TECNOLÓGICO NACIONAL DE MEXICO
INSTITUTO TECNOLÓGICO DE CIUDAD MADERO

Carrera: Sistemas Computacionales

Investigación Unidad 6.

Alumno:

Reyes Villar Luis Ricardo | 21070343

Profesor: David Alejandro Girón Mendoza

Materia: Sistemas Operativos

Hora: 10:00 – 11:00 hrs

Grupo: 3505-A

Semestre: Agosto 2023 – Diciembre 2023

6.4. Implantación de matrices de acceso.

Un modelo de protección puede ser visto abstractamente como una matriz, llamada matriz de derecho. Los renglones de la matriz representan dominios y las columnas representan objetos. Cada entrada en la matriz contiene un conjunto de derechos 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 información. Dado que los objetos son definidos explícitamente por la columna, se puede omitir el nombre del objeto en el derecho de acceso. La entrada "Matriz [i, j]" define el conjunto de operaciones que un proceso ejecutándose en el dominio "Dj" puede realizar sobre el objeto "Oj".

Matriz de Acceso: Es una representación abstracta del concepto de dominio de protección. La matriz cuenta con tantas columnas como objetos / recursos y tantas filas como dominios.

Las celdas contienen los accesos los cuales son los derechos de acceso que tienen los procesos que se ejecutan en ese dominio sobre el correspondiente objeto.

El mecanismo de protección es la matriz, junto con todos los elementos que se han de añadir para que se cumplan de manera efectiva todas las restricciones de acceso a los objetos.

- La política consiste en decidir cómo rellenar las distintas celdas de la matriz.
- La matriz de acceso permite implementar operaciones de cambio de domino.
- El objeto sobre el que trabajamos es el Dominio.
- Aparecen tantas columnas como dominios en el sistema.
- La operación es la conmutación de un dominio a otro.

Los objetos se dividen en dos tipos:

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

Los objetos están 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 más comunes son:

- Acceso de lectura.
- Acceso de escritura.
- Acceso de ejecución.

Una forma de implementación es mediante una matriz de control de acceso con:

- Filas para los sujetos.
- Columnas para los objetos.
- Celdas de la matriz para los derechos de acceso que un usuario tiene a un objeto.
- Una matriz de control de acceso debe ser muy celosamente protegida por el S. O.

6.7. Cifrado.

La gran desventaja de las llaves secretas es que requieren un canal seguro para ser distribuidas. Si una contraseña es enviada por un canal inseguro puede ser interceptada, y no habría manera de lograr que quien la intercepte descifre con ella los mensajes enviados, o evitar que modifique o envié mensajes falsificando su identidad. No siempre disponemos de un canal seguro. Lo que, es más, estrictamente hablando, los canales seguros simplemente no existen. Sea como sea que la información sea transmitida, siempre podrá ser escuchada por un tercero. Si hace falta tener un canal seguro para intercambiar las contraseñas, la utilidad de las contraseñas se vuelve nula.

El cifrado es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo. Por ejemplo, si realiza una compra a través de Internet, la información de la transacción (como su dirección, número de teléfono y número de tarjeta de crédito) suele cifrarse a fin de mantenerla a salvo. El cifrado es usado cuando desee un alto nivel de protección de la información.

Métodos y Técnicas de Cifrado:

Cifrado de sustitución.

El cifrado de sustitución consiste en reemplazar una o más entidades (generalmente letras) de un mensaje por una o más entidades diferentes.

Existen varios tipos de criptosistemas de sustitución:

- La sustitución mono alfabética consiste en reemplazar cada una de las letras del mensaje por otra letra del alfabeto.
- La sustitución poli alfabética consiste en utilizar una serie de cifrados mono alfabéticos que son reutilizados periódicamente.
- La sustitución homófona hace posible que cada una de las letras del mensaje del texto plano se corresponda con un posible grupo de caracteres distintos.
- La sustitución poligráfica consiste en reemplazar un grupo de caracteres en un mensaje por otro grupo de caracteres.

Cifrado César.

Este código de cifrado es uno de los más antiguos ya que su uso se remonta a Julio César. El principio de cifrado se basa en la adición de un valor constante a todos los caracteres de un mensaje o, más precisamente, a su código ASCII.

Cifrado ROT 13.

El caso específico del cifrado César donde la clave de cifrado es N (la 13º letra del alfabeto) se denomina ROT 13.

Se eligió el número 13, la mitad de 26, para que sea posible cifrar y descifrar fácilmente mensajes textuales.

Cifrado de Transposición.

El método de cifrado por transposición consiste en reordenar datos para cifrarlos a fin de hacerlos ininteligibles. Esto puede significar, por ejemplo, reordenar los datos geométricamente para hacerlos visualmente inutilizables.

Cifrado simétrico.

Los sistemas de cifrado simétrico son aquellos que utilizan la misma clave para cifrar y descifrar un documento. El principal problema de seguridad reside en el intercambio de claves entre el emisor y el receptor, ya que ambos deben usar la misma clave. Por lo tanto, se tiene que buscar también un canal de comunicación que sea seguro para el intercambio de la clave. Es importante que dicha clave sea

muy difícil de adivinar, ya que en la actualidad los ordenadores pueden adivinar claves muy rápidamente. Por ejemplo, el algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 72 mil billones de claves posibles. Actualmente ya existen ordenadores especializados que son capaces de probar todas ellas en cuestión de horas. Actualmente se utilizan claves de 128 bits que aumentan el "espectro" de claves posibles (2^{128}) de forma que aunque se uniesen todos los ordenadores existentes en estos momentos no lo conseguirían en miles de millones de años.

Cifrado asimétrico.

También son llamados sistemas de cifrado de clave pública. Este sistema de cifrado usa dos claves diferentes. Una es la clave pública y se puede enviar a cualquier persona y otra que se llama clave privada, que debe guardarse para que nadie tenga acceso a ella. Para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrar el mensaje. Una vez que lo ha cifrado, solamente con la clave privada del destinatario se puede descifrar, ni siquiera el que ha cifrado el mensaje puede volver a descifrarlo. Por ello, se puede dar a conocer perfectamente la clave pública para que todo aquel que se quiera comunicar con el destinatario lo pueda hacer.

Un sistema de cifrado de clave pública basado en la factorización de números primos se basa en que la clave pública contiene un numero compuesto de dos números primos muy grandes. Para cifrar un mensaje, el algoritmo de cifrado usa ese compuesto para cifrar el mensaje. Para descifrar el mensaje, el algoritmo de descifrado requiere conocer los factores primos, y la clave privada tiene uno de esos factores, con lo que puede fácilmente descifrar el mensaje.

Es fácil, con los ordenadores de hoy en día, multiplicar dos números grandes para conseguir un número compuesto, pero es muy difícil la operación inversa, Dado ese número compuesto, factorizarlo para conocer cada uno de los dos números. Mientras que 128 bits se consideran suficiente en las claves de cifrado simétrico, y dado que la tecnología de hoy en día se encuentra muy avanzada, se recomienda en este caso que la clave pública tenga un mínimo de 1024 bits. Para un ataque de fuerza bruta, por ejemplo, sobre una clave publica de 512 bits, se debe factorizar un numero compuesto de hasta 155 cifras decimales.

Autenticación.

Autenticación (Griego: αυθεντικ = verdadero o genuino, de ' los authentes' = el autor) es el acto de establecimiento o confirmación de algo (o alguien) como autentico, es decir que reclama el hecho de que por o sobre la cosa es verdadero. La autenticación de un objeto puede significar (pensar) la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad. La autenticación depende de uno o varios factores de autenticación.

En términos de seguridad de redes de datos, se puede considerar uno de los tres pasos fundamentales (AAA). Cada uno de ellos es, de forma ordenada:

Autenticación En la seguridad de ordenador, la autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador. En una web de confianza, "autenticación" es un modo de asegurar que los usuarios son quien ellos dicen que ellos son, es decir, que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer eso.

Mecanismo general de autenticación

La mayor parte de los sistemas informáticos y redes mantienen de uno u otro modo una relación de identidades personales (usuarios) asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación de usuarios permite a estos sistemas asumir con una seguridad razonable que quien se está conectando es quien dice ser para que luego las acciones que se ejecuten en el sistema puedan ser referidas luego a esa identidad y aplicar los mecanismos de autorización y/o auditoria oportunos.

El primer elemento necesario (y suficiente, estrictamente hablando) por tanto, para la autenticación, es la existencia de identidades biunívocamente identificadas con un identificador único. Los identificadores de usuarios pueden tener muchas formas siendo la más común una sucesión de caracteres conocida comúnmente como login.

El proceso general de autenticación consta de los siguientes pasos:

1. El usuario solicita acceso a un sistema.
2. El sistema solicita al usuario que se autentique.
3. El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación.
4. El sistema valida según sus reglas si las credenciales aportadas son suficientes para dar acceso al usuario o no.

Referencias.

https://misistema-operativo.blogspot.com/p/63-implantacion-de-matrices-de-acceso.html

https://so-sistemas-operativoss.blogspot.com/2017/12/64-implantacion-de-matrices-de-acceso.html

https://so-sistemas-operativoss.blogspot.com/2017/12/67-cifrado.html

https://misistema-operativo.blogspot.com/p/67-cifrado.html