Sistemas Operativos

Grado en Ingeniería Informática del Software

Tema 7: Seguridad en SO

Tabla de contenidos

Seguridad

- . Un sistema es seguro cuando actúa como está previsto que lo haga:
  - Permite a cada usuario realizar las operaciones a las que está autorizado.
  - Impide a cada usuario realizar operaciones a las que no está autorizado

Objetivos de la seguridad

- Confidencialidad.
- Integridad.
- Disponibilidad.

Daños a la confidencialidad

- Acceso indebido al sistema *(usurpación),* pudiendo obtener copias de datos y programas almacenados accesibles al usuario legal.
- Acceso a las comunicaciones (*sniffing),* pudiendo obtener copias de los mensajes o ficheros intercambiados entre máquinas.
- Acceso físico a la máquina o al dispositivo de almacenamiento, pudiendo realizar copias o sustrayendo el hardware.
- Acceso lógico o físico a copias de seguridad de los datos y programas.
- Acceso a los datos/programas mediante el uso de ingeniería social.
- Acceso de los datos/programas mediante el uso de malware.

Daños a la integridad

- Acceso indebido al sistema *(usurpación),* pudiendo obtener modificar datos y programas almacenados accesibles al usuario legal.
- Acceso a las comunicaciones (*sniffing, man in the middle),* pudiendo obtener acceder a los mensajes o ficheros intercambiados entre máquinas, modificándolos o inventando nuevos
- Acceso físico a la máquina o al dispositivo de almacenamiento, pudiendo modificar directamente los datos/programas almacenados.
- Modificación de los datos/programas mediante el uso de ingeniería social.
- Empleo de malware.

Daños a la disponibilidad

- Saturación del sistema mediante el empleo de malware (gusanos, bacterias, …)
- Saturación del sistema mediante ataques DoS.
- Eliminación o avería del hardware del sistema o de comunicaciones.
- Apagado del sistema.
- Supresión del suministro eléctrico del sistema o de los dispositivos de comunicaciones.

Amenaza

- Conjunto de circunstancias cuya probabilidad de producirse es significativo.

Vulnerabilidad

- Debilidad (técnica, física, de procedimiento, humana, …) en la seguridad de un sistema.

Exploit

- Técnica que permite aprovechar una vulnerabilidad para lanzar un ataque.

Control o contramedida

- Medida de protección que elimina o reduce un riesgo. Puede ser:
  - prevención
  - obstaculización
  - desvío
  - detección
  - recuperación.
- Pueden ser proporcionados por
  - El Sistema Operativo
  - Otros componentes (tecnológicos, humanos, organizativos).

Tabla de contenidos

La seguridad y el SO

En lo que respecta a la seguridad, el sistema operativo debe proveer mecanismos para:

1. Evitar vulnerabilidades en su funcionamiento.
2. Realizar una autenticación efectiva de los usuarios que acceden al sistema.
3. Controlar de manera efectiva el uso de los recursos.
4. Incorporar medidas ante software dañino (*malware).*

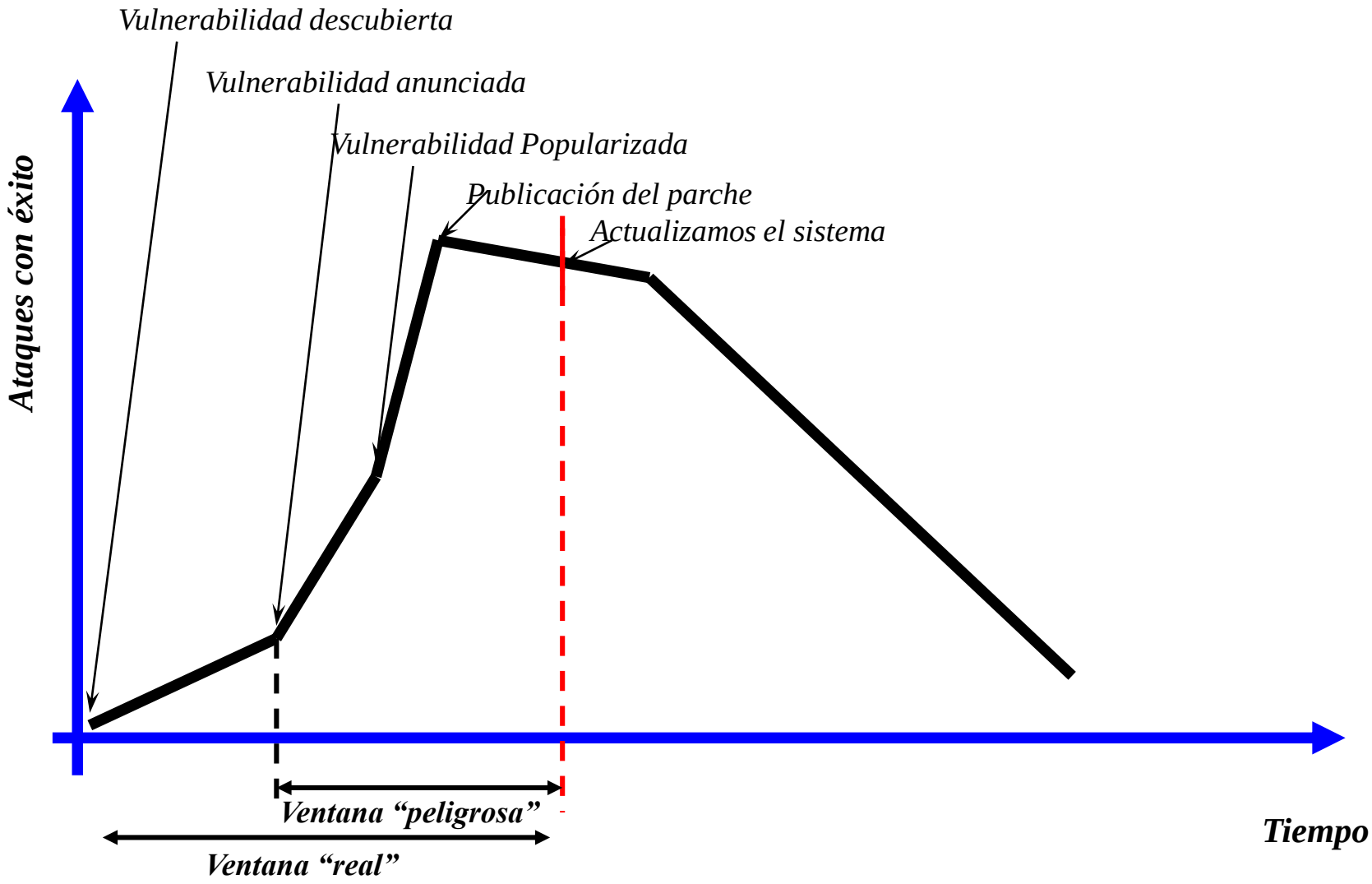
La seguridad y el Sistema Operativo
Actualizaciones

- Todo sistema operativo recién instalado debe actualizarse inmediatamente:
  - Desde la fecha de distribución del sistema, **seguro** que se han descubierto vulnerabilidades en el sistema o en las aplicaciones que lo acompañan.
  - Es preciso, pues, descargar e instalar las actualizaciones de seguridad disponibles.
- Todos los sistemas operativos actualmente disponen de herramientas que facilitan la tarea:
  - Windows Update (o Windows Server Update Services –WSUS para instalaciones con muchos ordenadores).
  - apt-get, rpm, …, en Linux (según distribución).

La seguridad y el Sistema Operativo
Actualizaciones

- Después de la actualización inicial, ha de establecerse un calendario de actualización para mantener el sistema a salvo de *exploits*.
- Hay que considerar que NO se puede estar al tanto de TODAS las vulnerabilidades:
  - Según Wietse Venema: "*Hay aproximadamente un bug de seguridad por cada 1000 líneas de código fuente*"
  - Si el S.O. tiene 100 millones de líneas de código (Windows 10 2003 tiene unas 80 millones), hay cientos de miles de bugs de seguridad potenciales en el S.O.
  - El CERT (*Computer Emergency Response Team*) descubre una media de 5000 bugs/año -> 20 años en descubrir todas.

La seguridad y el Sistema Operativo
Vulnerabilidad de día cero



La seguridad y el Sistema Operativo
Configuración del sistema

Además de actualizar el sistema, hay que prestar especial cuidado con la **configuración** inicial del mismo.

1. En concreto, es importante instalar únicamente aquellos servicios que se van a utilizar:
   - Los servicios no utilizados son un peligro adicional:
     - No ofrecen nada a los usuarios (no se utilizan).
     - Proveen nuevos frentes de ataque.
     - Nadie suele estar pendiente de ellos, con lo que cualquier ataque puede pasar mucho tiempo inadvertido.
2. Además, hay que configurar los límites (de disco, de memoria, de procesos, etc.) que puede utilizar cada usuario para evitar el acaparamiento de recursos por parte de algún usuario.

3. Hay que asignar privilegios a usuarios con mucho cuidado (*mínimo privilegio*):
   a) No permitir acceder a programas *delicados* (programas de configuración del sistema, de gestión de usuarios, etc.).
   b) No dejar instalar aplicaciones.
   c) Restringir el uso de recursos (como la red).
4. No habilitar comunicaciones no encriptadas.
5. Restringir las máquinas desde las que se pueden realizar operaciones *delicadas* (acceso de administración, *backups*, etc)
6. Tener en cuenta las precauciones específicas de sistemas concretos.

Tabla de contenidos

Autenticación de usuarios

- Debe asegurarse:
  - Que los usuarios **NO** autorizados **NO** puedan acceder al sistema.
  - Que los usuarios autorizados **SÍ** puedan acceder al sistema.
- La autentificación de usuarios puede estar basada en:
  - Algo que **sabe** el usuario: *contraseña, pin, …*
  - Algo que **tiene** el usuario: *tarjeta magnética, llave, …*
  - Quién **es** el usuario: biométricos (*huella dactilar, geometría de la mano, retina, iris, cara, firma, voz, …*)
  - Varios de los anteriores.

Autenticación de usuarios
Autenticación por contraseña

- Es el mecanismo más utilizado:
  - No requiere hardware especial.
  - La tasa de falso rechazo (FRR – *False Rejection Rate*) es nula.
  - La tasa de falsa aceptación (FAR – *False Acceptance Rate*) también es nula.

Autenticación de usuarios
Autenticación por contraseña

- Es el más fácilmente atacable:
  - Cualquiera puede intentar averiguar contraseñas.
  - Las contraseñas deben almacenarse en el sistema, luego alguien puede intentar conseguirlas.
    - Para solventar este problema, se almacenan encriptadas (preferiblemente con cifrado no reversible).
  - Independientemente de si se consigue el fichero de contraseñas encriptado o no, se puede intentar averiguarlas:
    - Por ingeniería social:
      - Obteniéndolas directamente del usuario.
      - Usando información relacionada con el usuario.
    - Por ataque de “fuerza bruta”.

Autenticación de usuarios
Autenticación por contraseña

- Algunas precauciones que pueden tomarse:
  - Asegurarse que todos los usuarios tienen contraseñas seguras.
  - No dejar ninguna cuenta sin contraseña.
  - No almacenar contraseñas en ficheros accesibles por usuarios normales.
  - No almacenar contraseñas sin cifrar o con cifrado reversible.
  - No dejar sesiones abiertas desatendidas.
  - Bloquear cuentas con exceso de intentos infructuosos de acceso.
  - Vigilar los ficheros de *log* para localizar accesos sospechosos.
  - Inhabilitar cuentas no utilizadas.
  - Cambiar el nombre de cuentas conocidas (administrador, invitado, …)
- Algunas cuestiones son de educación del usuario y/o del administrador; otras pueden vigilarse por medios técnicos.

Autenticación de usuarios
Autenticación por elemento físico

- Los usuarios se identifican con algo que poseen: una tarjeta magnética, una tarjeta inteligente, etc.
- Es fácilmente utilizable:
  - Requiere hardware especial, pero no suele ser muy costoso.
  - La tasa de falso rechazo (FRR – *False Rejection Rate*) es nula.
  - La tasa de falsa aceptación (FAR – *False Acceptance Rate*) también es nula.
  - Casi todos los sistemas operativos proveen mecanismos para incorporarlos como elemento de control de acceso.

Autenticación de usuarios
Autenticación biométrica

- Los usuarios se identifican con alguna característica propia: huella dactilar, iris, retina, voz, …
- No suele utilizarse demasiado:
  - Requiere hardware especial, relativamente costoso.
  - La tasa de falso rechazo (FRR – *False Rejection Rate*) puede llegar a ser inaceptable.
  - La tasa de falsa aceptación (FAR – *False Acceptance Rate*) puede ser peligrosamente alta.
  - Los fabricantes suelen ajustar el umbral de aceptación prefiriendo rechazar usuarios legales que aceptar usuarios no autorizados.
  - Casi todos los sistemas operativos proveen mecanismos para incorporarlos como elemento de control de acceso.

Autenticación de usuarios
Otros mecanismos

- Utilizando un par de claves privada – pública o certificados de usuario:
  - En este caso sólo se puede acceder desde las máquinas que tengan instalada la parte privada de la clave del usuario.
- Utilizando “claves de un solo uso” (*one time passwords*).
- Utilizando autenticación de doble factor.

Tabla de contenidos

Control de acceso a recursos
La matriz de acceso

En general, debe gestionarse una **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

Listas de control de acceso (por columnas)

- Cada recurso guarda la lista de clientes con sus permisos (vector columna de la matriz)

Capacidades (por filas)

- Cada cliente guarda la lista de capacidades (recurso+permisos) que tiene disponibles.

Control de acceso a recursos
Listas de control de acceso

Cuando un cliente realiza una petición sobre un recurso

- El S.O. (mecanismo de protección) comprueba si el cliente está en la LCA del recurso.
- Mecanismo usado por Unix y Windows para el control de acceso a ficheros y a otros recursos.

Inconvenientes de las 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

Control de acceso a recursos
Dominios de protección

- Cada sistema operativo determina a quién garantiza o niega unos determinados tipos de acceso a los recursos.
- En Unix se distinguen tres dominios: *propietario, grupo y resto de usuarios*.
- En Unix, con el paquete ACL instalado, se pueden incluir *n* dominios: usuarios independientes en cualquier número, grupos en cualquier número y “otros”.
- En Windows se pueden incluir *n* dominios: usuarios independientes en cualquier número y grupos en cualquier número.

Control de acceso a recursos
Tipos de acceso

- Cada sistema operativo determina entre qué tipos de accesos distingue, pudiendo garantizarlos o negarlos.
- En Unix, los tipos tradicionales son tres: *lectura, escritura y ejecución*.
  - La combinación de los permisos de los ficheros y de los directorios que los contiene dan más flexibilidad (pero poca).

Windows

Operaciones básicas por dominio:

- Control Total
- Modificar
- Lectura y ejecución
- Mostrar contenido de carpeta
- Leer
- Escribir

Operaciones avanzadas por dominio:

- Control total,
- Recorrer carpeta/Ejecutar archivo
- Listar carpeta/leer datos
- atributos de lectura
- atributos extendidos de lectura
- crear archivos/escribir datos
- crear carpetas/anexar datos
- atributos de escritura
- atributos extendidos de escritura
- eliminar archivos/carpetas
- eliminar
- permisos de lectura
- cambiar permisos
- tomar posesión

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 S.O (mecanismo de protección) comprueba si en la capacidad existe permiso para la operación solicitada. Análogo a entrada a cine.
- No hay que acceder a ninguna ACL ni similar.

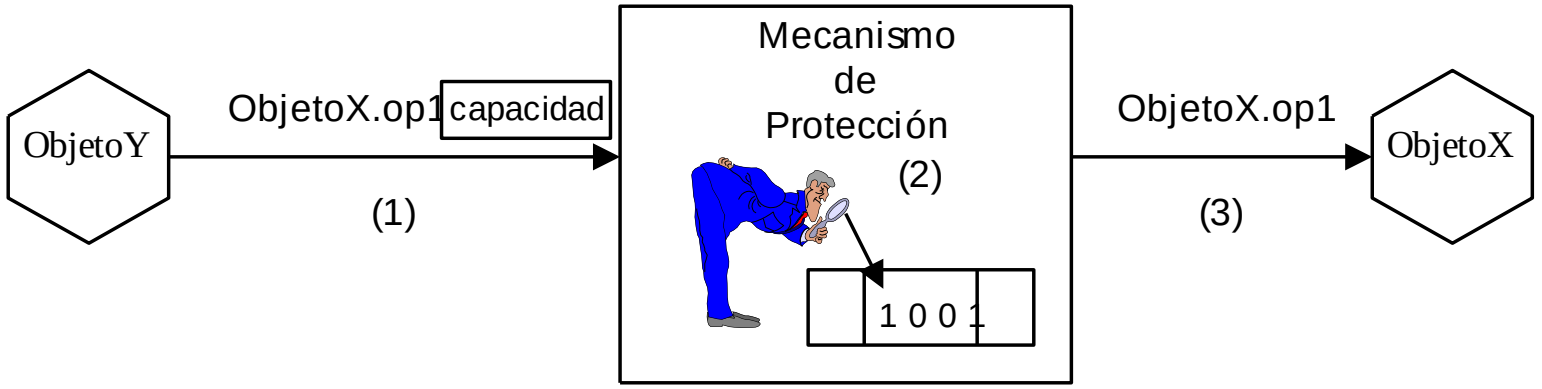


Tabla de contenidos

Malware

- Existen multitud de tipos de programas malicioso:
  - Caballos de troya
  - Virus, gusanos, bacterias, …
  - Rootkits
  - Bombas lógicas, trampas, puertas traseras, …
- Contra ellos, hay varias técnicas que se pueden utilizar:
  - Firewalls
  - Antivirus.
  - Encarcelamiento.
  - IDS (Intrusion Dectection Systems)
  - Educación de los usuarios:
    - Programas firmados.
    - Apertura de adjuntos de ficheros.
    - ….