Tema 6 - Mecanismos de seguridad

- ▼ Seguridad en un SO
  - ▼ Definición
    - Conjunto de mecanismos/políticas/controles que permiten proteger recursos de sistema frente a accesos no autorizados
  - ▼ Objetivos
    - Garantizar confidencialidad, integridad y disponibilidad
    - Evitar pérdida de datos
    - Controlar privacidad de datos
    - Controlar acceso a recursos y datos
- ▼ Políticas de seguridad
  - Conjunto de reglas abstractas que definen qué acciones están permitidas o prohibidas
- ▼ Mecanismos de seguridad
  - Implementaciones técnicas dentro del SO que permiten hacer cumplir las políticas de seguridad de forma automática y verificable
- ▼ Problemas de seguridad
  - ▼ Físicos
    - Desastres naturales y relacionados con la instalación
    - Rotura de elementos
    - Accesos físicos no autorizados
  - ▼ Lógicos
    - ▼ Usuarios descuidados/malintencionados
      - Claves poco seguras
      - Sesiones abiertas sin supervisión
      - Borrados accidentales/malintencionados

- Programas con errores
- Uso indebido/malicioso de programas

▼ Tareas del SO

▼ Autenticación

- Verificación de identidad de usuario o proceso antes de prmitir acceso al sistema
- Asociación de todas las acciones realizadas en el sistema a una identidad específica
- Almacenamiento de credenciales de forma segura (evitando su exposición directa)

▼ Autorización

- Determinar qué acciones pueden realizar un usuario autenticado sobre los recursos del sistema
- Principio de mínimo privilegio → cada usuario o proceso debe tener únicamente permisos estrictamente necesarios

▼ Control de acceso

- Evaluación de si un sujeto tiene permiso para realizar una acción sobre un proceso

▼ Elementos

- Sujeto → usuario/proceso
- Objeto → archivo/memoria/dispositivo
- Operación → leer/escribir/ejecutar

▼ Modelo

▼ DAC

- Permisos definidos por propietario de recurso

▼ MAC

- Sistema aplica políticas centralizadas y etiquetas de seguridad

▼ RBAC

        - Permisos asignados en función de roles organizacionales

▼ Seguridad de sistema de archivos

- SO controla estrictamente acceso a archivos y directorios

▼ Elementos

- Permisos de lectura/escritura/ejecución
- Propietario y grupo
- Listas de control de acceso (ACL)

▼ Aislamiento de procesos

- Cada proceso se ejecute en su propio espacio de memoria
- Impide que un proceso acceda o modifique el estado interno de otro → menor impacto de errores y ataques

▼ Protección de memoria

- Evita accesos no autorizados a direcciones de memoria

▼ Mecanismos

- Paginación
- Segmentación
- Bits de protección

▼ Modo usuario

- Ejecución de aplicaciones
- Acceso restringido a determinadas aplicaciones

▼ Modo kernel

- Ejecución de SO
- Control total de hardware

▼ Llamadas al sistema

- Única vía controlada mediante la cual las aplicaciones pueden solicitar kernel
- SO valida cada solicitud → evitan accesos directos y peligrosos al hardware

- ▼ Seguridad del kernel
  - Protección contra modificaciones no autorizadas y ejecución de código malicioso
  - ▼ Mecanismos
    - Protección de memoria del kernel
    - Verificación de módulos
    - Firmas digitales
- ▼ Auditoría y registro de eventos
  - SO registra eventos relevantes para seguridad
  - Detección de incidentes
  - Análisis de ataques
  - Cumplimiento de normativas
  - Accesos fallidos
  - Cambio de permisos
  - Uso de privilegios
- ▼ Actualizaciones y parches de seguridad
  - Actualizaciones que corrigen vulnerabilidades del SO
  - ▼ Sistema sin parches → altamente vulnerables
    - Atacantes suelen explotar fallos públicos y documentados
- ▼ Secure Boot
  - Verifica integridad de software durante arranque
  - Sólo se ejecuta software confiable → protección frente a rootkits y malware persistente

▼ Técnicas de diseño de sistemas seguros

- ▼ Separación de recursos
  - Física → usando distintas plataformas hardware
  - Temporal → restricción de acceso a determinados recursos en determinadas franjas horarias

    - Criptografía
    - Lógica → creación de espacios lógicos separados para los procesos
- Entornos virtuales
- Diseño por capas con distintos niveles de confianza
- Mecanismos de recuperación