Seguridad y Competencias Profesionales
Tema 6: Seguridad de los sistemas operativos
Curso 2012–2013

Ingeniería en Informática (2° ciclo)

Departamento de Ingeniería Informática
Universidad de Cádiz

Cádiz, 5 noviembre 2012

Índice

Contenido

Objetivos

Al finalizar el tema el estudiante deberá ser capaz de:

- Distinguir entre las distintas categorías de métodos de autenticación y dar ejemplos de cada una de ellas.
- Enumerar las características que debe tener una buena contraseña y las normas de seguridad que deben seguir los usuarios para mantenerlas seguras.
- Enumerar los pasos que se siguen cuando se utilizan métodos de autenticación biométricos.
- Distinguir entre la tasa de falso rechazo y la tasa de falsa aceptación.
- Enumerar los elementos básicos de un modelo de control de acceso.
- Diferenciar entre las listas de control de acceso y las listas de capacidades.

Objetivos (cont.)

- Describir las características generales de un sistema de control de acceso a la información mediante niveles de seguridad.
- Dado un ejemplo concreto de clasificaciones y categorías saber determinar si un determinado sujeto tendría acceso a un objeto dado para hacer una operación sobre él.
- Dado un caso concreto, ser capaz de planificar una política de copias de seguridad que se adapte a las características de éste.
- Enumerar los objetivos que se persiguen al activar el sistema de auditorías de un sistema operativo.
- Enumerar ejemplos de eventos auditables y de información auditable para cada evento.
- Enumerar los aspectos claves para que la activación de un sistema de auditorías sea eficiente.

Seguridad en el sistema

La seguridad de un sistema debe contemplar 3 aspectos fundamentales:

- Control de acceso al sistema
- Control de acceso a los datos
- Administración del sistema y de la seguridad

Control de acceso al sistema

Los sistemas operativos suelen proporcionar un mecanismo de control del acceso de los usuarios. Éste suele constar de dos pasos:

1. Identificación del usuario
2. Autenticación del usuario

Métodos de autenticación

Los métodos de autenticación se suelen dividir en tres grandes categorías:

1. Algo que el usuario sabe.
2. Algo que el usuario posee.
3. Una característica física del usuario (autenticación biométrica).

La elección de las contraseñas

Principio general

Una buena contraseña debe ser difícil de adivinar (tanto por los humanos como mediante métodos automatizados).

Recomendaciones

- Deben ser lo más largas posible (mínimo 8 caracteres).
- Conviene combinar caracteres numéricos y alfanuméricos, letras mayúsculas, minúsculas y caracteres especiales (%, $, &, . . .)
- Deben evitarse las palabras de cualquier idioma y los nombres propios.
- No deben utilizarse combinaciones simples de datos personales: iniciales del nombre, fecha de nacimiento, DNI, teléfono, matrícula del coche, etc.
- Utilizar contraseñas fáciles de recordar, para evitar tenerlas apuntadas.
- Son especialmente recomendables los acrónimos de frases que uno recuerde fácilmente.

Protección de las contraseñas

Precauciones a tomar por los usuarios

- No compartir nunca su contraseña.
- Cambiarla cada cierto tiempo.
- No escribir ni teclear su contraseña delante de otras personas.
- No enviar la contraseña por correo electrónico.
- Si la contraseña se guarda por escrito, hacerlo en un lugar de difícil acceso para otras personas y de forma que no pueda ser adivinada su función.

Protección de las contraseñas (cont.)

Precauciones a tomar por el administrador

- No debe crear nunca cuentas sin contraseña.
- Cambiar la contraseña después de instalar el sistema.
- Proteger de forma adecuada el fichero del sistema donde se almacenan las contraseñas.
- Vigilar las cuentas de los usuarios accidentales, ya que son las más propensas a la penetración por parte de intrusos.

Protección de las contraseñas (cont.)

Protección automatizada:

- Número limitado de intentos de acceso
- Control de calidad de las contraseñas
- Caducidad de contraseñas
- Generación automática de contraseñas
- Bloqueo de cuentas
- Registro de entradas

Protección de las contraseñas (cont.)

Protección del fichero de contraseñas

- Las contraseñas tienen que guardarse cifradas. El método criptográfico utilizado debe ser irreversible para que no sea posible descifrarlas.
- El fichero que contiene las contraseñas no debería ser visible a los usuarios.

Las contraseñas en UNIX/Linux

El sistema clásico

- Las contraseñas se guardan cifradas en el fichero `/etc/passwd` (lectura pública).
- Formato del fichero:
  `login:passwd:UID:GID:varios:dir-entrada:shell`
- Problemas: Se pueden adivinar contraseñas comparando palabras de un diccionario cifradas con las almacenadas en el fichero `/etc/passwd`.

Las contraseñas en UNIX/Linux (cont.)

Mejora de la seguridad de las contraseñas

- El fichero `/etc/passwd` no contiene la contraseña codificada.
- Ésta se encuentra en el fichero /etc/shadow que no es de lectura pública.

Sistemas de autenticación biométrica

- Pueden utilizar cualquier característica única y mensurable del individuo. Se han utilizado:
  - Iris del ojo
  - Retina del ojo
  - Huellas dactilares
  - Geometría de la mano
  - Firma
  - Voz

Sistemas de autenticación biométrica (cont.)

Fases

1. Captura o lectura de los datos que el usuario presenta para su validación.
2. Extracción de ciertas características de la muestra.
3. Comparación de tales características con las guardadas en una base de datos.
4. Decisión de si el usuario es válido o no.

Problemas

Tasa de falso rechazo	Probabilidad de que el sistema de autenticación rechace a un usuario legítimo.
Tasa de falsa aceptación	Probabilidad de que el sistema autentique correctamente a un usuario ilegítimo.

Sistemas de autenticación biométrica (cont.)

Ejercicio 6.1

Si un sistema de autenticación biométrica tiene una tasa de falso rechazo elevada:

- ¿Para quién sería más perjudicial, para los usuarios o para el sistema?
- ¿Y si fuera elevada la tasa de falsa aceptación?

Mecanismos de control de acceso a la información

- Determinan qué información puede ser utilizada por cada usuario del sistema.
- Pueden constituir una segunda barrera ante los intrusos que consigan saltarse los mecanismos de control de acceso al sistema.

Modelo de control de acceso

Elementos básicos

Sujeto Es una entidad capaz de acceder a los objetos. En general, podemos equiparar el concepto de sujeto con el de proceso.

Objeto Cualquier recurso cuyo acceso deba controlarse, por ejemplo, ficheros, partes de ficheros, segmentos de memoria, etc.

Derecho de acceso La forma en que un sujeto accede a un objeto, por ejemplo, lectura, escritura y ejecución.

	Fichero1	Fichero2	Fichero3
Usuario A	r w	r	
Usuario B		r w	r
Usuario C			r w

Listas de control de acceso y listas de capacidades

Listas de control de acceso

- Resultan de la descomposición por columnas de la matriz de acceso.
- Existe una por cada objeto del sistema y enumera los usuarios y los derechos de acceso de éstos al objeto.

Listas de capacidades

- Resultan de la descomposición por filas de la matriz de acceso.
- Hay una por cada sujeto y enumera los derechos de acceso de éste a los objetos del sistema.

Listas de control de acceso y listas de capacidades (cont.)

Características de las listas

- Acceso secuencial.
- Añadir un elemento puede hacerse en un tiempo constante (si se almacena un puntero al último).
- Eliminar un elemento requiere un barrido (hay que buscarlo y luego retirarlo).

Consideraciones a tener en cuenta

- En un sistema normalmente hay mucho más objetos que sujetos.
- Añadir una entrada tiene menor coste que crear una lista.

Listas de control de acceso y listas de capacidades (cont.)

Posibilidades de las listas de control de acceso y de las listas de capacidades en términos de:

- Facilidad para determinar *un* acceso autorizado durante la ejecución de un proceso:
  - Lista de control de acceso, si nº objetos > nº sujetos.
- Facilidad para añadir *un* acceso para un nuevo sujeto:
  - Lista de control de acceso, si añadir una entrada tiene menor coste que crear una lista.
- Facilidad para borrar *un* acceso de un sujeto:
  - Lista de control de acceso, si nº objetos > nº sujetos.
- Facilidad para crear *un* objeto nuevo al cual deberían tener acceso todos los sujetos:
  - Lista de control de acceso.

Listas de control de acceso y listas de capacidades (cont.)

Posibilidades de las listas de control de acceso y de las listas de capacidades en términos de:

- Facilidad para determinar *un* acceso autorizado durante la ejecución de un proceso:
  - Lista de control de acceso, si nº objetos > nº sujetos.
- Facilidad para añadir *un* acceso para un nuevo sujeto:
  - Lista de control de acceso, si añadir una entrada tiene menor coste que crear una lista.
- Facilidad para borrar *un* acceso de un sujeto:
  - Lista de control de acceso, si nº objetos > nº sujetos.
- Facilidad para crear *un* objeto nuevo al cual deberían tener acceso todos los sujetos:
  - Lista de control de acceso.

Listas de control de acceso y listas de capacidades (cont.)

Posibilidades de las listas de control de acceso y de las listas de capacidades en términos de:

- Facilidad para determinar *un* acceso autorizado durante la ejecución de un proceso:
  - Lista de control de acceso, si nº objetos > nº sujetos.
- Facilidad para añadir *un* acceso para un nuevo sujeto:
  - Lista de control de acceso, si añadir una entrada tiene menor coste que crear una lista.
- Facilidad para borrar *un* acceso de un sujeto:
  - Lista de control de acceso, si nº objetos > nº sujetos.
- Facilidad para crear *un* objeto nuevo al cual deberían tener acceso todos los sujetos:
  - Lista de control de acceso.

Listas de control de acceso y listas de capacidades (cont.)

Posibilidades de las listas de control de acceso y de las listas de capacidades en términos de:

- Facilidad para determinar *un* acceso autorizado durante la ejecución de un proceso:
  - Lista de control de acceso, si nº objetos > nº sujetos.
- Facilidad para añadir *un* acceso para un nuevo sujeto:
  - Lista de control de acceso, si añadir una entrada tiene menor coste que crear una lista.
- Facilidad para borrar *un* acceso de un sujeto:
  - Lista de control de acceso, si nº objetos > nº sujetos.
- Facilidad para crear *un* objeto nuevo al cual deberían tener acceso todos los sujetos:
  - Lista de control de acceso.

Control por niveles de seguridad

Acceso discrecional y obligatorio

Acceso discrecional Deja en manos de los usuarios la decisión de qué tipos de acceso permite para los ficheros que posee.

Acceso obligatorio Es el sistema el que toma todas las decisiones sobre el acceso a los datos basándose en unas reglas fijas y en un esquema de clasificación que establece los niveles de seguridad de los distintos sujetos y objetos que comparten el sistema. Esta política puede ser implementada por medio del denominado control por niveles de seguridad.

Control por niveles de seguridad (cont.)

- Es apropiado para organizaciones que tienen requisitos elevados de seguridad y los usuarios operan de modo jerárquico y disciplinado (organizaciones militares, agencias de inteligencia, empresas con altos requisitos de seguridad).
- Cada sujeto y objeto tiene asociada una etiqueta.
- La etiqueta consta de dos partes: **Clasificación** y un conjunto de **Categorías**.
- Ejemplo de etiqueta:
  Secreto [Armas-Químicas Oriente-Medio]

Control por niveles de seguridad (cont.)

Niveles de seguridad en entorno militar

1. Alto secreto
2. Secreto
3. Confidencial
4. No clasificado

Niveles de seguridad en entorno empresarial

1. Propietario
2. Directivo
3. Jefe de Departamento
4. Empleado
5. Público

Control por niveles de seguridad (cont.)

Categorías

- Las categorías no son jerárquicas.
- Representan las distintas áreas de información del sistema.
- Ejemplo de categorías en una empresa: Ventas, Personal, Producción, Marketing...

Decisión:

- Etiqueta del sujeto
- Etiqueta del objeto
- Tipo de acceso que se quiere realizar

Control por niveles de seguridad (cont.)

Regla de lectura

Para leer un objeto, el nivel de seguridad del sujeto debe ser igual o superior al del objeto y además, el conjunto de categorías del sujeto debe incluir todas las del objeto.

Regla de escritura

Para poder escribir en un objeto, el nivel de seguridad del objeto debe ser igual o superior al del sujeto y además, el conjunto de categorías del sujeto deben estar incluidas en las del objeto.

Control por niveles de seguridad (cont.)

Ejercicio 6.2

Considere los siguientes sujetos de un sistema con sus etiquetas:

María	**Público [Ventas]**
Pedro	**Empleado [Ventas Personal]**
Jesús	**Directivo [Ventas Marketing]**
Rosa	**Propietario [Ventas]**

- ¿Cuáles de estos usuarios pueden leer el fichero **Venta03** cuya etiqueta es **Directivo[Ventas Marketing]**?
- ¿Cuáles podrían escribir en el mismo fichero?

Utilidad de las copias de seguridad

Único mecanismo para recuperar datos perdidos

Casos en que son necesarias

- Un usuario o un administrador ha borrado de forma no intencionada alguna información que era importante.
- Un intruso ha borrado información importante.
- Fallo de hardware.
- Un robo.
- Desastres naturales: inundación, incendio...

Casos reales

- Ma.gnolia:
  `http://www.error500.net/articulo/magnolia-hizo-crack`
- Sidekick:
  `http://news.cnet.com/8301-17938_105-10372521-1.html`

¿Qué debemos copiar?

Hay dos tendencias: copiar todo o sólo una parte

Copia completa

Copiamos todos los ficheros del sistema.

Ventajas	La recuperación del sistema, en caso de tener que recuperarlo completo, es más sencilla.
Inconvenientes	Consume más recursos (soporte y tiempo).

Copia parcial

Copiamos aquello que sea específico de nuestro sistema: ficheros de usuarios, ficheros de configuración...

Ventajas	Consume menos recursos.
Inconvenientes	Si hay que recuperar todo el sistema, tendremos que empezar instalando el SO, todo el software adicional instalado (más parches...) y, por último, la copia de seguridad.

Tipos de copias de seguridad

Completas

Copia todos los ficheros de interés.

Progresivas

Sólo se copian aquellos ficheros que han sido creados o modificados desde la última copia completa o progresiva efectuada.

Diferenciales

Sólo se copian los ficheros que han sido creados o modificados desde la última copia completa realizada.

Plan de copias de seguridad

Contenidos

- Tipos de copias que se van a realizar
- Ciclos de copia y rotación de soportes
- Frecuencia
- Momento en que se van a realizar las copias

Otros aspectos a considerar

- Protección
- Comprobación
- Recursos para la realización de copias de seguridad

Ejercicios de copias de seguridad

Ejercicio 6.3

- Considere los siguientes escenarios:
  - Copias completas y progresivas
  - Copias completas y diferenciales
- Explique cómo llevaría a cabo estas acciones en cada caso:
  - Recuperar el sistema completo
  - Recuperar un fichero individual

Ejercicios de copias de seguridad (cont.)

Ejercicio 6.4: copias completas

Busque información sobre 2 herramientas de la siguiente lista y describa cómo crear y recuperar copias completas con ellas, preservando los metadatos de los ficheros:

- dd (ver dd(1))
- tar (`http://www.gnu.org/software/tar/manual/`)
- clonezilla (`http://clonezilla.org/`)

Ejercicio 6.5: copias progresivas y diferenciales

Como el ejercicio 6.4, pero para copias progresivas y diferenciales y escogiendo de:

- tar, dar (ver dar(1))
- rsync (ver rsync(1))
- Unison (`http://www.cis.upenn.edu/~bcpierce/unison/`)

Introducción

Concepto de auditoría

Consiste en la monitorización del funcionamiento del sistema de forma automatizada y sistemática mediante el registro de los sucesos clave que se producen en éste.

Objetivos

- Revisar accesos por usuarios a los objetos del sistema.
- Revisar la efectividad de los mecanismos de seguridad del sistema.
- Descubrir intentos de saltarse los mecanismos de seguridad.
- Descubrir usuarios con privilegios excesivos.
- Servir de elemento disuasor para los atacantes.
- Ayudar a la recuperación de desastres informáticos.
- Proporcionar pruebas materiales de los ataques.

Conceptos básicos

Evento auditable

- Acciones que queremos que queden registradas en el sistema de auditoría.
- Ejemplos: Arranque o parada del sistema, conexión o desconexión de un usuario, cambio de privilegios de acceso a los objetos de un sistema, creación/modificación/borrado de un objeto...

Información auditable

- Datos relacionados con el evento auditable que pueden ser útiles.
- Ejemplos: Fecha y hora en que se produce el evento, tipo de evento, éxito o fracaso, datos del usuario que lo desencadena...

Detección de ataques

Tipos más comunes

- Intentos fallidos de entrada al sistema
- Suplantaciones
- Flujos de información prohibidos
- Obtención de información restringida
- Caballos de Troya
- Virus
- Abuso de recursos

Mecanismos para la detección de ataques

Perfil de usuario

- Recoge las acciones que cada usuario realiza normalmente en el sistema.
- Si un intruso utiliza la cuenta de un usuario se puede detectar debido a que se aparta del perfil del usuario.
- Puede avisar de acciones legales que se aparten del perfil.

Perfil de intruso

- Los intrusos suelen actuar de una forma similar cuando entran en un sistema ajeno: mirar quién está conectado al sistema, examinar el sistema de ficheros, moverse por los directorios tratando de obtener información, no suelen estar conectado mucho tiempo.

Mecanismos para la detección de ataques (cont.)

Acciones puntuales

Hay ciertas acciones que por sí mismas denuncian la presencia de un ataque o intento de ataque:

- Intento de acceso a la administración del sistema.
- Intento de explotación de agujeros de seguridad conocidos.
- Uso de herramientas que detectan agujeros de seguridad: Crack, Satan, Cops...
- Uso de órdenes de otros sistemas operativos.

Prácticas recomendadas

- Disponer de un administrador.
- Parametrizar de forma adecuada el sistema de auditoría:
  - Establecer los eventos y la información auditables.
  - Definir perfiles.
  - Proteger los ficheros de auditoría.
- Compresión y respaldo de los ficheros de auditoría.
- Determinar el método de análisis que se va a realizar sobre los ficheros de auditoría.
- Cuidar las implicaciones de tipo ético.