Unidad 4:
Seguridad y Protección en Sistemas Operativos.

Tema 7,

Seguridad en Sistemas Operativos:

7.1 Amenazas a la seguridad de un sistema.
7.2 Seguridad en el uso de recursos y servicios.
7.3 Seguridad en el acceso al sistema.
7.4 Seguridad en el uso de redes.
7.5 Seguridad en Sistemas Operativos.

7.1 Amenazas a la seguridad de un sistema.

- Introducción:
  - Seguridad de la información debido a:
    - *Expansión de los ordenadores.*
    - *Uso de Sistemas Distribuidos y Redes.*
  - Diferenciación entre Seguridad y Protección:
    - **Seguridad (política):**
      - ¿Qué accesos son permitidos?.
      - ¿Qué usuarios tienen que tener qué accesos a qué recursos?.
    - **Protección (mecanismo):**
      - ¿Cómo controlar los accesos?.
      - Proporcionar los medios para llevar a cavo las políticas de seguridad.
  - Generalización del término **“Seguridad”.**
  - Mecanismo flexible para albergar políticas.

7.1 Amenazas a la seguridad de un sistema.

- **Requisitos a cumplir por el sistema:**
  - **Confidencialidad:**
    - Los elementos del sistema sólo serán visibles por aquellos grupos autorizados.
  - **Integridad:**
    - Los elementos del sistema sólo serán modificados por los grupos autorizados.
  - **Disponibilidad:**
    - Los elementos del sistema sólo estarán disponibles para grupos autorizados.

- **Elementos amenazados:**
  - Hardware.
  - Software.
  - Datos.
  - Líneas de comunicación.

7.1 Amenazas a la seguridad de un sistema.

- Elementos del sistema a los que afecta la seguridad:

Elemento	Confidencialidad	Integridad	Disponibilidad
Hardware			Robo o sobrecarga de equipos, eliminando el servicio
Software	Realización de copias no autorizadas del software	Alteración de un programa en funcionamiento haciéndolo fallar durante la ejecución o haciendo que realice alguna tarea no pretendida	Eliminación de programas denegando el acceso a los usuarios
Datos	Lecturas de datos no autorizadas. Revelación de datos ocultos de manera indirecta por análisis de datos estadísticos.	Modificación de archivos existentes o invención de nuevos	Eliminación de archivos, denegando el acceso a los usuarios
Líneas de Comunicación	Lectura de mensajes. Observación de la muestra de tráfico de mensajes.	Mensajes modificados, retardados, reordenados o duplicados. Invención de mensajes falsos.	Destrucción o eliminación de mensajes. Las líneas de comunicación o redes se hacen no disponibles.

7.1 Amenazas a la seguridad de un sistema.

- Aspectos en que se agrupa la seguridad:
  - **1. Seguridad en el uso de recursos y servicios: control de acceso.**
    - Utilizar un mecanismo de control de acceso a los recursos que tan sólo permita el acceso si existe el permiso correspondiente.
  - **2. Seguridad en el acceso al sistema:**
    - Asegurar que sólo entran los usuarios autorizados.
  - **3. Seguridad en el uso de redes:**
    - Evitar que se puedan producir escuchas y alteraciones en los datos que viajan por la red.

7.2 Seguridad en el uso de recursos y servicios.

- **Evolución del control de acceso a recursos y servicios:**
  - Ninguna protección: ej, MS-DOS.
  - Protección de recursos básicos:
    - Memoria, ficheros, modo usuario/supervisor.
  - Protección de servicios generales del sistema.
  - Protección de servicios proporcionados por los propios usuarios:
    - Arquitecturas cliente/ servidor.

- **Situación actual:**
  - **Heterogeneidad en la protección:**
    - Base de computación fiable grande.
    - “Agujeros” por interacción no prevista entre mecanismos.
  - **Inseguridad en distribución:**
    - Falta de protección para interoperabilidad de objetos distribuidos.
    - Pocas y malas soluciones de seguridad.

7.2 Seguridad en el uso de recursos y servicios.

- Principios de Diseño de un Sistema de Seguridad:
  - **Mínimo Privilegio:**
    - Los derechos de acceso deben adquirirse sólo por permiso explícito; por omisión el acceso no debe estar permitido.
  - **Ahorro de Mecanismos:**
    - Lo más simples y pequeños como sea posible.
  - **Aceptación:**
    - No deben interferir excesivamente en el trabajo de los usuarios.
  - **Mediación Total:**
    - Cada acceso debe ser cotejado con la información de control.
  - **Diseño abierto.**

7.2 Seguridad en el uso de recursos y servicios.

- Modelos de protección:
  - **Modelo de matriz de acceso como principal modelo de protección:**
    - **Filas: clientes.** **Columnas: recursos.**
    - M[i,j]: permisos del cliente i sobre el recurso j.
    - Dos implantaciones de la matriz:
      - **Lista de control de acceso (por columnas):**
        - Cada recurso guarda la lista de clientes con sus permisos.
      - **Capacidades (por filas):**
        - Cada cliente guarda la lista de capacidades (recursos+permisos) que tiene disponibles.

7.2 Seguridad en el uso de recursos y servicios.

- **Control de acceso:**
  - **Mecanismo de control de acceso con LCA:**
    - Cuando un cliente realiza una petición sobre un recurso.
      - El SO (protección) comprueba si el cliente está en la LCA del recurso.
    - Mecanismo usado por Unix y Windows para el control de acceso a ficheros.
    - **Inconvenientes de la LCA:**
      - **Falta de escalabilidad:**
        - Muchos clientes ⇒ LCA muy grandes.
        - Muchos recursos ⇒ muchas LCA.
      - **Solución:**
        - Agrupar los clientes ⇒ disminuye el nº de entradas de la LCA.
        - Agrupar recursos ⇒ disminuye el nº de LCA.
  - **Mecanismo de control de acceso con capacidades:**
    - Cuando un cliente realiza una petición sobre un recurso.
      - El cliente presenta la capacidad sobre el recurso.
      - El SO (protección) comprueba si en la capacidad existe permiso para la operación solicitada (similar a una entrada de cine).

7.3 Seguridad en el acceso al sistema.

- **Amenazas a la seguridad en el acceso al sistema:**
  - Intrusos.
  - Programas malignos.

- **Intrusos:**
  - **Piratas o hackers:** individuos que acceden al sistema sin autorización.
  - **Los sistemas presentan agujeros** por donde los hackers consiguen colarse.
  - **Técnicas de intrusión:**
    - Averiguar contraseñas (más del 80% de las contraseñas son simples).
    - Probar exhaustivamente.
    - Decifrar archivo de contraseñas.
    - Intervenir líneas.
    - Usar caballos de Troya.

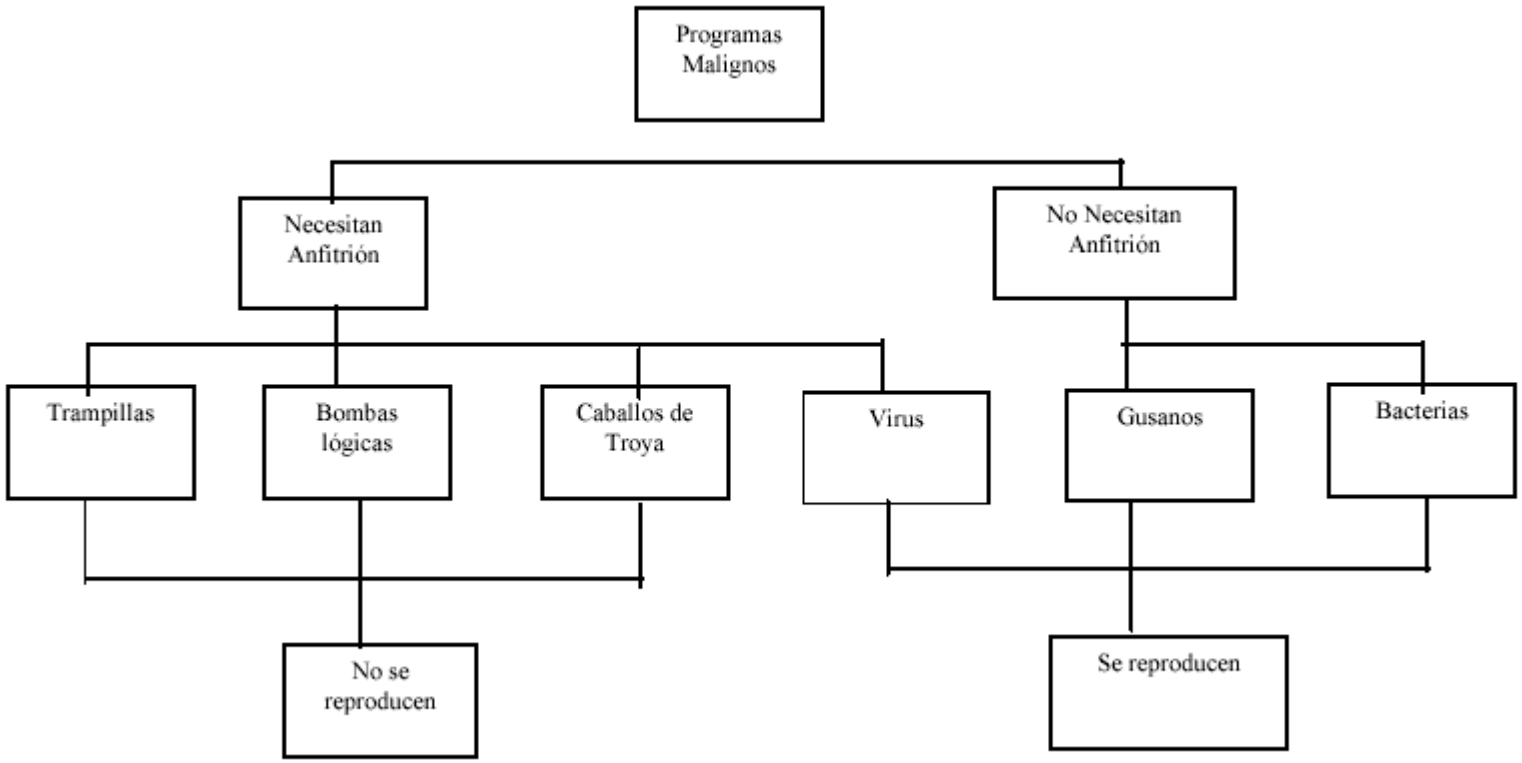
7.3 Seguridad en el acceso al sistema.

- Técnicas de prevención de intrusos:
  - Establecer una buena estrategia de elección de contraseñas:
    - Contraseñas generadas por ordenador (difícil memorización).
    - Inspección activa (proceso periódico de averiguación).
    - Inspección proactiva (decidir si es buena en su creación.

- Técnicas de detección de intrusos:
  - Investigar actividades inusuales:
    - Detección de anomalías estadísticas.
      - Uso de registros de auditoría que recogen información del comportamiento de cada usuario.
    - Detección basada en reglas.
      - Conjunto de reglas empleadas para decidir si una actividad es inusual.

7.3 Seguridad en el acceso al sistema.

- Programas malignos:



7.3 Seguridad en el acceso al sistema.

- Programas malignos que necesitan anfitrión:
  - Forman parte de un programa.
  - **Trampillas:**
    - Punto de entrada secreto a un programa.
    - Se usan para depuración y prueba.
    - Pueden usarse para acceso no autorizado.
  - **Bomba lógica:**
    - Se ejecutan cuando se cumplen ciertas condiciones.
    - Ej: se borra el disco duro si programador no está en nómina.
  - **Caballo de Troya:**
    - Código dañino incrustado en programa que se ejecuta cuando se ejecuta el programa.

7.3 Seguridad en el acceso al sistema.

- Programas malignos que no necesitan anfitrión:
  - **Gusanos:**
    - Programas independientes.
    - Se reproducen a través de la red.
    - Además de propagarse pueden causar daños.
  - **Bacterias:**
    - No dañan explícitamente.
    - Su único objetivo es reproducirse.
    - Se reproducen exponencialmente agotando la capacidad del procesador.

7.3 Seguridad en el acceso al sistema.

- Programas malignos:
  - **Virus:**
    - Código incrustado en un programa.
    - Se reproducen e insertan en otros programas.
    - Pueden causar daños.
  - **Algoritmo de virus muy simple (tan sólo se reproduce):**
    - Encontrar 1ª instrucción de un ejecutable del disco.
    - Sustituirla por salto a posición siguiente a la última instrucción.
    - Insertar copia del código de virus (este algoritmo) en dicha posición.
    - Hacer que el virus simule la instrucción sustituida por el salto.
    - Saltar a la segunda posición.

7.4 Seguridad en el uso de redes.

- Tipos de amenazas:
  - **Amenazas pasivas:**
    - Revelación del contenido del mensaje.
    - Análisis del tráfico:
      - En caso de que los mensajes vayan encriptados.
      - Determinar las máquinas que se comunican y la frecuencia y longitud de los mensajes.
  - **Amenazas activas:**
    - Alteración del flujo de mensajes.
    - Privación del servicio:
      - Impide el uso normal de los servicios de comunicaciones.
    - Suplantación:
      - Cuando una entidad finge ser otra diferente.

7.4 Seguridad en el uso de redes.

- Cifrado de datos:
  - Transforma un mensaje original en otro ilegible.
  - **Algoritmos de cifrado:**
    - Transforman un objeto ocultando el contenido del mismo.
    - **Tipos de algoritmos:**
      - **Sustitución:** Cambian parte del texto original por otro texto.
        - Monoalfabéticos: Cambian cada carácter por otro símbolo.
        - Homofónicos: Sustituye cada letra por un código de una lista de códigos asociados (para evitar el análisis de frecuencias).
        - Polialfabéticos: Cambian cada carácter por otro dependiendo de la posición.
      - **Permutación o Trasposición:** Reordenan la estructura del objeto.

7.4 Seguridad en el uso de redes.

- Cifrado de datos:
  - **Claves:**
    - Patrón que usan los algoritmos de cifrado y descifrado para manipular los mensajes en ambos sentidos.
    - Añaden más seguridad a los algoritmos de cifrado.
    - Hay que recuperar el objeto original cifrado.
  - **Tipos de algoritmos atendiendo a sus claves:**
    - **Simétricos (o de clave privada):**
      - Función de descifrado inversa de la de cifrado.
      - Emisor y receptor comparten la misma clave.
      - Problema: Distribución de claves.
    - **Asimétricos (o de clave pública):**
      - Claves distintas para cifrado y descifrado.
      - Clave de cifrado: pública; clave de descifrado: secreta.
      - Cualquiera puede mandar un mensaje cifrado.
      - Sólo el propietario de la clave de descifrado puede hacerlo.

7.4 Seguridad en el uso de redes.

- Cifrado de datos:
  - **Aplicaciones de los sistemas simétricos:**
    - **Privacidad de la comunicación.**
      - Clave de cifrado pública y de descifrado privada.
    - **Autentificación del origen (firmas digitales).**
      - Clave de cifrado privada (firma) y de descifrado pública.
    - Se pueden combinar ambos aspectos:
      - Encriptar el mensaje a enviar.
      - Firmarlo digitalmente y enviarlo.
      - Al recibirlo se verifica la firma y se desencripta.

7.5 Seguridad en Sistemas Operativos.

- **Seguridad en Linux**:
  - Autenticación de usuarios ante el sistema.
  - Configurable sin modificar la aplicación.
  - Homogénea para todos los servicios.

- **Seguridad en Windows NT:**
  - **Logon:** Ventanas de diálogo.
  - **Autoridad de seguridad local:** Controla permisos de acceso al sistema. Gestiona servicios de autenticación, política de auditoria y registro de eventos auditados.
  - **Gestor de cuentas de usuario:** mantiene la DB de usuarios y grupos. Proporciona servicios de validación de usuarios.
  - **Monitor de referencia de seguridad:** Control de acceso de usuarios a los objetos, verificando permisos, aplicando políticas de seguridad y generando eventos para registros de auditoría.