Sistemas Operativos
Tema 10

Seguridad y Protección

UNED

Manuel Fernández Barcell

http://www.mfbarcell.es

@gavilanetc

Introducción

- Seguridad de un sistema informático
  - Es más general ya que involucra consideraciones legales, políticas, administrativas y técnicas
- Protección del sistema informático
  - Se refiere a aspectos internos del sistema, como los mecanismos de protección que suministra el sistema operativo

10.2 Seguridad de un Sistema Informático

- Objetivos de la seguridad
  - Confidencialidad
    - Los datos almacenados en un sistema informático solo deben ser leía por aquellos usuarios autorizados por el usuario propietario de los datos.
  - Integridad
    - El contenido de los datos almacenados en un sistema informático únicamente puede ser modificados por su propietario y por los usuarios autorizados por él.
      - Se incluyen las operaciones de escritura, borrado, cambio de estado y creación.
  - Disponibilidad.
    - Los recursos del sistema deben encontrarse disponibles para los usuario autorizados.

Políticas de seguridad

- El conjunto de reglas que especifican
  - Qué usuarios pueden acceder al sistema y bajo qué restricciones,
  - Cómo se puede leer y escribir la información del sistema, y
  - Cuáles son los flujos de información permitidos dentro del sistema.
- Políticas de seguridad de **control de acceso discrecional**
  - Son definidas por el propietario de un recurso y especifican cuáles son los derechos de acceso de los restantes usuarios a dicho recurso
- Políticas de seguridad de **control de acceso obligatorio**
  - Son definidas a nivel de diseño del sistema y regulan el acceso y el flujo de información dentro del mismo
- En un sistema pueden existir varios niveles de seguridad o autorización.
  - Cada recurso tiene asignado un determinado nivel de seguridad
- La selección de las políticas de seguridad más adecuadas para un sistema informático debe realizarse después de evaluar los posibles riesgos y el coste de lograr un determinado nivel de seguridad

Autenticación de usuarios

- Autenticación de usuarios que permitan identificar a los usuarios autorizados y denegar el acceso al sistema a los intrusos
- Mecanismos de autenticación se basan en alguno de los siguientes
  - Elementos que debe poseer el usuario
    - Secreto o conocimiento (nombre de usuario y contraseña),
    - Objeto físico (llave o tarjeta)
    - Rasgo fisiológico o de comportamiento que posee el usuario
      - Huellas dactilares, patrón de retina, firma, etc
- La eficacia de un mecanismo de autenticación se mide por
  - El porcentaje de intrusos a los que se les concede el acceso
  - El porcentaje de usuarios legítimos a los que se les deniega el acceso

Contraseñas

- Las contraseñas ordinarias son relativamente fáciles de obtener o adivinar por un intruso cualificado
- Las contraseñas que más resisten a los ataques son aquellas que usan todo la longitud disponible para la contraseña, y que mezclan letras en mayúsculas y minúsculas con números, signos de puntuación y caracteres especiales.
- Las contraseñas el sistema las cifran antes de almacenarlas
- Técnicas
  - Envejecimiento de contraseñas.
    - Las contraseñas solo son validas durante un determinado periodo de tiempo, transcurrido el cual expiran y deben ser cambiadas.
  - Contraseñas de un solo uso
  - Reto dinámico

Autenticación

- Objetos físicos
  - Se basa en el uso de un objeto físico como por ejemplo una tarjeta electrónica inteligente.
- Características fisiológicas o de comportamiento
  - Se basan en *técnicas biométricas*

Software malicioso

- Todo aquel software diseñado causar daños o utilizar recursos de un computador (o de una red de computadores) sin el conocimiento y consentimiento de sus usuarios legítimos.
  - Bomba lógica
    - Es un fragmento de código insertado en un programa legítimo que únicamente **se activa cuando se cumplen o dejan de darse unas condiciones** prestablecidas, como por ejemplo, fecha y hora determinadas.
  - Puerta secreta
    - Es un fragmento de código insertado en un programa o sistema con la finalidad de poder saltarse los procedimientos de autenticación o ganar privilegios.
    - Se activa al introducir cierto secuencias especiales de entrada o con una determinada secuencia de eventos.
  - Caballo de Troya
    - Es un programa aparentemente inofensivo que aparte de realizar aparentemente la función para la que está diseñado realiza una función desconocida y no deseable por el usuario del programa, como el borrado de archivos, el envío de información a un intruso o permitir el acceso remoto de un intruso al sistema.
  - Gusano
    - Es un programa capaz de reproducirse y propagarse a otros computado -generalmente a través de una red informática.
      - Básicamente provoca una denegación del servicio o servicio deficiente a los usuarios de los computadores, ya que en su función de reproducción realiza consumo desproporcionado de los recursos de los computadores y del ancho de banda de la red porque se propaga.
  - Programa espía
    - Es un programa que se instala de forma furtiva en computador por un virus o un troyano y que se dedica a recopilar información sobre la actividad de usuarios para enviárselas a terceros.

Virus

- Es un fragmento de código insertado dentro del código de un programa anfitrión que se ejecuta si el usuario abre el programa anfitrión
- Un virus se propaga insertando copias de su código en otros archivos ejecutables.
- Fases
  - La fase latente
    - El virus se encuentra dormido.
      - Éste despierta cuando se produce algún evento, como por ejemplo, que se alcance una determinada fecha.
  - La fase de propagación
    - El virus inserta copias de sí mismo en otros archivos ejecutables ubicados en memoria secundaria, o en ciertas partes del disco duro como el sector de arranque maestro
  - *La fase de activación*
    - Sirve de transición hacia *la fase de ejecución* en la cual se ejecuta la función para la que fue diseñado el virus.
- Los virus insertados en macros
- El alcance del daño y la propagación que puede causar un virus está limitado por los privilegios de ejecución que tenga el programa anfitrión.
  - Así en sistemas operativos donde es posible limitar estos privilegios la acción de los virus puede ser acotada.
- Un *antivirus* busca en todos los archivos del computador susceptibles de estar infectado, los patrones de instrucciones que, de acuerdo con su base de datos, identifican a un posible virus

10.5 Mecanismos de protección

- Un proceso de usuario puede, de forma intencionada o involuntaria, intentar ejecutar acciones que perjudiquen el funcionamiento del sistema, como por ejemplo,
  - Acaparar el uso del procesador
  - Instrucciones de E/S ilegales,
  - Escribir o leer en las direcciones de memoria asignadas al sistema operativo o a otros procesos,
  - Leer o modificar archivos, etc.
- El sistema operativo dispone de una gran variedad de mecanismos de protección de los recursos del computador
- El modelo de protección más utilizado se basa en la abstracción conocida como ***matriz de acceso***.
  - En las siguientes secciones se describe cómo se define la matriz de acceso y sus dos implementaciones más frecuentes:
    - Las *listas de control de acceso* y
    - Las *listas de capacidades.*

Matriz de acceso

- Un sistema informático dispone de un conjunto de recursos hardware y software, también denominados **objetos**
  - Son utilizados por los procesos de los usuarios.
  - Cada objeto posee un **identificador** o nombre que lo distingue de los demás.
- Estos objetos son utilizados por un conjunto de procesos, también denominados **sujetos**.
- ***Un dominio de protección*** (o simplemente *dominio)* establece para un subconjunto de objetos las operaciones permitidas o derechos de acceso sobre cada uno de ellos.
  - De esta forma un dominio queda definido por un conjunto de pares de la forma
    - [objeto, derechos].
- Un mismo objeto puede estar en varios dominios simultáneamente con *los mismos* o con distinto derechos de acceso
- Un dominio se puede asociar a un usuario o a un proceso
- La asociación del dominio es ***estática***
  - Si el dominio asignado no cambia durante toda la sesión del usuario o durante el tiempo de vida del proceso
- Una asociación de dominio ***dinámica***
  - Un usuario o un proceso puede en cambiar de dominio.

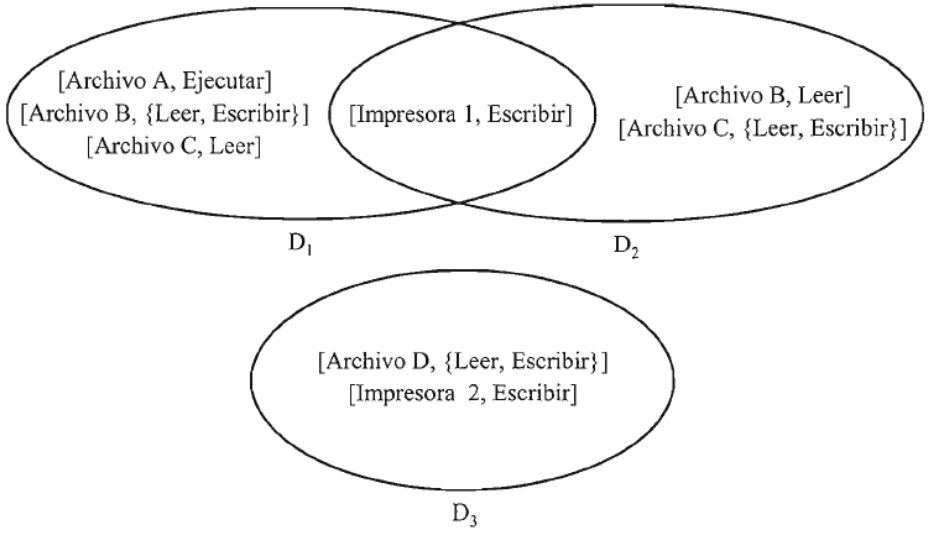

Figura 10.1 – Tres dominios de protección

Matriz de acceso o matriz de protección.

- Cada fila i de la matriz está asociada un dominio Di.
- Mientras que cada columna j de la matriz está asociada a un objeto Oj
- Cada elemento Aj de la matriz contiene los derechos de acceso asociados al objeto Oj dentro del dominio Dį.
- La matriz de acceso se suele implementar como
  - Un conjunto de *listas de control de acceso para objetos*
  - Un conjunto de *listas de capacidades para dominios.*

	Archivo A	Archivo B	Archivo C	Archivo D	Impresora 1	Impresora 2	D_1	D_2	D_3
D_1	Ejecutar	Leer Escribir	Leer		Escribir			Conmutar	
D_2		Leer	Leer Escribir		Escribir				Conmutar
D_3				Leer Escribir		Escribir			

Figura 10.2 – Matriz de acceso del Ejemplo 10.3

Listas de control de acceso

- Asociar con cada objeto una lista denominada lista de control de acceso (Access Control List, ACL).
  - Cada entrada de la lista contiene pares de la forma
    - [dominio, derechos]
  - Permite fácilmente revocar derechos de forma selectiva sobre objetos

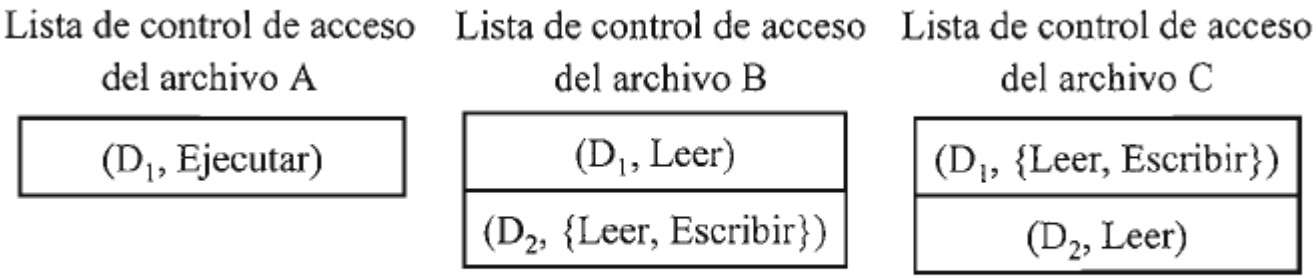

Figura 10.3 – Listas de control de acceso del Ejemplo 10.4

Listas de Capacidades

- Asociar con cada dominio una lista, denominada lista de capacidades.
  - Cada entrada de la lista contiene un identificador de un objeto, que indica la localización del objeto o de una estructura de datos que contiene su localización, y sus derechos de acceso.
  - A la dupla (objeto, derechos) se le denomina capacidad
- Acceso al contenido de una lista de capacidades es muy rápido
  - Ventaja: El Id del proceso actúa como índice
  - Inconveniente: El coste que supone para el sistema la revocación de los permisos para un objeto en concreto, ya que requiere acceder a todas las listas de capacidades existentes y buscar en cada una si existe la capacidad que se desea revocar.
  - Soluciones para revocar TODOS los permisos de un objeto
    - Tabla global:
      - Cada entrada tupla [identificador objeto, derechos]
      - Lista de capacidades: puntero a la tabla
      - Eliminamos derechos eliminando la entrada del objeto en la tabla
    - Clave maestra
      - Clave maestra en el núcleo y clave en la capacidad. Si coinciden se autoriza.
      - Cambiando la clave, se eliminan todos los derechos de acceso
  - En ambas soluciones no es posible realizar una revocación selectiva de los derechos

Lista de capacidades del dominio D_1
(Archivo A, Ejecutar)
(Archivo B, {Leer, Escribir})
(Archivo C, Leer)
(Impresora 1 , Escribir)
(Dominio D_2, Conmutar)

Lista de capacidades del dominio D_2
(Archivo B, Leer)
(Archivo C, {Leer, Escribir})
(Impresora 1 , Escribir)
(Dominio D_3, Conmutar)

Lista de capacidades del dominio D_3
(Archivo D, {Leer, Escribir})
(Impresora 2 , Escribir)

Figura 10.4 – Listas de capacidades del Ejemplo 10.5

Sistemas confiables

- Un sistema informático se denomina confiable si cumple con los requerimientos de seguridad o política de seguridad que se había impuesto.
- Todo sistema confiable dispone de una Base de Computador Confiable (Trusted Computer Base, TCB),
  - Un conjunto de elementos hardware y software que le permiten implementar los requisitos de seguridad establecidos.
- El *monitor de referencia*
  - Se encarga de comprobar todas las llamadas al sistema que pueden comprometer la seguridad del sistema, como son la creación de procesos o la apertura de archivos, y decidir si pueden ser procesadas o deben ser rechazadas.

Seguridad multinivel

- Modelo de seguridad multinivel que distingue varios niveles de seguridad.
  - A cada objeto y usuario se le asigna un determinado nivel
- Reglas
  - Imposibilidad de leer objetos de niveles superiores
  - Imposibilidad de escribir objetos de niveles inferiores

Principios de diseño de sistemas operativos seguros

- El diseño del sistema deber ser público
- El estado por defecto es el de no acceso
- Principio del mínimo privilegio
- Los mecanismos de protección debe ser simples y estar integrados en las capas más bajas del sistema
- Los mecanismos de protección deben ser aceptados por los usuarios