Seminario de Sistemas Operativos

Departamento de Ciencias Computacionales

Centro Universitario de Ciencias Exactas e Ingenierías

Universidad de Guadalajara

Violeta del Rocío Becerra Velázquez

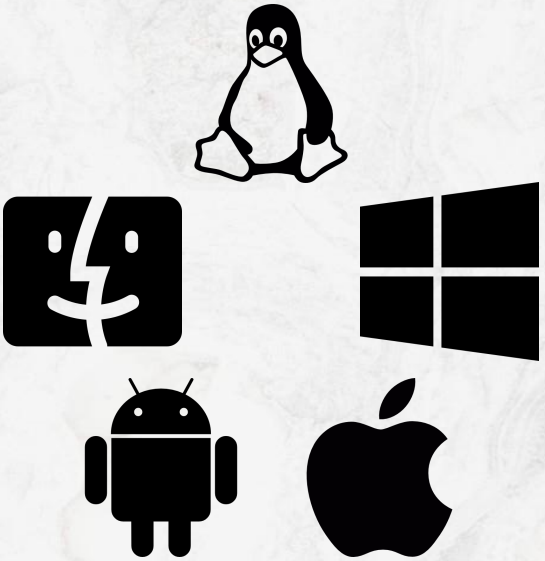
Saul Alejandro Castañeda Pérez

Actividad de Aprendizaje 13

13:00 - 14:55

217564323

D02



CUCEI

Índice

Seminario de Sistemas Operativos

Controladores

Un controlador es un componente de software que permite al sistema operativo y un dispositivo comunicarse entre sí, actúan como puentes entre las aplicaciones y los dispositivos, encargándose de que ambos interactúen, el controlador actúa como un intermediario entre el hardware y el software del sistema operativo, proporcionando una interfaz común para que ambos puedan comunicarse.

Cada dispositivo de hardware tiene su propio controlador, que se debe instalar en el sistema operativo para que el dispositivo funcione correctamente, los controladores permiten que el sistema operativo interactúe con dispositivos como impresoras, cámaras, tarjetas de red, tarjetas de sonido y muchos otros dispositivos de hardware.

Cuando el sistema operativo necesita interactuar con un dispositivo de hardware, utiliza el controlador correspondiente para enviar comandos al dispositivo y recibir información de él, se debe mantener los controladores actualizados y compatibles con el sistema operativo, ya que los controladores obsoletos o incompatibles pueden causar problemas de funcionamiento o incluso fallos del sistema, los controladores son esenciales para el correcto funcionamiento del hardware en un sistema operativo y para que los usuarios puedan realizar tareas de manera eficiente y sin problemas.

Disco de estado sólido

Un SSD es un tipo de dispositivo de almacenamiento que utiliza memoria flash para almacenar datos a diferencia de los discos duros tradicionales, que utilizan discos magnéticos giratorios para leer y escribir datos, los SSD no tienen partes móviles y utilizan chips de memoria flash NAND para almacenar información, esto una de las razones por las que los SSD consumen menos energía en general.

En comparación con el método tradicional de almacenamiento HDD, las unidades SSD se construyen sin la unidad de disco giratoria tradicional y sin cabezales de disco duro móviles que se utilizan para leer y escribir nueva información en el disco, y al no tener partes móviles, los SSD son más rápidos y duraderos que los discos duros tradicionales, su tiempo de acceso es más rápido, lo que significa que los datos se pueden leer y escribir más rápidamente, lo que mejora el rendimiento general del sistema.

También son menos propensos a sufrir daños por golpes o vibraciones, lo que los hace ideales para su uso en dispositivos portátiles como laptops o tabletas, aunque su costo por gigabyte de almacenamiento suele ser más alto que el de los discos duros, su rendimiento y durabilidad los hacen una buena opción para aquellos que buscan un almacenamiento de alta velocidad y confiable.

Seguridad y protección

La función principal de un Sistema Operativo es la de tomar todos los recursos físicos de un sistema de cómputo y brindarlos de manera virtual, esto es logrado por medio de una abstracción del hardware, pero no es suficiente con permitir el manejo y uso del hardware si no se maneja seguridad y protección.

- **La seguridad**: es la ausencia de un riesgo, haciendo referencia al riesgo de accesos no autorizados, de manipulación de información, manipulación de las configuraciones, entre otros.
- **La protección**: son los diferentes mecanismos utilizados por el SO para cuidar la información, los procesos, los usuarios, etc.

La seguridad y protección son fundamentales para garantizar su estabilidad y funcionamiento adecuado, así como para proteger los datos y recursos del usuario, algunas medidas de seguridad y protección que se pueden implementar son:

- **Autenticación**: el sistema debe contar con mecanismos de autenticación que permitan verificar la identidad del usuario, como contraseñas, tokens de autenticación o autentificación biométrica.
- **Autorización**: una vez que se ha autenticado al usuario, el sistema debe verificar que tenga los permisos necesarios para acceder a los recursos y realizar las operaciones que se solicitan.
- **Protección de archivos**: los archivos deben ser protegidos mediante permisos de acceso, que indiquen qué usuarios o grupos pueden leer, escribir o ejecutar un archivo determinado.
- **Actualizaciones de seguridad**: el sistema operativo debe ser actualizado regularmente para corregir vulnerabilidades y mejorar la seguridad del sistema.
- **Antivirus y antimalware**: el uso de software de protección, como antivirus y antimalware, es fundamental para proteger el sistema contra virus y malware.
- **Firewalls**: los firewalls permiten controlar el tráfico de red y bloquear conexiones no autorizadas.
- **Control de acceso a dispositivos**: algunos SO permiten controlar el acceso a dispositivos como USB o CD/DVD para evitar la propagación de virus o la pérdida de datos.
- **Auditorías de seguridad**: se deben realizar auditorías de seguridad periódicas para detectar posibles vulnerabilidades y corregirlas.

La implementación de estas medidas de seguridad y protección puede variar dependiendo del sistema operativo utilizado y del entorno en el que se utiliza, es importante mantener el sistema actualizado, utilizar software de protección y seguir buenas prácticas de seguridad, como no compartir contraseñas o no descargar software de fuentes no confiables.

Criptografía

La criptografía se utiliza para proteger datos sensibles y prevenir el acceso no autorizado o la modificación de la información durante su transmisión o almacenamiento por medio de la aplicación de técnicas matemáticas y algoritmos para proteger la confidencialidad, integridad y autenticidad de la información, por lo que se utiliza en diferentes aplicaciones, como el cifrado de contraseñas, la protección de la privacidad en las comunicaciones electrónicas, la autenticación de usuarios, la protección de datos en bases de datos y sistemas de almacenamiento, entre otros, la criptografía en informática se divide en dos categorías:

- La **criptografía simétrica** utiliza una clave compartida para cifrar y descifrar información.
- La **criptografía asimétrica** utiliza claves públicas y privadas para cifrar y descifrar información.

La elección de la técnica y el algoritmo criptográfico a utilizar dependerá del nivel de seguridad requerido, la complejidad de la información a proteger y el contexto en el que se utiliza.

La criptografía busca garantizar la confidencialidad e integridad tanto de los datos en tránsito como de los datos en reposo, también puede autenticar a remitentes y destinatarios entre sí y proteger contra el repudio, además puede proteger las comunicaciones que se llevan a cabo en redes que no son de confianza.

Esteganografía

La esteganografía es una técnica utilizada para ocultar información dentro de otros archivos, sin que sea detectada su presencia, a diferencia de la criptografía, que se enfoca en hacer inteligible el mensaje para terceros, la esteganografía se enfoca en hacer invisible la existencia del mensaje, la información que se desea ocultar se inserta dentro de un archivo portador, como una imagen, un audio o un video, se modifica la estructura del archivo portador de forma que el mensaje oculto no sea perceptible a simple vista.

El objetivo principal es asegurar la privacidad y confidencialidad de la información, sin llamar la atención de terceros que puedan estar monitoreando la comunicación, algunas de las aplicaciones incluyen el intercambio de información sensible, la protección de la propiedad intelectual y la ocultación de información en investigaciones de seguridad y forenses, sin embargo, también puede ser utilizada con fines maliciosos, como la distribución de malware o la ocultación de información ilegal y por esta razón, es importante contar con herramientas de detección de esteganografía en informática y tener precaución al abrir archivos de origen desconocido.

Conclusión

La criptografía y la esteganografía son dos técnicas fundamentales en el ámbito de la seguridad en SO que se utilizan para proteger y ocultar información delicada, una se enfoca en hacer ininteligible el mensaje para terceros, mientras que la otra se enfoca en hacer invisible la existencia del mensaje, pero ambas técnicas se utilizan para asegurar la privacidad y confidencialidad de la información, ya sea durante su transmisión o almacenamiento.

La elección de la técnica dependerá del nivel de seguridad requerido, la complejidad de la información a proteger, también es importante mencionar que pueden ser utilizadas con fines maliciosos, como la distribución de malware o la ocultación de información ilegal, por lo que debemos tener precaución al abrir archivos de origen desconocido.

Referencias

A. (2023a, marzo 8). ¿Qué es un controlador? - Windows drivers. Microsoft Learn. https://learn.microsoft.com/es-es/windows-hardware/drivers/gettingstarted/what-is-a-driver-

colaboradores de Wikipedia. (2022, 29 noviembre). Controlador de dispositivo. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Controlador_de_dispositivo

colaboradores de Wikipedia. (2023b, marzo 27). Unidad de estado sólido. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Unidad_de_estado_s%C3%B3lido

Fernández, Y. (2023, 12 enero). HDD vs SSD: diferencias y ventajas de ambos tipos de disco duro. Xataka. https://www.xataka.com/basics/hdd-vs-ssd

Técnicas para proteger el sistema operativo. (s. f.). © Copyright IBM Corp. 2014. https://www.ibm.com/docs/es/cognos-analytics/10.2.2?topic=SSEP7J_10.2.2/com.ibm.swg.ba.cognos.crn_arch.10.2.2.doc/c_securing_the_operating_system.htm

Muñoz, S. L. (2023, 21 marzo). Claves para la protección y seguridad de sistemas operativos en una empresa. Legaltech. https://blog.lemontech.com/proteccion-seguridad-sistemas-operativos/

https://nic.ar/es/enterate/novedades/que-es-criptografia#:~:text=La%20criptograf%C3%ADa%20es%20el%20desarrollo,no%20est%C3%A9n%20autorizados%20a%20hacerlo.

Mazara, K. (2021, 21 junio). ¿Qué es la esteganografía? - Recursos de arquitectura y diseño seguros (CompTIA Security+ SY0-601). LinkedIn. https://es.linkedin.com/learning/recursos-de-arquitectura-y-diseno-seguros-comptia-security-plus-sy0-601/que-es-la-esteganografia