Instituto Tecnológico de Costa Rica

Escuela de Ingeniería en Computación

Curso: Principios de Sistemas Operativos

Tercer Examen Parcial

1. (Cap.14 - 20 puntos) Describa en forma detallada el funcionamiento de las siguientes técnicas utilizadas para el manejo de las operaciones de E/S en sistemas computacionales.

    a. E/S programada: El módulo E/S ejecuta la acción solicitada cuando se establece los bits apropiados en el registro de estado de E/S pero no toma ninguna acción para alertar al procesador. Como no existen interrupciones, el procesador debe determinar cuando la instrucción se completa. Ventaja: Sencillo de implementar, no se requieren mecanismos especiales. Desventaja: El procesador se mantiene chequeando el estado mientras se realiza la lectura (espera ocupada).

    b. E/S basada en interrupciones: El procesador genera un comando de E/S a un módulo y luego va a hacer algún otro trabajo útil. El módulo de E/S podría entonces interrumpir al procesador para solicitar servicio cuando esté listo para intercambiar datos con el procesador. Ventaja: Elimina la espera innecesaria. Desventaja: Todo pasa a través del procesador y requiere mecanismos especiales (interrupciones).

    c. Acceso Directo a Memoria (DMA): Ejecutado por un módulo separado en el sistema. Cuando se necesita una lectura/escritura el procesador envía un comando al módulo DMA. Ventaja: El procesador solo es involucrado cuando se inicia y termina la transferencia. Mucho más eficiente. Desventaja: Solo es útil en transferencias grandes.

2. (Cap.15 - 20 puntos) Describa en forma detallada cada uno de los siguientes métodos utilizados para la revocación de derechos de acceso, bajo el esquema de protección llamado “capacidades”.

    a. Retropunteros
    b. Indirección
    c. Claves

3. (Cap.16 - 20 puntos) Describa en forma detallada los siguientes tipos de virus. En particular interesa conocer el mecanismo de activación, de ocultarse y de reproducirse, de cada uno de ellos.

    a. Archivo (ejecutable)

Un virus de archivo infecta un sistema insertándose a un archivo y modificando el inicio del programa para que la ejecución salte al código del virus. Luego regresan el control al programa para que no se pueda detectar. Este tipo de virus no dejan ningún archivo completo detrás suyo y permiten que el programa huésped siga funcionando.

b. Arranque

Un virus de arranque infecta el sector de arranque del sistema, ejecutándose cada vez que el sistema se arranca y antes que se cargue el sistema operativo. El virus busca otros soportes de arranque y también los infecta. Este tipo de virus no aparece en el sistema de archivos, sólo en memoria.

c. Macro

Los virus de macro están escritos en lenguaje de alto nivel, como Visual Basic. Estos virus se activan cuando se inicia un programa capaz de ejecutar la macro. Por ejemplo, un virus de macro podría estar escondido en un archivo de hoja de cálculo.

d. Código fuente

Un virus de código fuente busca código fuente (PHP, Python, etc.) y lo modifica para incluir el virus y ayudar a su distribución. El virus se esconde en subrutinas codificadas de forma complicada y que no puedan ser detectadas fácilmente.

e. Multiparte

Los virus de este tipo son capaces de infectar múltiples partes de un sistema, incluyendo los sectores de arranque, la memoria y los archivos. Esto hace que sea difícil detectarlos y evitgar su propagación.

4. (Cap. 16 - 20 puntos) Explique en forma detallada cada uno de los siguientes mecanismos de cifrado. En particular interesa conocer sus características principales, ventajas y desventajas.

a. Cifrado simétrico (llave única)

En un algoritmo de cifrado simétrico, se utiliza la misma clave para cifrar y descifrar, es decir, el mensaje desencriptado mediante una llave k puede deducirse a partir del mensaje encriptado con la misma llave k. Por tanto, es necesario proteger el secreto de la llave k. Generalmente, estos algoritmos funcionan tomando un valor de n bits y una clave de m bits y realizando una serie de transformaciones. Estas transformaciones están basadas en operaciones de sustitución y permutación. Estos algoritmos se consideran inseguros con llaves pequeñas. Por otra parte, la tarea de suministrar la clave simétrica a sus usuarios legítimos constituye un reto importante y resulta en uno de sus principales problemas.

b. Cifrado asimétrico (llave pública y privada)

   En un algoritmo de cifrado asimétrico, las claves de cifrado y descifrado son distintas. Comienza con la publicación de la clave pública del destino. La criptografía asimétrica se basa en funciones matemáticas lo que hace que sea mucho más cara, en términos de recursos computacionales que el cifrado simétrico y por tanto no se utiliza para el cifrado de grandes cantidades de datos. Uno de los ataques más comunes en contra del cifrado asimétrico es la interposición. En este caso, la persona que desea recibir un mensaje cifrado envía su clave pública, pero un atacante también envía su clave pública "mala". La persona que desea enviar el mensaje cifrado desconoce esto y utiliza la clave mala para cifrar el mensaje.

5. (Cap.17 - 20 puntos) Describa en forma detallada cada una de las siguientes técnicas utilizadas para verificar la validez de los datos almacenados en la caché de un sistema de archivos distribuidos. Adicionalmente, comente las ventajas y desventajas de cada tipo de técnica.

   1. Iniciado por parte cliente. El cliente inicia una comprobación de validez en la que contacta con el servidor y comprueba si los datos locales son coherentes con la copia maestra. La frecuencia puede variar, pudiendo realizarse la comprobación para cada acceso o solo en el primer acceso a un archivo (básicamente durante la apertura de un archivo); también puede utilizarse cualquier otra frecuencia entre estos dos extremos. Todos los accesos que lleven aparejada una comprobación de validez sufrirán un cierto retardo, comparados con los accesos a los que se de servicio inmediatamente utilizando los datos de la caché. Alternativamente, esas comprobaciones pueden iniciarse a intervalos de tiempo fijos. Dependiendo de su frecuencia, las comprobaciones de validez pueden imponer una gran carga tanto a la red como al servidor.

   2. Iniciado por parte del servidor. El servidor registra, para cada cliente, los archivos (o partes de los mismos) que estos tienen almacenados en cache. Cuando el servidor detecta una incoherencia potencial, debe reaccionar a la misma. Una posibilidad de incoherencia se produce cuando dos clientes distintos que operan con modos conflictivos almacenan en caché un mismo archivo. El servidor deberá ser notificado cada vez que se abra un archivo, y deberá indicarse el modo deseado (lectura o escritura) para cada apertura archivo. El servidor puede entonces actuar cuando detecte que el archivo ha sido abierto simultáneamente en modos conflictivos, desactivando en ese caso el mecanismo de caché para ese archivo concreto.