Seguridad en Sistemas Operativos Modernos

Ciberseguridad – FPUNA

2024-05-21

Contenido

1. Introducción
2. Estados privilegiados y no privilegiados.
3. Procesos e hilos de aplicaciones.
4. Memoria
5. Sistemas de archivos
6. Virtualización. Hipervisores.
7. Creación y operación de tecnología de virtualización.
8. Principios fundamentales de diseño de seguridad aplicados a un sistema operativo.
9. Controles de Acceso.
10. Separación de dominios, aislamiento de procesos, encapsulación de recursos, disminuir privilegios.

Introducción

Sistema Operativo

- Es un **software fundamental** que se ejecuta en una computadora y **gestiona los recursos de hardware y software** de este. Es el **intermediario** entre el usuario y la máquina, permitiendo que interactúen de manera eficiente y segura.

Funciones principales

- **Administrar la memoria**: Asigna y libera memoria para los programas que se ejecutan.
- **Gestionar procesos**: Coordina la ejecución de múltiples programas al mismo tiempo.
- **Controlar dispositivos de entrada/salida**: Permite la interacción con periféricos como teclado, ratón, impresora, etc.
- **Proporcionar una interfaz de usuario**: Ofrece una forma de interactuar con el sistema, ya sea mediante una interfaz gráfica o de comandos.
- **Gestionar el sistema de archivos**: Organiza y almacena los archivos en el disco duro.
- **Proporcionar servicios de seguridad**: Protege el sistema de accesos no autorizados y malware.
- **Ejecutar aplicaciones**: Permite ejecutar programas de software para realizar diversas tareas.

Tipos de sistemas operativos

- **Escritorio**: Diseñados para computadoras personales, como Windows, macOS y Linux.
- **Móviles**: Para dispositivos móviles como smartphones y tablets, como Android e iOS.
- **Embebidos**: Integrados en dispositivos específicos, como televisores, routers y automóviles.
- **Servidor**: Para servidores que alojan sitios web, correo electrónico y otras aplicaciones.
- **De red**: Para administrar y controlar redes de computadoras.

SISTEMAS OPERATIVOS PARA DESKTOP MÁS USADOS EN 2023

Sistema operativo	Porcentaje
Windows	69
OS X	19
Unknown	6
Chrome OS	3
Linux	3
Other	0

Sistemas operativos para desktop más usados en 2023

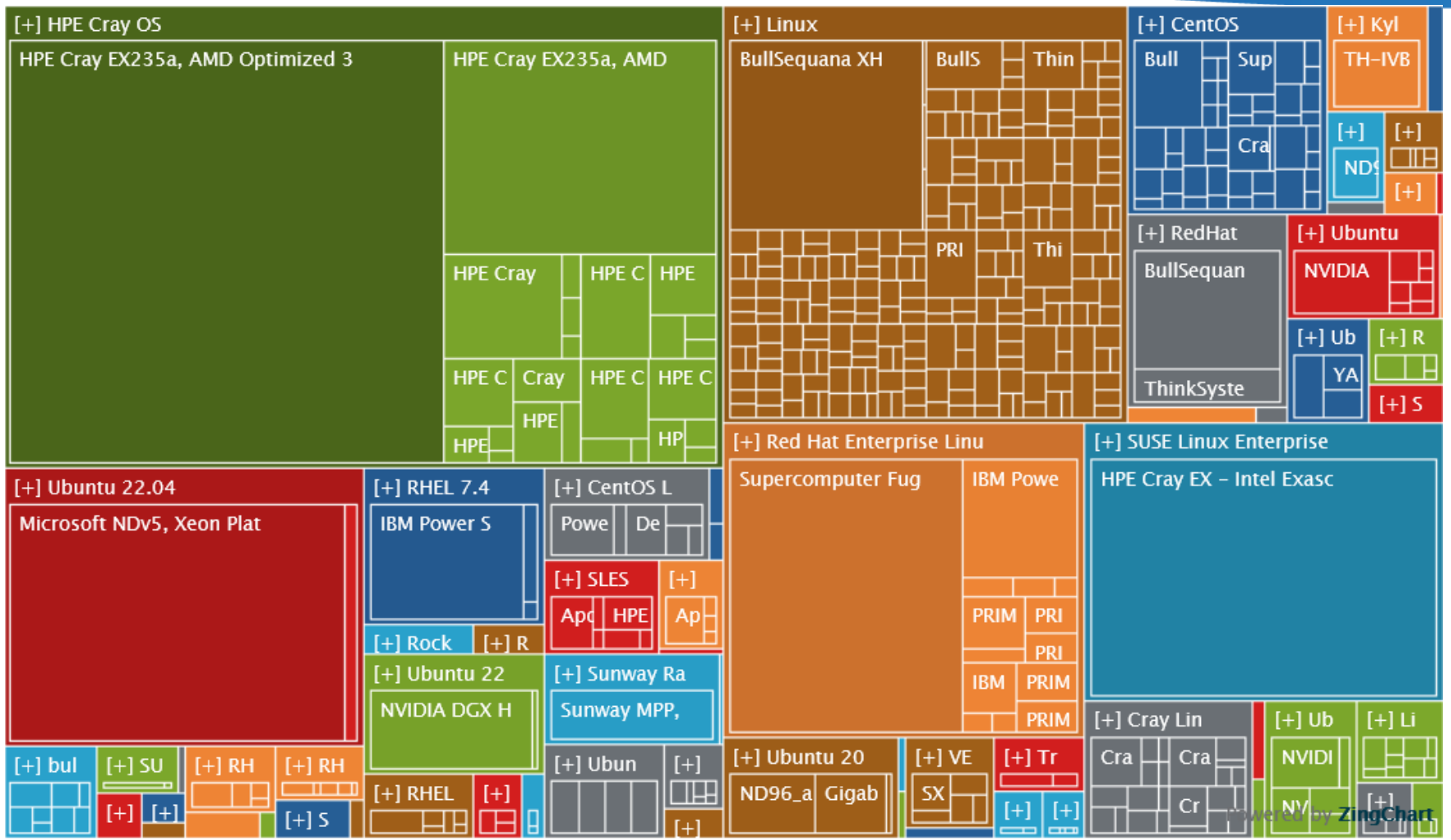
https://itsoftware.com.co/content/sistemas-operativos-mas-usados/#Sistemas_operativos_para_desktop_mas_usados_en_2023

SISTEMAS OPERATIVOS PARA MÓVILES MÁS USADOS EN 2023

Sistema operativo	Porcentaje
Android	69,12
iOS	29,65
Xbox	0,51
Samsung	0,36
Unknown	0,14
KaiOS	0,13
Playstation	0,03
Windows	0,02
Linux	0,02
Other	0,03

Sistemas operativos para Móviles más usados en 2023

https://itsoftware.com.co/content/sistemas-operativos-mas-usados/#Sistemas_operativos_para_Moviles_mas_usados_en_2023



https://top500.org/statistics/treemaps/

Importancia de los Sistemas Operativos (1/4)

Habilitan las tecnologías clave:

- **Internet**: Permiten la conexión a internet, que es esencial para acceder a información, realizar transacciones comerciales y comunicarse online.
- **Computación en la nube**: Brindan la plataforma para ejecutar aplicaciones y almacenar datos en la nube, lo que impulsa la flexibilidad, la escalabilidad y la colaboración.
- **Inteligencia artificial (IA) y Machine Learning (ML)**: Ofrecen la base para ejecutar aplicaciones de IA y ML que están revolucionando industrias como la atención médica, las finanzas y el comercio minorista.
- **Internet de las cosas (IoT)**: Conectan y administran dispositivos IoT, que están transformando hogares, ciudades y empresas.

Importancia de los Sistemas Operativos (2/4)

Potencian la productividad:

- **Interfaces de usuario intuitivas**: Facilitan el uso de las computadoras, lo que aumenta la productividad de los trabajadores.
- **Multitarea eficiente**: Permiten ejecutar múltiples programas al mismo tiempo, optimizando el tiempo.
- **Herramientas de colaboración**: Facilitan el trabajo en equipo y la comunicación entre colegas, clientes y socios.
- **Seguridad robusta**: Protegen los datos y sistemas de las ciberamenazas, lo que es crucial para las empresas en la economía digital.

Importancia de los Sistemas Operativos (3/4)

Impulsan la innovación:

- **Plataformas abiertas**: Fomentan la creación de nuevas aplicaciones y servicios, impulsando la innovación en diversos sectores.
- **Entornos de desarrollo amigables**: Facilitan el trabajo de los desarrolladores, acelerando el desarrollo de nuevas tecnologías.
- **Soporte para tecnologías emergentes**: Integran las últimas tecnologías, como la realidad virtual y aumentada, abriendo nuevas posibilidades para la innovación.

Importancia de los Sistemas Operativos (4/4)

Facilitan el acceso a la información y los servicios:

- **Conectividad universal**: Permiten que personas en todo el mundo accedan a información, educación y servicios online, lo que reduce la brecha digital y promueve el desarrollo económico.
- **Comercio electrónico**: Brindan la base para las plataformas de comercio electrónico, que facilitan la compra y venta de bienes y servicios a nivel global.
- **Gobierno electrónico**: Permiten a los ciudadanos interactuar con los gobiernos de manera digital, mejorando la eficiencia y la transparencia.

Seguridad a través de los Sistemas Operativos

- **Confidencialidad**: implementar mecanismos para garantizar que los datos almacenados, procesados y transmitidos solo sean accesibles a los usuarios y aplicaciones legítimas. Esto se logra mediante técnicas como el cifrado, el control de acceso y la autenticación.
- **Integridad**: proteger la integridad de los datos, programas y el sistema en sí para evitar que sean manipulados o dañados por actores malintencionados. Esto se logra mediante técnicas como el control de acceso, la firma digital y la detección de intrusiones.
- **Disponibilidad**: garantizar que los datos y los recursos del sistema estén disponibles para los usuarios legítimos cuando lo necesiten, incluso en presencia de amenazas o fallos. Esto se logra mediante técnicas como la redundancia de datos, la recuperación de desastres y la tolerancia a fallos.

Kernel

- El kernel o núcleo es como el cerebro o corazón del sistema operativo. Es un software fundamental que se ejecuta en modo privilegiado (conocido también como modo kernel).

Funciones del kernel

- **Administrar los recursos de hardware**: Controla el acceso y la utilización de componentes como la CPU, la memoria, el disco duro, los dispositivos de entrada/salida y otros periféricos.
- **Gestionar procesos**: Coordina la ejecución de múltiples programas al mismo tiempo, asignando recursos y asegurando que no interfieran entre sí.
- **Proporcionar una interfaz de programación de aplicaciones (API)**: Permite que los programas de software interactúen con el hardware y el sistema operativo de manera controlada.
- **Proteger el sistema**: Implementa medidas de seguridad para evitar accesos no autorizados, malware y otras amenazas.
- **Comunicarse con el hardware**: Traduce las solicitudes del software en instrucciones que el hardware puede entender.
- **Administrar la memoria**: Asigna y libera memoria para los programas que se ejecutan, evitando que se agote o se use de manera ineficiente.
- **Gestionar el sistema de archivos**: Organiza y almacena los archivos en el disco duro, permitiendo al usuario acceder y manipularlos.
- **Proporcionar servicios básicos**: Ofrece funcionalidades como la gestión del tiempo, la comunicación entre procesos y la entrada/salida de datos.

Estados privilegiados y no privilegiados

Estados privilegiados y no privilegiados

- Corresponde a los diferentes niveles de acceso y control que tienen los programas y usuarios sobre los recursos del sistema.

Estado privilegiado

- También conocido como **modo núcleo** o **modo supervisor**.
- Concede acceso completo a los recursos del sistema, incluyendo la memoria, el procesador, los dispositivos de entrada/salida y los archivos.
- Solo los programas y usuarios autorizados, como el sistema operativo en sí, los administradores del sistema y algunas aplicaciones específicas, pueden operar en este estado.
- Permite realizar acciones que podrían comprometer la seguridad o estabilidad del sistema si se ejecutan incorrectamente.

Estado no privilegiado

- También conocido como **modo usuario**.
- La mayoría de los programas y usuarios operan en este estado con acceso restringido a los recursos del sistema.
- Las restricciones impiden que los programas no privilegiados interfieran entre sí o con el funcionamiento del sistema operativo.
- Ayuda a mantener la estabilidad y seguridad del sistema al limitar las acciones que pueden realizar los usuarios y programas.

Comparación

Característica	Estado privilegiado	Estado no privilegiado
Acceso a recursos	Completo	Restringido
Programas y usuarios autorizados	Sistema operativo, administradores, aplicaciones específicas	La mayoría de los programas y usuarios
Acciones permitidas	Potencialmente peligrosas	Seguras
Objetivo	Control total del sistema	Funcionamiento normal del usuario

Ejemplo

No privilegiado

- Un usuario normal que ejecuta un navegador web que opera en estado no privilegiado. Puede navegar por internet, abrir páginas web y descargar archivos, pero no puede acceder directamente a la memoria del sistema o modificar archivos del sistema operativo.

Privilegiado

- Un administrador del sistema que instala software nuevo para gestionar un nuevo dispositivo opera en estado privilegiado. Puede realizar cambios en la configuración del sistema, instalar controladores de dispositivo y acceder a archivos que están restringidos a usuarios normales.

Seguridad

- La distinción entre estados privilegiado y no privilegiado es crucial para la seguridad y estabilidad de los sistemas operativos. Limita las acciones que pueden realizar los usuarios y programas, lo que ayuda a prevenir daños accidentales o intencionales al sistema.
- El principio de **privilegios mínimos** dicta que los programas y usuarios solo deben tener los privilegios necesarios para realizar sus tareas específicas, lo que reduce aún más la superficie de ataque para posibles amenazas.

Procesos e hilos

Procesos e hilos (Threads)

- Son unidades fundamentales de ejecución que permiten la gestión eficiente de recursos y la ejecución concurrente de múltiples tareas.

Procesos

- Un proceso es una instancia en ejecución de un programa. Cada proceso tiene su propio espacio de memoria, recursos asignados y estado de ejecución.
- Los procesos se crean, ejecutan y terminan por el sistema operativo, que gestiona su concurrencia y sincronización para garantizar un funcionamiento ordenado y eficiente.

Hilos (Threads)

- Un hilo es una unidad de ejecución dentro de un proceso. Múltiples hilos pueden coexistir dentro de un mismo proceso, compartiendo su espacio de memoria y recursos.
- Los hilos permiten una ejecución más eficiente de tareas dentro de un proceso, especialmente para operaciones que pueden ejecutarse de forma independiente.

Seguridad en Procesos e Hilos

- La seguridad de los procesos e hilos se aborda mediante una combinación de mecanismos del sistema operativo, prácticas de programación seguras y medidas de seguridad a nivel de aplicación.

Mecanismos del sistema operativo

- Aislamiento de procesos y memoria
- Protección de memoria
- Control de acceso
- Sincronización de hilos
- Aislamiento de hilos

Prácticas de programación seguras

- **Programación defensiva**: Escribir código que sea resistente a entradas y condiciones inesperadas para evitar errores y ataques.
- **Validación de entradas**: Validar cuidadosamente las entradas de usuario y datos externos para evitar inyecciones de código o datos maliciosos.
- **Gestión de memoria segura**: Utilizar técnicas de gestión de memoria seguras, como la asignación dinámica de memoria con liberación adecuada, para evitar fugas de memoria y ataques de desbordamiento de búfer.

Medidas de seguridad a nivel de aplicación

- **Control de acceso basado en roles**: Limitar el acceso a recursos y funcionalidades de la aplicación en función de los roles y privilegios de los usuarios.
- **Cifrado de datos**: Cifrar datos confidenciales en reposo y durante la transmisión para protegerlos de accesos no autorizados.
- **Análisis de vulnerabilidades**: Realizar análisis de vulnerabilidades regulares para identificar y corregir debilidades de seguridad en la aplicación.

Seguridad en Procesos

- **Aislamiento de procesos**: Cada proceso tiene su propio espacio de memoria, lo que evita que un proceso acceda o modifique los datos de otro proceso. Esto ayuda a contener el impacto de errores o ataques maliciosos.
- **Protección de memoria**: El sistema operativo utiliza mecanismos de protección de memoria para evitar que un proceso acceda a áreas de memoria no asignadas o privilegiadas. Esto ayuda a prevenir la ejecución de código malicioso o la corrupción de datos críticos.
- **Control de acceso**: El sistema operativo controla el acceso de los procesos a recursos del sistema, como archivos, dispositivos y servicios de red. Esto ayuda a prevenir que procesos no autorizados accedan a recursos sensibles.

Seguridad en Hilos

- **Sincronización de hilos**: Los hilos dentro de un proceso deben sincronizarse para acceder y modificar recursos compartidos de forma segura. El sistema operativo proporciona mecanismos de sincronización, como semáforos y mutex, para evitar conflictos y garantizar la integridad de los datos.
- **Aislamiento de hilos**: Aunque los hilos comparten el espacio de memoria del proceso, existen mecanismos para aislar su ejecución y evitar que un hilo malicioso afecte a otros hilos del mismo proceso.
- **Seguridad de las bibliotecas compartidas**: Los hilos pueden acceder a bibliotecas compartidas que contienen código de terceros. Es importante asegurarse de que estas bibliotecas sean confiables y no contengan vulnerabilidades que puedan ser explotadas por hilos maliciosos.