Universidad de Guadalajara.

Centro Universitario de Ciencias Exactas e Ingenierías.

DIVISIÓN DE TECNOLOGÍAS PARA LA INTEGRACIÓN CIBER-HUMANA.

DEPARTAMENTO DE CIENCIAS COMPUTACIONALES.

TEMA: Modo usuario y modo super usuario.

NOMBRE DEL ESTUDIANTE: Padilla Perez Jorge Daray.

NOMBRE DE LA MATERIA: Sistemas operativos

NOMBRE DEL PROFESOR: Ramiro Lupercio Coronel

Table of Contents

Modo Usuario y super usuario (Windows)

Modo Usuario

las aplicaciones se ejecutan de manera aislada, cada una con su propio espacio de direcciones virtuales privadas y una tabla de identificadores privados. Esto garantiza que, si una aplicación se bloquea, no afectará a otras aplicaciones ni al sistema operativo. Además, las aplicaciones en modo de usuario no pueden acceder a direcciones virtuales reservadas para el sistema operativo, lo que protege los datos críticos del sistema.

El sistema operativo gestiona muchos «procesos» al mismo tiempo, que son las tareas que realizan las aplicaciones. La CPU les da tiempo según lo que necesiten y lo que consuman de energía.

Al abrir una aplicación, se crean procesos, que pueden funcionar de dos formas: en modo usuario o en modo kernel.

Un proceso de Windows en modo usuario solo puede usar su propia memoria virtual y su tabla para manejarla. El software guarda datos en RAM y pide recursos con estas tablas. No puede acceder directamente a la memoria ni al hardware, y el sistema operativo se encarga de asignar esos espacios virtuales al hardware de la computadora.

Modo kernel (super usuario)

El modo kernel en Windows es una forma de ejecutar código que tiene acceso directo al hardware y la memoria del sistema. El modo kernel se usa para los componentes principales del sistema operativo, como el núcleo, los controladores de dispositivos y algunos servicios. El modo kernel ofrece más rendimiento y funcionalidad que el modo de usuario, pero también implica más riesgos de fallas y daños.

El sistema operativo tiene un componente esencial llamado Kernel o Núcleo. Su función es hacer que el software y el hardware del ordenador se comuniquen y coordinen en un mismo sistema. Para ello, gestiona la memoria y el tiempo de procesador que usan los programas y procesos, y permite que los periféricos y otros componentes físicos del equipo funcionen correctamente. Al abrir una aplicación, esta entra en el modo usuario, donde Windows le asigna un proceso propio. Cada aplicación solo puede usar su propia memoria virtual, y no puede modificar ni acceder a los datos de otras aplicaciones ni del sistema operativo. Este es el modo con menos privilegios, y el acceso al hardware es restringido. Las aplicaciones tienen que usar la API de Windows para solicitar los servicios del sistema.

El modo kernel es diferente, ya que el código que se ejecuta en él puede acceder a todo el hardware y la memoria del equipo. Todo el código tiene un espacio virtual compartido, y puede acceder a los espacios de memoria de todos los procesos del modo usuario. Esto es arriesgado, ya que si un driver en el modo kernel hace algo indebido podría afectar al funcionamiento de todo el sistema operativo.

Modo usuario y super usuario (Linux)

Modo usuario

El modo usuario Linux es una forma de ejecutar procesos que solo tienen acceso a su propio espacio de memoria virtual y a los recursos del sistema a través de las llamadas al sistema. El modo usuario Linux ofrece más protección y estabilidad que el modo kernel, ya que los procesos no pueden interferir ni dañar el hardware ni el núcleo del sistema operativo.

Usuarios normales

- Se usan para usuarios individuales.
- Cada usuario dispone de un directorio de trabajo, ubicado generalmente en /home.
- Cada usuario puede personalizar su entorno de trabajo.
- Tienen solo privilegios completos en su directorio de trabajo o HOME.
- Por seguridad, es siempre mejor trabajar como un usuario normal en vez del usuario root, y cuando se requiera hacer uso de comandos solo de root, utilizar el comando su.
- En las distros actuales de Linux se les asigna generalmente un UID superior a 500.

El modo de usuario es el modo en el que se ejecutan las aplicaciones de usuario, como un editor de texto, bajo el control del sistema operativo. Para acceder a los recursos del sistema o manejar una interrupción, las aplicaciones deben cambiar al modo kernel, que es el modo privilegiado. El bit de modo indica si el sistema está en modo de usuario (1) o en modo kernel (0). Linux en modo usuario (UML) es una forma de ejecutar Linux sobre Linux, usando una máquina virtual. El hardware de la máquina virtual es simulado por el sistema Linux anfitrión, que provee los recursos necesarios. UML permite ejecutar casi cualquier aplicación que se pueda ejecutar en el sistema anfitrión.

El modo de usuario y el modo kernel son dos formas distintas de operar la CPU (unidad central de procesamiento) en una computadora con Windows. El modo de usuario es el que usan las aplicaciones de usuario, y el modo kernel es el que usa el sistema operativo para acceder al hardware y a los recursos del sistema. La CPU cambia de un modo a otro dependiendo del tipo de código que se esté ejecutando.

Modo de usuario en Unix: Es el modo en que se ejecutan las aplicaciones de usuario, sin acceso directo al kernel ni al hardware.

Procesos que no pertenecen al kernel: Son los procesos que se ejecutan en modo de usuario, con su propia memoria protegida.

Protección y estabilidad: El modo de usuario evita que los procesos interfieran o dañen el sistema operativo o los demás procesos.

Modo super usuario

Usuario root

- También llamado superusuario o administrador.
- Su UID (User ID) es 0 (cero).
- Es la única cuenta de usuario con privilegios sobre todo el sistema.
- Acceso total a todos los archivos y directorios con independencia de propietarios y permisos.
- Controla la administración de cuentas de usuarios.
- Ejecuta tareas de mantenimiento del sistema.
- Puede detener el sistema.
- Instala software en el sistema.
- Puede modificar o reconfigurar el kernel, controladores, etc.

Usuarios especiales

- Ejemplos: bin, daemon, adm, lp, sync, shutdown, mail, operator, squid, apache, etc.
- Se les llama también cuentas del sistema.
- No tiene todos los privilegios del usuario root, pero dependiendo de la cuenta asumen distintos privilegios de root.
- Lo anterior para proteger al sistema de posibles formas de vulnerar la seguridad.
- No tienen contraseñas pues son cuentas que no están diseñadas para iniciar sesiones con ellas.
- También se les conoce como cuentas de "no inicio de sesión" (nologin).
- Se crean (generalmente) automáticamente al momento de la instalación de Linux o de la aplicación.
- Generalmente se les asigna un UID entre 1 y 100 (definifo en /etc/login.defs)

Cuenta root: Es la cuenta de usuario que tiene el máximo nivel de autoridad y control sobre el sistema operativo Linux. Puede ejecutar cualquier comando, modificar cualquier archivo y acceder a cualquier recurso del sistema.

Acceso root: Es la capacidad de ejecutar comandos o procesos como si fueran el usuario root. Se puede obtener mediante el comando su, que cambia el usuario actual por el root, o mediante el comando sudo, que ejecuta un comando específico como root.

Sistema de archivos: Es la forma en que Linux organiza y almacena los archivos y directorios en el disco duro. Algunos comandos que afectan al sistema de archivos son: fdisk, que crea y modifica

particiones; mkfs, que formatea una partición con un sistema de archivos específico; y mount, que monta una partición en un punto de acceso.

Seguridad y estabilidad: El uso de la cuenta root implica riesgos de seguridad y estabilidad, ya que puede comprometer la integridad del sistema operativo, los datos y el hardware. Por eso, se recomienda usarla solo cuando sea necesario y con precaución. Además, se aconseja establecer una contraseña segura para la cuenta root y bloquearla cuando no se use.

Conclusión:

Para concluir el modo usuario y el modo kernel son dos modos de la CPU que determinan el nivel de acceso al hardware y la memoria.El modo usuario es más seguro y estable, pero limita el acceso al hardware y requiere usar las API para pedir los servicios del sistema. El modo kernel es más rápido y funcional, pero más riesgoso y dañino. El modo kernel se usa para el núcleo, los drivers y algunos servicios del sistema operativo. En Windows y Linux, hay cuentas de superusuario que tienen acceso total al sistema, pero que deben usarse con cuidado.

Referencias:

Modo de usuario y modo kernel. (2021). Microsoft Docs. Recuperado el 17 de enero de 2024, de https://docs.microsoft.com/es-es/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode

wikiHow. (s. f.). Cómo ingresar como usuario root en Linux. Recuperado el 17 de enero de 2024, de https://es.wikihow.com/ingresar-como-usuario-root-en-Linux

¿Qué es el modo de usuario frente al modo kernel en Windows? (2024, 17 de enero)(sin autor). Recuperado de https://www.geeknetic.es/Windows/Que-es-el-modo-de-usuario-frente-al-modo-kernel-en-Windows.html

FM, Y. (2017, 16 de enero). Cómo es el Kernel de Windows y cuales son sus diferencias con el de Linux. Genbeta. https://www.genbeta.com/a-fondo/como-es-el-kernel-de-windows-y-cuales-son-sus-diferencias-con-el-de-linux

Cómo usar el comando usermod en Linux: ejemplos y opciones. (2023, 17 de enero). Recuperado de https://linuxhandbook.com/es/usermod-command/

González, S. (2024). Administración de usuarios en Linux. LinuxTotal.com.mx. Recuperado el 17 de enero de 2024, de https://linuxtotal.com.mx/index.php?cont=info_admon_001

¿Cuál es el uso del modo de usuario en Linux? (s. f.). Recuperado el 17 de enero de 2024, de https://www.example.com/mode-user-linux