| Worms | Virus | Bacteria |
|---|---|---|
| An independent program that can replicate itself and often spreads to different sites over a network. | **Virus** is a type of malicious software program that spreads through computer files without the user's knowledge. | programs that duplicate themselves. |
| >It does not need another program to spread itself.<br>>does not attack other programs or files.<br>>it consumes network resources and can shutdown the network | >It needs a host program to replicate.<br>>It inserts copies of itself into other programs.<br>>It executes when the infected program runs.<br>>It can cause harm to the system and its files. | >Bacteria programs copy themselves.<br>>Copies run to replicate again.<br>>Growth is exponential.<br>>They consume all system resources. |

Intrusion detection: is the process of identifying unauthorized or unusual activities in a system using audit records.

Firewall: it monitors and controls data traffic between a private network and the internet, deciding to allow or block connections based on its configuration.

Profiles: define normal behavior between subjects and objects to detect and report abnormal activities.

- Logon and Session Activity: Audit records show the user (subject), log-on location (object), and actions like log on/off.
- Command or Program Execution: Audit records show the user (subject), program name (object), and execution action, with measures like frequency, resource use, and denied executions.
- File Access Activity: Audit records show user actions (read, write, create, delete, append) on files.

## Security Concepts:

1. Identification: Users are identified to a computer or an application through a user-id.
2. Authentication: the process used to verify the identity claimed by the user.
3. Authorization: the process of assigning access rights to each user (ID).
4. Access Control: the process of enforcing access rights for network resources.

5. Confidentiality: the process used to protect secret information from unauthorized disclosure.
6. Data Integrity: allows detection of unauthorized modification of data , it detects whether the data has been modified during transmission.
7. Non-repudiation: the capability to provide proof of the origin of data or proof of the delivery of data.
8. Denial of Service: one in which the attacker takes over or consumes a resource so that no one else can use it.

## Authentication method:

- Something unique to the user, like fingerprints or voice patterns, verified by comparing with system data.
- Something the user has, such as keys or badges, used to verify their identity.
- Something the user knows, like a secret password known only to the user and the system.

**Access control:** is the regulation of user access to resources based on a security policy, such as access to files, databases, or system settings.

**Capability List**: defines the access rights a subject has to specific objects, such as files or devices. Each subject has its own list.

**Access rights:** Define how a subject can access the object. Access rights are specified for each pair of subjects and objects.

**Audit Trail:** Records important events for later review, such as repeated login attempts by an intruder.

## Audit Requirements:

1. Automatically collects information on all security-sensitive activities.
2. Stores information in a standard record format.
3. Creates and saves audit records automatically without administrator intervention.
4. Minimally impacts normal system operation and performance.
5. Protects audit logs under a security scheme.

**One-Time Passwords Using Token Cards:** One-time passwords (OTP) are single-use passwords generated by token cards that become invalid after use.

## One-way hash function:

Used to detect errors during data transmission by generating a fixed-size checksum from data of any size. It is easy to implement in hardware and software.

## Requirements:

1. Applies to data blocks of any size.
2. Produces a fixed-size digest (usually 128 or 160 bits).
3. Simple to implement in hardware and software.

## Client:

A program and operating system that interacts with the user, prepares requests for access server, communicates with the server, and analyzes data to present to user

## Server:

provides one or more services like databases or image processing, responds only to client requests, does not initiate communication on its own, and may communicate with other servers .

**Encrypted Message:** Used to protect the content of the message from unauthorized access.

**Digital Signature:** Verifies the sender's identity and ensures the message has not been altered.

**Decrypted Signature:** Uses the public key to verify the validity of the signature.

**Message Digest:** A short representation of the message content used to detect any modifications.

**ACL:** An Access Control List ACL for a given object defines the access rights for each subject.

**Anomaly Records:** Created when behavior deviates from the normal profile.

**Encryption:** is the process of converting data into an unreadable form that can only be recovered using decryption and a key.

- The original data is called plaintext, and the encrypted data is called ciphertext.

**asymmetric:** uses one key for encryption and a different but related key for decryption.

**symmetric :** uses the same key for encryption and decryption

**private key :** every user has two keys, a private key (known only to the user)

**public key :** each user is published in yellow pages or made available through other means (known to every one).

# Attack Types