Sistemas Operativos 2

Unidad 5: Seguridad

Componentes de la seguridad

René Ornelis
Primer semestre de 2025

Contenido

Índice de figuras

Componentes de seguridad

En cualquier situación en que se hable de seguridad se deben tener tres elementos esenciales: autenticación, autorización y auditoría (AAA). Si falta alguno de estos no se tiene una seguridad completa.

1 Autenticación o identificación

La autenticación es el proceso por medio del cual el sistema operativo determina la identidad de la persona que accede al sistema. Esta función se suele cumplir a través de al menos uno de tres medios:

1. **Saber:** La identidad se determina a través de algo que el usuario sabe. Esta es la estrategia predominante en la actualidad por medio del uso de contraseñas. También incluye el uso de frases. Por ejemplo: para recuperar una contraseña el usuario puede configurar previamente un conjunto de preguntas personales como "El nombre de tu primera escuela", "Tu mejor amigo de la niñez", etc, que es información que supuestamente otras personas no sabrían sobre el usuario. Asimismo, en esta categoría se pueden incluir el uso de envío de una contraseña de un solo uso (One Time Password u OTP) a un correo electrónico, ya que se supone que solo el usuario sabe la contraseña de su correo.
2. **Tener**: Se asocia al usuario la pertenencia de un objeto físico. Esta estrategia es utilizada por ejemplo en las puertas con tarjetas de proximidad. Otra forma es a través de un dispositivo de cálculo de un número único basado en la hora, que puede ser verificado con el mismo cálculo en el servidor (Timebased One Time Password o TOTP). Actualmente, los tokens físicos han sido reemplazado por aplicaciones en celulares con el estándar RFC 6238 de la IETF.
3. **Ser**: Biométrica. Es la identificación a través de las características físicas de la persona como la huella digital, el iris de los ojos, reconocimiento facial, reconocimiento de voz, etc. En general, se buscan las características físicas de una persona que distinguen a cada uno de manera única.

En un sistema de alta seguridad se pueden incluir combinaciones de estos elementos para una autenticación:

- Puertas: Combinación de un código de seguridad con una tarjeta de proximidad.
- Sitio web: ingreso de usuario, contraseña y un SMS enviado a un celular
- Cajero automático (ATM): combinación de una tarjeta y un código personal

Recordemos los sistemas de seguridad de la película Misión Imposible:

- Reconocimiento de voz

- Código de seguridad

- Tarjeta de seguridad

- Escaneo de retina

Aquí se aplican combinaciones de los tres medios de autenticación.

2 Autorización

La autorización es el proceso por medio del cual un usuario **autenticado** se le concede acceso a realizar una acción (derecho) a un elemento del sistema (objeto).

1. Derecho de acceso: la habilidad de ejecutar una operación sobre un objeto
2. Dominio: colección de derechos de accesos, en pares (Objeto, derecho)
    1. Ej. ACL
3. Asociación estática o dinámica (cambio de dominio)
    1. Ej: sudo
4. Implementaciones
    1. Dominio por usuario
        1. Listas de control de accesos
    2. Dominio por proceso: definición de roles, que son la asociación de un programa con un conjunto de derechos de acceso.
        1. Capacidades
5. Matriz de acceso: es la forma de ver los diferentes dominios, en la cual se especifica en columnas los objetos y en las filas los dominios, y en cada celda el acceso.
6. SELinux

2.1 Modelo militar

El modelo de seguridad militar de anillos concéntricos y grupos es un enfoque estratégico utilizado para proteger instalaciones o activos críticos que se utiliza en los ejércitos. Este modelo se basa en la idea de que la seguridad debe implementarse en múltiples niveles o capas, formando anillos alrededor de un objetivo central, en el cada anillo representa un nivel de seguridad que protege el siguiente y dentro de cada anillo, se pueden formar grupos o equipos de seguridad responsables de monitorear y gestionar la seguridad en su área asignada. Este mismo modelo se puede aplicar a la seguridad de la información en el que a cada objeto de seguridad (archivo, computadora, puerto, etc) tiene asignado un grupo y un nivel mínimo de acceso. Paralelamente, cada usuario tiene asignado un grupo y un nivel de acceso y la autorización a un elemento se da si y solo si el objeto y el usuario están en el mismo grupo y si el nivel de acceso del usuario es mayor o igual que el nivel de acceso requerido por el usuario.

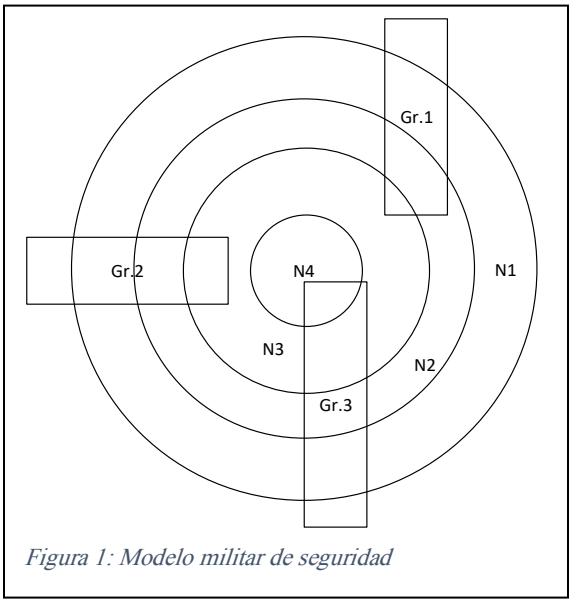

Figura 1: Modelo militar de seguridad

Si se compara con un esquema en el que se almacena (objeto, usuario), el modelo militar requiere un menor número de tuplas, lo que en un sistema complejo puede ser determinante para el rendimiento del sistema.

3 Auditoría

La auditoría y el manejo adecuado de las bitácoras dentro de la seguridad de los sistemas informáticos es un tema fundamental, son temas de importancia crítica, no solo por la seguridad misma, sino también por la capacidad de deducir responsabilidades de manera clara y objetiva en caso de que surjan problemas o incidentes.

A lo largo del tiempo, hemos visto que las bitácoras en las aplicaciones cumplen una función vital: registrar las acciones y decisiones del sistema, así como las interacciones con el usuario. En el pasado, por ejemplo, las aplicaciones solían incluir preguntas como "¿Está seguro de que desea realizar esta acción?", "¿Está seguro de que quiere revertir esta transacción?". Estas preguntas eran una manera de involucrar al usuario, asegurando que cualquier acción importante fuera confirmada por él antes de proceder. A continuación, el sistema registraba los datos relevantes: la identidad del usuario, la acción que realizó y el estado general de la máquina en ese momento.

Este proceso, aunque en principio parecía simple, tiene un objetivo fundamental: garantizar que, en caso de que ocurra un incidente, sea posible identificar quién fue responsable y bajo qué circunstancias. A menudo, el sistema puede ser culpado por fallos que, en realidad, pueden ser consecuencia de decisiones humanas o de una interacción inapropiada. Al contar con una bitácora detallada, la organización puede demostrar que el usuario fue quien dio la orden o cometió el error, y no el sistema en s

- Post mortem:
    - La auditoría sucede después de realizadas las acciones, aunque el tiempo pueda ser mínimo
    - Caso de las tarjetas de crédito
- Bitácoras sin información sensible
- Deducir responsabilidades: definir las acciones realizadas por un usuario.
- Detección de ataques: Una auditoría constante permite detectar posibles ataques al sistema
- Oportunidad de mejoras al realizar análisis de bitácoras
    - Errores frecuentes
    - Tiempo de ejecución de procesos y servicios.

3.1 Medios de bitácoras

El almacenamiento de bitácoras puede realizarse en diferentes medios: textos, bases de datos o utilizar servicios del sistema. Cada uno tiene sus ventajas y desventajas:

- Textos:
    - Es lo más común
    - Facilidad de implementación
    - Consideraciones de rendimiento y concurrencia
    - Complejidad de análisis
- Bases de datos:
    - Tabla con campos fijos y variables:

        - Usuario
        - IP
        - Fecha y hora
        - Operación realizada
        - Nivel de información: error, warning, info, debug
        - Descripción (variable)
    - Mejor estructuración para análisis y reportes
    - Mejor administración de la concurrencia
    - Capa adicional de software
    - Interferencia de las consultas con la operación diaria
    - Mantenimiento de la base de datos
- Servicio del sistema:
    - Eficiencia de registro (desde el punto de vista del proceso)
    - Posibilidad de bitácora remota
    - El almacenamiento puede ser en texto o base de datos
    - ej Syslog

3.2 Mantenimiento de bitácoras

- Respaldo
- Liberación de espacio
- Constante: usar mecanismos automáticos
- En cualquier medio de almacenamiento
- Linux: logrotate