UNIDAD V:

SEGURIDAD Y RESPALDO DE LA INFORMACIÓN

Conceptos y objetivos de protección

La protección es un mecanismo control de acceso de los programas, procesos o usuarios al sistema o recursos.

Hay importantes razones para proveer protección. La más obvia es la necesidad de prevenirse de violaciones intencionales de acceso por un usuario. Otras de importancia son, la necesidad de asegurar que cada componente de un programa, use solo los recursos del sistema de acuerdo con las políticas fijadas para el uso de esos recursos.

Un recurso desprotegido no puede defenderse contra el uso no autorizado o de un usuario incompetente. Los sistemas orientados a la protección proveen maneras de distinguir entre uso autorizado y desautorizado.

Objetivos

1.- Inicialmente protección del SO frente a usuarios poco confiables.

2.- Protección: control para que cada componente activo de un proceso solo pueda acceder a los recursos especificados, y solo en forma congruente con la política establecida.

3.- La mejora de la protección implica también una mejora de la seguridad.

4.- Las políticas de uso se establecen:

- Por el hardware.
- Por el administrador / SO.
- Por el usuario propietario del recurso.

5.- Principio de separación entre mecanismo y política:

Mecanismo → con que elementos (hardware y/o software) se realiza la protección.

Política → es el conjunto de decisiones que se toman para especificar como se usan esos elementos de protección.

6.- La política puede variar

• Dependiendo de la aplicación, y

• A lo largo del tiempo.

7.-La protección no solo es cuestión del administrador, sino también del usuario.

8.-El sistema de protección debe:

- Distinguir entre usos autorizados y no-autorizados.
- Especificar el tipo de control de acceso impuesto.
- Proveer medios para el aseguramiento de la protección.

Funciones del sistema de protección

Control de acceso que hace referencia a las características de seguridad que controlan quien puede obtener acceso a los recursos de un sistema operativo. Las aplicaciones llaman a las funciones de control de acceso para establecer quien puede obtener acceso a los recursos específicos o controlar el acceso a los recursos proporcionados por la aplicación.

Un sistema de protección deberá tener la flexibilidad suficiente para poder imponer una diversidad de políticas y mecanismos.

Existen varios mecanismos que pueden usarse para asegurar los archivos, segmentos de memoria, CPU, y otros recursos administrados por el Sistema Operativo.

Por ejemplo, el direccionamiento de memoria asegura que unos procesos puedan ejecutarse solo dentro de sus propios espacios de dirección. El timer asegura que los procesos no obtengan el control de la CPU en forma indefinida.

La protección se refiere a los mecanismos para controlar el acceso de programas, procesos, o usuarios a los recursos definidos por un sistema de computación. Seguridad es la serie de problemas relativos a asegurar la integridad del sistema y sus datos.

Mecanismos y Políticas

El sistema de protección tiene la función de proveer un mecanismo para el fortalecimiento de las políticas que gobiernan el uso de recursos. Tales políticas se pueden establecer de varias maneras, algunas en el diseño del sistema y otras son formuladas por el administrador del sistema. Otras pueden ser definidas por los usuarios individuales para proteger sus propios archivos y programas.

Las políticas son diversas, dependen de la aplicación y pueden estar sujetas a cambios a lo largo del tiempo.

Un principio importante es la separación de políticas de los mecanismos. ‘Los mecanismos determinan como algo se hará. Las políticas deciden que se hará'.

La separación es importante para la flexibilidad del sistema.

Dentro de las funciones del sistema de protección del sistema encontramos:

- Controlar el acceso a los recursos
- Asegurarse que todos los accesos a los recursos del sistema están controlados

Diferencias entre las distintas formas de protección:

Seguridad: La obligación de cumplimiento por núcleo ofrece un grado de seguridad que el código de seguridad ofrecido por el compilador.

Flexibilidad: La flexibilidad de la implementación por núcleo es limitada. Si un lenguaje no ofrece suficiente flexibilidad, se puede extender o sustituir, perturbando menos cambios en el sistema que si tuviera que modificarse el núcleo.

Eficiencia: Se logra mayor eficiencia cuando el hardware apoya la protección. La especificación de protección en un lenguaje de programación permite describir en alto nivel las políticas de asignación y uso de recursos.

La especificación de protección en un lenguaje de programación permite describir en alto nivel las políticas de asignación y uso de recursos. El programador de aplicaciones necesita un mecanismo de control de acceso seguro y dinámico para distribuir capacidades a los recursos del sistema entre los procesos de usuario.

Las construcciones que permiten al programador declarar las restricciones tienen tres operaciones básicas

Distribuir capacidades de manera segura y eficiente entre procesos clientes.

Especificar el tipo de operaciones que un proceso podría invocar en un recurso asignado.

Especificar el orden en que un proceso dado puede invocar las operaciones de un recurso.

La especificación de protección en un lenguaje de programación permite la descripción de alto nivel de políticas para la asignación y uso de recursos.

La implementación del lenguaje puede proveer software para hacer cumplir la protección cuando no se pueda validar si el hardware está soportado.

Interpretar las especificaciones de protección para generar llamadas en cualquier sistema de protección provisto por el hardware y el SO.

Concepto de seguridad

Los términos seguridad y protección se utilizan en forma indistinta. Sin embargo, es útil hacer una distinción entre los problemas generales relativos a la garantía de que los archivos no sea leídos o modificados por personal no autorizado, lo que incluye aspectos técnicos, de administración, legales y políticos, por un lado y los sistemas

específicos del sistema operativo utilizados para proporcionar la seguridad, por el otro. Para evitar la confusión, utilizaremos el termino seguridad para referirnos al problema general y el termino mecanismo de protección para referirnos a los mecanismos específicos del sistema operativo utilizado para resguardar la información de la computadora. Sin embargo, la frontera entre ellos no está bien definida.

La seguridad tiene muchas facetas. Dos de las más importantes son la perdida de datos y los intrusos. Algunas de las causas más comunes de la perdida de datos son:

- Actos divinos: Incendios, inundaciones, terremotos, guerras, revoluciones o ratas que roen las cintas o discos flexibles.

- Errores de Hardware o Software: Mal funcionamiento de la CPU, discos o cintas ilegibles, errores de telecomunicación o errores en el programa.

- Errores Humanos: Entrada incorrecta de datos, mal montaje de las cintas o el disco, ejecución incorrecta del programa, perdida de cintas o discos.

La mayoría de estas causas se pueden enfrentar con el mantenimiento de los respaldos adecuados; de preferencia, en un lugar alejado de los datos originales.

Un problema más interesante es que hacer con los intrusos. Estos tienen dos variedades. Los intrusos pasivos solo desean leer archivos que no están autorizados a leer.

Los intrusos activos son más crueles: Desean hacer cambios no autorizados a los datos. Si se desea diseñar un sistema seguro contra los intrusos, es importante tener en cuenta el tipo de intruso con el que se desea tener protección. Algunas de las **categorías comunes** son:

- **Curiosidad casual de usuarios no técnicos.** Muchas personas tienen en sus escritorios terminales para sistemas con tiempo compartido y, por la naturaleza humana, algunos de ellos leerán el correo electrónico de los demás u otros archivos, si no existen barreras en frente de ellos. Por ejemplo, la mayoría del sistema UNIS tienen pre definido que todos los archivos se pueden leer de manera pública.

- **Conocidos husmeando.** Algunos estudiantes, programadores de sistemas, operadores y demás personal técnico consideran como un reto personal romper la seguridad del sistema de cómputo local. A menudo son muy calificados y están dispuestos a invertir una cantidad sustancial de su tiempo en este esfuerzo.

- **Un intento deliberado de hacer dinero**. Algunos programadores en banco han intentado penetrar un sistema bancario con el fin de robarle al banco. Los esquemas han variado desde cambiar el software para truncar y no redondear el interés, para quedarse con una pequeña fracción de dinero, hasta sacar dinero de las cuentas que no se han utilizado en anos o el "correo negro" .

- **Espionaje comercias o militar**. El espionaje indica un intento serio y fundamentado por parte de un competidor u otro país para robar programas, secretos comerciales, patentes, tecnología, diseño de circuitos, planes de comercialización, etc. A menudo, este intento implica la cobertura de cables o el levantamiento de antenas hacia la computadora con el fin de recoger su radiación electromagnética.

Otro aspecto del problema de la seguridad es la privacidad: la protección de las personas respecto del mal uso de la información en contra de uno mismo. Esto implica en forma casi inmediata muchos aspectos morales y legales.

Para proteger un sistema, debemos optar las necesarias medidas de seguridad en cuatro niveles distintos:

Físico. El nodo o nodos que contengan los sistemas informáticos deben dotarse de medidas de seguridad físicas frente a posibles intrusiones armadas o subrepticias por parte de potenciales intrusos. Hay que dotar de seguridad tanto a las habitaciones donde las maquinas residan como a los terminales o estaciones de trabajo que tengan acceso a dichas maquinas.

Humano. La autorización de los usuarios debe llevarse a cabo con cuidado, para garantizar que solo los usuarios apropiados tengan acceso al sistema. Sin embargo, incluso los usuarios autorizados pueden verse “motivados” para permitir que otros usen su acceso (por ejemplo, a cambio de un soborno). También pueden ser engañados para permitir el acceso de otros, mediante técnicas de ingeniería social. Uno de los tipos de ataque basado en las técnicas de ingeniería social es el

denominado phishing ; con este tipo de ataque, un correo electrónico o página web de aspecto autentico llevan a engaño a un usuario para que introduzca información confidencial. Otra técnica comúnmente utilizada es el análisis de desperdicios, un término autorizado a la computadora (por ejemplo, examinando el contenido de las papeleras, localizando listines de teléfonos encontrando notas con contraseñas). Estos problemas de seguridad son cuestiones relacionadas con la gestión y con el personal, más que problemas relativos a los sistemas operativos.

Sistema operativo. El sistema debe auto protegerse frente a los diversos fallos de seguridad accidentales o premeditados. Un problema que este fuera de control puede llegar a constituir un ataque accidental de denegación de servicio. Asimismo, una cierta consulta a un servicio podría conducir a la revelación de contraseñas o un desbordamiento de la pila podría permitir que se iniciara un proceso no autorizado. La lista de posibles fallos es casi infinita.

Red. Son muchos los datos en los modernos sistemas informáticos que viajen a través de líneas arrendadas privadas, de líneas compartidas como Internet, de conexiones inalámbricas o de líneas de acceso telefónico. La interceptación de estos datos podría ser tan dañina como el acceso a un computador, y la interrupción en la comunicación podría constituir un ataque remoto de denegación de servicio, disminuyendo la capacidad de uso del sistema y la confianza en el mismo por parte de los usuarios.

Si queremos poder garantizar la seguridad del sistema operativo, es necesario garantizar la seguridad en los primeros dos niveles. Cualquier debilidad en uno de los niveles altos de seguridad (físico o humano) podría puentear las medidas de seguridad que son estrictamente de bajo nivel (del nivel del sistema operativo). Así, la frase que afirma que una cadena es tan fuerte como el más débil de sus eslabones es especialmente cierta cuando hablamos de seguridad de los sistemas. Para poder mantener la seguridad, debemos contemplar todos estos aspectos.

Además, el sistema debe proporcionar mecanismos de protección para permitir la implementación de las características de seguridad. Sin la capacidad de autorizar a los usuarios y procesos, de controlar su acceso y de registrar sus actividades, sería imposible que un sistema operativo implementara medidas de seguridad o se ejecutara de forma segura. Para soportar un esquema global de protección hacen falta mecanismos de protección hardware. Por ejemplo, un sistema donde la memoria no esté protegido no puede nunca estar seguro.

Clasificaciones de la seguridad

La seguridad **interna** está relacionada a los controles incorporados al hardware y al Sistema Operativo para asegurar los recursos del sistema.

La seguridad **externa** consiste en:

- Seguridad física.
- Seguridad operacional.

La seguridad física incluye:

- Protección contra desastres(como inundaciones, incendios, etc.).
- Protección contra intrusos.

En la seguridad física son importantes los mecanismos de detección , algunos ejemplos son:

- Detectores de humo.
- Sensores de calor.
- Detectores de movimiento.

La protección contra desastres puede ser costosa y frecuentemente no se analiza en detalle; depende en gran medida de las consecuencias de la perdida.

La seguridad física trata especialmente de impedir la entrada de intrusos:

Se utilizan sistemas de identificación física:

- Tarjetas de identificación.
- Sistemas de huellas digitales.
- Identificación por medio de la voz.
- Seguridad Operacional

Consiste en las diferentes políticas y procedimientos implementados por la administración de la instalación computacional.

La autorización determina que acceso se permite y a quien.

La clasificación divide el problema en subproblemas:

Los datos del sistema y los usuarios se dividen en clases:

A las clases se conceden diferentes derechos de acceso.

Un aspecto critico es la selección y asignación de personal:

La pregunta es si se puede confiar en la gente.

El tratamiento que generalmente se da al problema es la división de responsabilidades:

Se otorgan distintos conjuntos de responsabilidades.

No es necesario que se conozca la totalidad del sistema para cumplir con esas responsabilidades.

Para poder comprometer al sistema puede ser necesaria la cooperación entre muchas personas:

Se reduce la probabilidad de violar la seguridad.

Debe instrumentarse un gran número de verificaciones y balances en el sistema para ayudar a la detección de brechas en la seguridad.

El personal debe estar al tanto de que el sistema dispone de controles, pero:

Debe desconocer cuáles son esos controles:

Se reduce la probabilidad de poder evitarlos.

Debe producirse un efecto disuasivo respecto de posibles intentos de violar la seguridad.

Para diseñar medidas efectivas de seguridad se debe primero:

- Enumerar y comprender las amenazas potenciales.
- Definir qué grado de seguridad se desea (y cuanto se está dispuesto a gastar en seguridad).
- Analizar las contramedidas disponibles.

Validación y amenazas al sistema

Identificar cada usuario que está trabajando en el sistema (usando los recursos).

Uso de contraseñas.

Vulnerabilidad de contraseñas.

1.- Que sean complejas y difíciles de adivinar.

2.- Cambiarlas de vez en cuando.

3.- Peligro de pérdida del secreto.

La contraseña debe guardar cifrado.

Protección por Contraseña

Las clases de elementos de autentificación para establecer la identidad de una persona son:

Algo sobre la persona:

Ej.: huellas digitales, registro de la voz, fotografía, firma, etc.

Algo poseído por la persona:

Ej.: insignias especiales, tarjetas de identificación, llaves, etc.

Algo conocido por la persona:

Ej.: contraseñas, combinaciones de cerraduras, etc.

El esquema más común de autentificación es la protección por contraseña:

El usuario elige una palabra clave, la memoriza, la teclea para ser admitido en el sistema computarizado:

La clave no debe desplegarse en pantalla ni aparecer impresa.

La protección por contraseñas tiene ciertas desventajas si no se utilizan criterios adecuados para elegir las contraseñas y comunicarlas fehacientemente en caso de que sea necesario:.

- Destruir las contraseñas luego de que han sido comunicadas.
- Modificarlas luego de algún tiempo.
- Los usuarios tienden a elegir contraseñas fáciles de recordar:
- Nombre de un amigo, pariente, perro, gato, etc.
- Numero de documento, domicilio, patente del auto, etc.
- Estos datos podrían ser conocidos por quien intente una violación a la seguridad mediante intentos repetidos, por lo tanto, debe limitarse la cantidad de intentos fallidos de acierto para el ingreso de la contraseña.
- La contraseña no debe ser muy corta para no facilitar la probabilidad de acierto.
- Tampoco debe ser muy larga para que no se dificulte su memorización, ya que los usuarios la anotarían por miedo a no recordarla y ello incrementaría los riesgos de que trascienda.

Contraseñas de un solo uso

- Al final de cada sesión, se le pide al usuario que cambie la contraseña.

- Si alguien “roba una contraseña”, el verdadero usuario se dará cuenta cuando vaya a identificarse de nuevo, pues el impostor habrá cambiado la contraseña, con lo que el fallo de seguridad queda detectado.