Unidad VI: Protección y seguridad

6.1 Concepto 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

- Inicialmente protección del SO frente a usuarios poco confiables.
- 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.
- La mejora de la protección implica también una mejora de la seguridad.
- Las políticas de uso se establecen:
- Por el hardware.
- Por el administrador / SO.
- Por el usuario propietario del recurso.
- 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.

• La política puede variar

• dependiendo de la aplicación,

• A lo largo del tiempo.

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

• 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.

6.2 Funciones del sistema de protección

Control de acceso que hace referencia a las caracteristicas 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 especificos o controlar el acceso a los recursos proporcionados por la aplicacion.

Un sistema de proteccion debera tener la flexibilidad suficiente para poder imponer una diversidad de politicas 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 direccion. El timer asegura que los procesos no obtengan el control de la CPU en forma indefinida.

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

6.3 Implantación de matrices de acceso

Los *derechos de acceso* definen *que acceso* tienen varios sujetos sobre varios objetos.

Los sujetos acceden a los objetos.

Los *objetos* son entidades que contienen *informacion.*

Los *objetos* pueden ser:

- Concretos:
    - Ej.: discos, cintas, procesadores, almacenamiento, etc.
- Abstractos:
    - Ej.: estructuras de datos, de procesos, etc.

Los objetos estan *protegidos* contra los sujetos.

Las *autorizaciones* a un sistema se conceden *a los sujetos.*

Los *sujetos* pueden ser varios tipos de entidades:

- Ej.: usuarios, procesos, programas, otras entidades, etc.

Los *derechos de acceso* mas comunes son:

- Acceso de lectura.
- Acceso de escritura.
- Acceso de ejecucion.

6.4 Protección basada en el lenguaje

6.5 Concepto de seguridad

Los terminos seguridad y proteccion se utilizan en forma indistinta. Sin embargo, es util hacer una distincion entre los problemas generales relativos a la garantia de que los archivos no sea leidos o modificados por personal no autorizado, lo que incluye aspectos tecnicos, de administracion, legales y politicos, por un lado y los sistemas especificos del sistema operativo utilizados para proporcionar la seguridad, por el otro. Para evitar la confusion, utilizaremos el termino seguridad para referirnos al problema general y el termino mecanismo de proteccion para referirnos a los mecanismos especificos del sistema operativo utilizado para resguardar la informacion de la computadora. Sin embargo, la frontera entre ellos no esta bien definida. Primero nos fijaremos en la seguridad; mas adelante analizaremos la proteccion.

La seguridad tiene muchas facetas. Dos de las mas importantes son la perdida de datos y los intrusos. Algunas de las causas mas 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 telecomunicacion o errores en el programa.

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

6.6 Clasificaciones de la seguridad

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

Seguridad Externa

La *seguridad externa* consiste en:

- Seguridad fisica.
- Seguridad operacional.

La *seguridad fisica* incluye:

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

En la seguridad fisica son importantes los *mecanismos de deteccion* , algunos ejemplos son:

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

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

La *seguridad fisica* trata especialmente de impedir la entrada de intrusos:

- Se utilizan sistemas de *identificacion fisica:*
    - Tarjetas de identificacion.
    - Sistemas de huellas digitales.
    - Identificacion por medio de la voz.

Seguridad Operacional

Consiste en las *diferentes politicas y procedimientos* implementados por la administracion de la instalacion computacional.

La *autorizacion* determina que acceso se permite y a quien.

La *clasificacion* 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 *seleccion y asignacion de personal:*

- La pregunta es si se puede *confiar en la gente.*
- El tratamiento que generalmente se da al problema es la *division 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 cooperacion entre muchas personas:
        - Se reduce la probabilidad de violar la seguridad.
    - Debe instrumentarse un gran numero de verificaciones y balances en el sistema para ayudar a la deteccion de brechas en la seguridad.
    - El personal debe estar al tanto de que el sistema dispone de controles, pero:

        - Debe desconocer cuales son esos controles:
            - Se reduce la probabilidad de poder evitarlos.
        - Debe producirse un efecto disuasivo respecto de posibles intentos de violar la seguridad.

Para disenar *medidas efectivas de seguridad* se debe primero:

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

6.7 Validación y amenazas al sistema

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

• Uso de contrasenas.

• Vulnerabilidad de contrasenas.

    - o Que sean complejas y dificiles de adivinar.
    - o Cambiarlas de vez en cuando.
    - o Peligro de perdida del secreto.

• La contrasena debe guardare cifrada.

Proteccion por Contraseña

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

Algo *sobre la persona:*

    - Ej.: huellas digitales, registro de la voz, fotografia, firma, etc.
- Algo *poseido por la persona:*
    - Ej.: insignias especiales, tarjetas de identificacion, llaves, etc.
- Algo *conocido por la persona:*
    - Ej.: contrasenas, combinaciones de cerraduras, etc.

El esquema mas comun de autentificacion es la *proteccion por contrasena:*

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 proteccion por contrasenas tiene ciertas *desventajas* si no se utilizan criterios adecuados para:

Elegir las contrasenas.

- Comunicarlas fehacientemente en caso de que sea necesario.
- Destruir las contrasenas luego de que han sido comunicadas.
- Modificarlas luego de algun tiempo.

6.8 Cifrado

Existen muchas defensas frente a los ataques informáticos, que abarcan toda la gama que va desde la metodologia a la tecnologia. La herramienta de caracter mas general que esta a disposicion de los usuarios y de los disenadores de sistemas es la criptografia. En esta seccion vamos a explicar algunos detalles acerca de la criptografia y de su uso en el campo de la seguridad informatica.

En una computadora aislada, el sistema operativo puede determinar de manera fiable quienes son el emisor y el receptor de todas las comunicaciones

interprocesos, ya que el sistema operativo controla todos los canales de comunicaciones de la computadora. En una red de computadoras, la situacion es bastante distinta. Una computadora conectada a la red recibe bits desde el exterior, y no tiene ninguna forma inmediata y fiable de determinar que maquina o aplicacion ha enviado esos bits. De forma similar, la propia computadora envia bits hacia la red sin tener ninguna forma de determinar quien puede llegar a recibirlos.