ Upon activation, logic bombs tried to meet its intended purpose which may range from alteration or deletion of data or entire files to rebooting a machine.

Trojan Horse - comes through genuine software upgrade and usually seems useful.

→ But as a hidden side effects, it contain hidden code that perform unwanted or harmful function.

→ Thus, it is a method through which unauthorized user could accomplish task that otherwise could not be performed directly by him.

→ Most common tasks - propagation of virus or worm, backdoor installations, deletion of data

→ It is a program that allow hackers to gain remote access to a target system

Worms self replicating programs that spread across the n/w due to poor security of infected computers.

→ Like virus worm is a program but unlike virus it does not require another program for propogation i.e it replicates itself and sends its replicas on d n/w connection.

→ For sending replicas on other capabilities like email, remote login may be utilized

→ A worm may even implant Trojan horse programs

→ Characteristics of worm are similar to virus: it has a dormant phase, propogation phase, triggering phase, execution phase

→ For propogation, worm search for addresses of other systems that can be infected,

→ It enumerates host tables of these systems and tries to establish a connection with the identified system.

→ Identification is followed by copying itself onto that system and then executing that copy

→ If a system is previously infected then it is not selected for infection.

→ A worm may conceal itself by changing its name or properties eg. it may change itself as a system process.

→ Hence, worms are diff. to deal with

Virus

→ Software component that causes infection to other programs and insert its replica during modification of host program.
→ The infected program further repeats this process for propogating virus and modifying other programs.
→ The viruses are usually spread by normal users who can't be suspected.
→ It usually takes advantages of the weakness of the system during its existence.
→ Virus is a sys. dependant entity.

4 phases of virus life cycle

① Dormant Phase : virus remains idle and shows no activity. The virus gets activated when stimulated by some trigger like presence of corrupted file, etc and enters next phase.
Not necessary for every virus to have this phase.

2) Propogation Phase - virus makes replicas of itself and insert into correct files on the disk. The virus is injected programs further enter into this phase & replicates

③ Triggering Phase – virus gets activated with some trigger for action and virus its intended purpose. Triggers include – count of no. of copies of virus becoming greater than some threshold value, etc

④ Execution Phase – Virus complete its func in this phase. During execution, depending upon its functionality, virus may or may not damage files or programs.

Computer virus has 3 parts:

① Infection mechanism – process through which virus spread or replicates.

② Trigger – event or condition for the payload to activate.

③ Payload – main virus functionality. Payload may involve harmful activity.

If a single program gets infected, virus is in a position to cause infection to other executable files on that system. Thus, virus should be protected from gaining entry into the system.

Types of viruses

(1) Parasitic virus - most commonly found virus and requires a host program. It gets attached to the running files and then makes copies of itself which then attacks other on going programs.

(2) Memory Resident virus - It resides in the main memory of the system. From there it attacks almost every running prog which exists in the main memory.

(3) Boot sector virus - It resides in the boot sector of any disk and spreads whenever a infected disk is used to boot a system.

(4) Stealth virus - Stealth is a technique in which infected virus not is designed to fool anti virus software i.e designed in such a way that anti virus software can't detect virus.

(5) Polymorphic virus - Polymorphic means more than one form. Such virus change its appearance in every infection due to which their detection becomes impossible