Instituto Politécnico Nacional

Escuela Superior de Cómputo

Sistemas Operativos

"Tarea 1. Seguridad"

Grupo: 2CM9

Integrantes:

- Martínez Coronel Brayan Yosafat
- Monteros Cervantes Miguel Angel
- Ramírez Olvera Guillermo
- Sánchez Méndez Edmundo Josué

Profesor: Cortés Galicia Jorge

Definiciones de Seguridad

Se dice que un sistema es seguro si sus recursos se utilizan de forma prevista y se accede como se pretendía

Existen dos tipos de violaciones de seguridad -Intencionadas (Maliciosas) - Accidentales

Una amenaza es la posibilidad de que exista una violación a la seguridad

Un ataque es un intento por romper la seguridad

Pueden haber distintos tipos de ataques como:

- Ruptura de confidencialidad
- Ruptura de la integridad
- Ruptura de la disponibilidad
- Robo de servicio
- Denegación de servios

La mascarada es un proceso común para romper la seguridad de un sistema, aquí uno de los participantes de la comunicación intenta ser otra persona

Los ataques de reproducción consisten en la repetición maliciosa o fraudulenta de una transmisión de datos valida

Un ataque por interposición consiste en hacerse pasar como emisor y receptor dependiendo del caso

Es imposible garantizar una protección absoluta del sistema

Para proteger un sistema, debemos tener medidas de seguridad en cuatro niveles distintos:

1. Físico
2. Humano
3. Sistema Operativo
4. Red

La mayoría de los Hackers busca crear una brecha de seguridad o trata de que un proceso normal cambie su comportamiento

Un segmento de código que utiliza inapropiadamente su entorno se le denomina Caballo de troya

Una puerta trasera es un agujero de software que solo el programado es capaz de utilizar

Una bomba lógica es un escenario donde diferentes circunstancias interactúan y generan un algún daño en el software

El desbordamiento de pila es el ataque más utilizado para tener acceso no autorizado al S.O.

Los virus pueden modificar o destruir archivos, provocando funcionamientos inadecuados de los sistemas

Implican el abuso de los servicios y de las conexiones

Los gusanos son procvesos que utilizan mecanismos de reproducción para afectar el rendimiento

El escaneo de puertos es un método que los hackers utilizan para detectar vulnerabilidades del sistema para atacarlas

Los ataques de denegación de servicio no están dirigidos para obtener información o para robar recursos, sino para impedir el uso légitimo del sistema

La criptología se utiliza para restringir los emisores y/o receptores potenciales

El cifrado es un medio de restringir lo posibles receptores de un mensaje

Un algoritmo de cifrado consta de los siguientes componentes:

- Un conjunto k de claves
- Un conjunto M de mensajes
- Un conjunto C de mensajes de texto cifrado

- Cifrado Asimétrico
  Se utiliza la misma clave para cifrar y descifrar
- Cifrado Simétrico
  En un algoritmo de cifrado asimétrico, las claves de cifrado y decifrado son distintas

La autenticación es en parte similar al cifrado, pero también puede ser utilizada para demostrar que un mensaje no ha sido modificado

Una función hash crea un pequeño bloque de datos de tamaño fijo conocidos como resumen de mensaje o valor hash

Los criptógrafos y criptoanalistas se encuentran en una batalla, ya que los algoritmos simétricos hacen que ambas partes necesiten la llave

Los protocolos de seguridad se ejcutan en los protocolos de comunicación en red, un ejemplo es SSL, el cual permite que dos computadoras se comuniquen de forma seura entre ellas

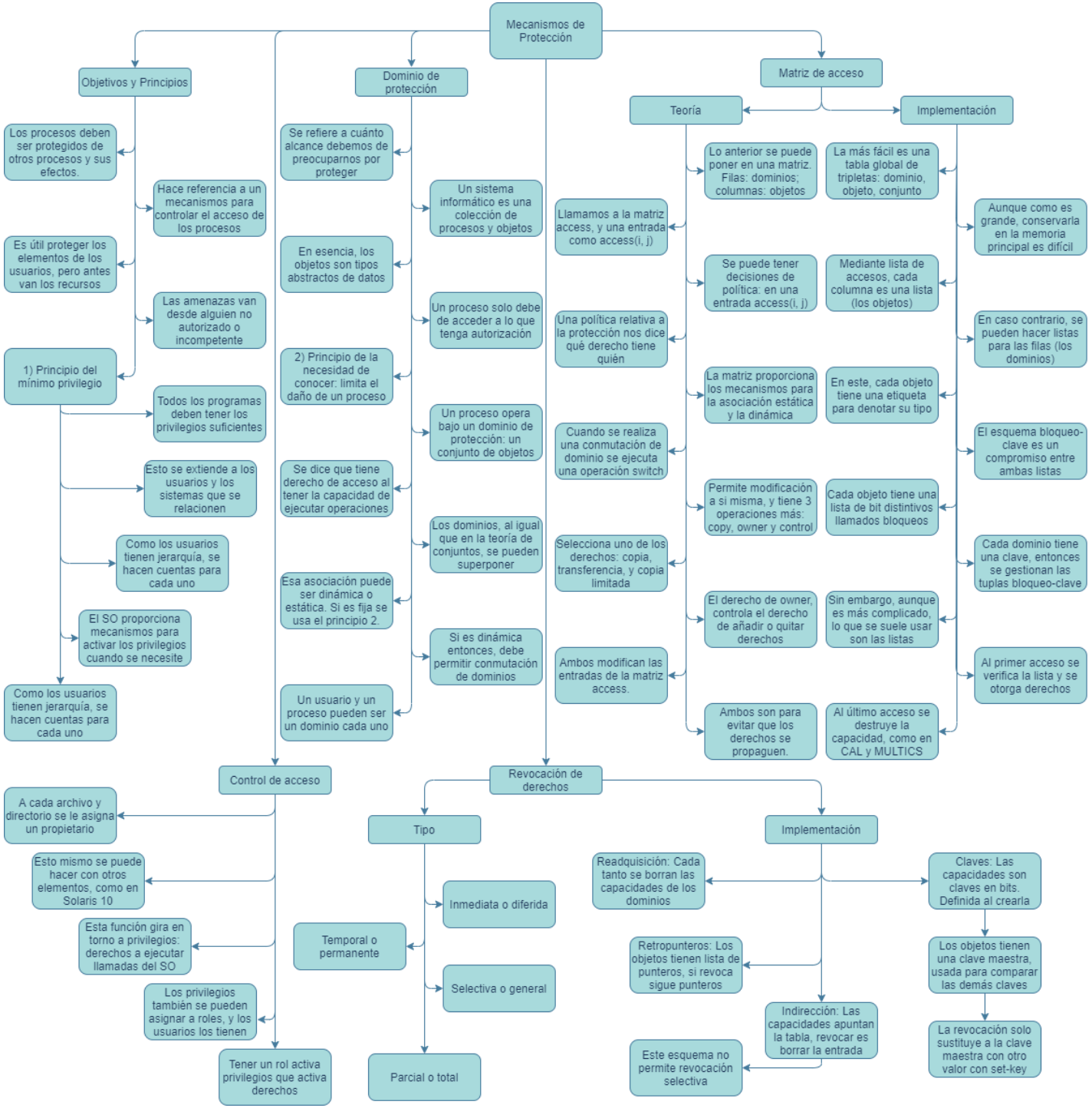
Por enzima de la autenticación de mensajes gracias a los diferentes protocolos, debemos primero autenticar a un usuario para validar la información

El modo más común para que un usuario se identifique es con un ID y una contraseña, pero estás pueden tener vulnerabilidades

Comúnmente se pueden adivinar, ser mostradas por accidente, se interceptadas o ilegalmente transferidas

Algunos sistemas utilizan un sistema de cifrado para evitar mantener en secreto la lista de contraseñas

Las contraseñas emparejadas consiste en que el sismeta otorga una parte de una contraseña, que a su vez pertenece a un conjunto de contraseñas, y el usuario debe poner el resto


Mecanismos de Protección
Objetivos y Principios
Los procesos deben ser protegidos de otros procesos y sus efectos.
Hace referencia a un mecanismos para controlar el acceso de los procesos
Es útil proteger los elementos de los usuarios, pero antes van los recursos
Las amenazas van desde alguien no autorizado o incompetente
1) Principio del mínimo privilegio
Todos los programas deben tener los privilegios suficientes
Esto se extiende a los usuarios y los sistemas que se relacionen
Como los usuarios tienen jerarquía, se hacen cuentas para cada uno
El SO proporciona mecanismos para activar los privilegios cuando se necesite
Como los usuarios tienen jerarquía, se hacen cuentas para cada uno
Dominio de protección
Se refiere a cuánto alcance debemos de preocuparnos por proteger
Un sistema informático es una colección de procesos y objetos
En esencia, los objetos son tipos abstractos de datos
Un proceso solo debe de acceder a lo que tenga autorización
2) Principio de la necesidad de conocer: limita el daño de un proceso
Un proceso opera bajo un dominio de protección: un conjunto de objetos
Se dice que tiene derecho de acceso al tener la capacidad de ejecutar operaciones
Los dominios, al igual que en la teoría de conjuntos, se pueden superponer
Esa asociación puede ser dinámica o estática. Si es fija se usa el principio 2.
Si es dinámica entonces, debe permitir conmutación de dominios
Un usuario y un proceso pueden ser un dominio cada uno
Matriz de acceso
Teoría
Llamamos a la matriz access, y una entrada como access(i, j)
Una política relativa a la protección nos dice qué derecho tiene quién
Cuando se realiza una conmutación de dominio se ejecuta una operación switch
Selecciona uno de los derechos: copia, transferencia, y copia limitada
Ambos modifican las entradas de la matriz access.
Lo anterior se puede poner en una matriz. Filas: dominios; columnas: objetos
Se puede tener decisiones de política: en una entrada access(i, j)
La matriz proporciona los mecanismos para la asociación estática y la dinámica
Permite modificación a si misma, y tiene 3 operaciones más: copy, owner y control
El derecho de owner, controla el derecho de añadir o quitar derechos
Ambos son para evitar que los derechos se propaguen.
Implementación
La más fácil es una tabla global de tripletas: dominio, objeto, conjunto
Mediante lista de accesos, cada columna es una lista (los objetos)
En este, cada objeto tiene una etiqueta para denotar su tipo
Cada objeto tiene una lista de bit distintivos llamados bloqueos
Sin embargo, aunque es más complicado, lo que se suele usar son las listas
Al último acceso se destruye la capacidad, como en CAL y MULTICS
Aunque como es grande, conservarla en la memoria principal es difícil
En caso contrario, se pueden hacer listas para las filas (los dominios)
El esquema bloqueo-clave es un compromiso entre ambas listas
Cada dominio tiene una clave, entonces se gestionan las tuplas bloqueo-clave
Al primer acceso se verifica la lista y se otorga derechos
Control de acceso
A cada archivo y directorio se le asigna un propietario
Esto mismo se puede hacer con otros elementos, como en Solaris 10
Esta función gira en torno a privilegios: derechos a ejecutar llamadas del SO
Los privilegios también se pueden asignar a roles, y los usuarios los tienen
Tener un rol activa privilegios que activa derechos
Revocación de derechos
Tipo
Inmediata o diferida
Temporal o permanente
Selectiva o general
Parcial o total
Implementación
Readquisición: Cada tanto se borran las capacidades de los dominios
Retropunteros: Los objetos tienen lista de punteros, si revoca sigue punteros
Indirección: Las capacidades apuntan la tabla, revocar es borrar la entrada
Este esquema no permite revocación selectiva
Claves: Las capacidades son claves en bits. Definida al crearla
Los objetos tienen una clave maestra, usada para comparar las demás claves
La revocación solo sustituye a la clave maestra con otro valor con set-key