Universidad de Guadalajara

Centro Universitario de Ciencias Exactas e Ingenierías

Departamento de ciencias computacionales.

Ingeniería en computación

Seminario de Solución de Problemas de Sistemas Operativos - D01.

Violeta del Rocío Becerra Velázquez

“Criptografía”

10/04/2023

Olguín Hernández Jair Benjamín

217439707

Índice

Contenido.

1. Controladores:

Un controlador o driver es un programa o software que permite que un dispositivo o componente de hardware se comunique con el sistema operativo y otras aplicaciones. Los controladores actúan como intermediarios entre el hardware y el software, permitiendo que el sistema operativo y otras aplicaciones se comuniquen con el dispositivo. Sin un controlador apropiado, el dispositivo no puede funcionar correctamente. Los controladores son específicos para cada tipo de dispositivo o componente de hardware, y suelen ser proporcionados por el fabricante del dispositivo. En algunos casos, los controladores pueden ser instalados automáticamente por el sistema operativo, mientras que en otros casos es necesario instalarlos manualmente. Algunos ejemplos de dispositivos que requieren controladores incluyen impresoras, escáneres, tarjetas de sonido, tarjetas de red, discos duros, ratones, teclados, cámaras web y dispositivos USB. Sin los controladores adecuados, estos dispositivos no podrían funcionar correctamente o incluso no podrían ser reconocidos por el sistema operativo.

2. Disco de estado sólido

Un disco de estado sólido, también conocido como SSD (del inglés "solid-state drive"), es un dispositivo de almacenamiento de datos que utiliza memoria no volátil para almacenar datos. A diferencia de los discos duros tradicionales, que utilizan discos magnéticos giratorios para almacenar datos, los SSD no tienen partes móviles y utilizan chips de memoria flash NAND para almacenar datos. Los SSD son más rápidos que los discos duros tradicionales, ya que no tienen que esperar a que un disco giratorio se posicione para acceder a los datos. Esto hace que el acceso a los datos en un SSD sea mucho más rápido que en un disco duro. Además, los SSD consumen menos energía y generan menos calor que los discos duros, lo que los hace ideales para portátiles y dispositivos móviles. Los SSD también son más resistentes a los golpes y vibraciones que los discos duros tradicionales, ya que no tienen partes móviles que puedan dañarse en caso de una caída o golpe fuerte. Además, los SSD no sufren los problemas de fragmentación que pueden afectar el rendimiento de los discos duros, ya que no tienen que buscar físicamente los datos en un disco giratorio.

En resumen, un disco de estado sólido es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para almacenar datos y ofrece una serie de ventajas sobre los discos duros tradicionales, incluyendo mayor velocidad, menor consumo de energía, mayor resistencia y menor susceptibilidad a la fragmentación.

3. Seguridad y protección.

La seguridad y protección en los sistemas operativos se refiere a las medidas de seguridad implementadas para proteger los sistemas y datos de usuarios de posibles amenazas externas e internas. Esto incluye la prevención de intrusiones, el control de acceso, la autenticación de usuarios y la protección de datos y recursos.

La seguridad en un sistema operativo se puede lograr a través de varias técnicas, tales como:

- Control de acceso: los sistemas operativos implementan un control de acceso para garantizar que los usuarios solo tengan acceso a los recursos para los que tienen permiso. Esto se hace mediante la asignación de permisos a los archivos, carpetas y dispositivos para usuarios y grupos de usuarios específicos.
- Autenticación: los sistemas operativos utilizan técnicas de autenticación para garantizar que solo los usuarios autorizados puedan acceder al sistema. Esto se hace mediante la utilización de contraseñas, biometría y otros métodos de autenticación.
- Firewall: los sistemas operativos pueden incluir un firewall para controlar el tráfico de red y bloquear las conexiones no autorizadas.
- Encriptación de datos: los sistemas operativos pueden proporcionar herramientas para encriptar los datos almacenados en el sistema para que solo los usuarios autorizados puedan acceder a ellos.
- Actualizaciones de seguridad: los sistemas operativos requieren actualizaciones periódicas para corregir vulnerabilidades de seguridad y proteger el sistema contra ataques..

4. Criptografía.

La criptografía es una técnica que se utiliza para proteger la información y mantenerla segura y privada. La criptografía se basa en el uso de algoritmos matemáticos para transformar la información original en una forma ilegible, llamada cifrado, que solo puede ser desencriptada por aquellos que tienen la clave correcta. La criptografía se utiliza ampliamente en la comunicación y el almacenamiento de información confidencial, como contraseñas, números de tarjetas de crédito, información financiera y datos personales. Al cifrar esta información, se hace mucho más difícil que un tercero no autorizado pueda acceder a ella o interceptarla. Existen diferentes tipos de criptografía, incluyendo la criptografía simétrica y la criptografía asimétrica. La criptografía simétrica utiliza la misma clave para cifrar y descifrar la información, mientras que la criptografía asimétrica utiliza dos claves diferentes: una clave pública y una clave privada. La clave pública se utiliza para cifrar la información, mientras que la clave privada se utiliza para descifrarla. Además de la protección de la información confidencial, la criptografía también se utiliza para verificar la integridad de la información y la autenticidad de las comunicaciones. Por ejemplo, los certificados digitales utilizados en el protocolo HTTPS de los sitios web se basan en criptografía para garantizar que el sitio web que está visitando es auténtico y que la información que envía y recibe está protegida.

5. Esteganografía.

La esteganografía es una técnica de seguridad que se utiliza para ocultar información dentro de otro tipo de información, como imágenes, audio, video o texto. A

diferencia de la criptografía, que se enfoca en cifrar información para protegerla, la esteganografía se enfoca en ocultar información dentro de otra información para que no sea detectable por terceros. La esteganografía se basa en la idea de que si se oculta información dentro de otra información, es menos probable que atraiga la atención de alguien que intente interceptarla o acceder a ella de manera no autorizada. La información oculta se puede recuperar solo si el receptor sabe cómo buscarla y tiene la clave o el método para extraerla. La esteganografía se utiliza en una variedad de aplicaciones, desde la protección de la privacidad de los mensajes secretos y la transferencia segura de datos hasta la protección de derechos de autor de medios digitales. Sin embargo, la esteganografía también puede ser utilizada con fines maliciosos, como la transferencia de información robada o la distribución de malware. Es importante tener en cuenta que la esteganografía no es una solución completa de seguridad, sino que puede ser una herramienta complementaria para proteger información confidencial. Además, la esteganografía también puede ser detectada y contrarrestada mediante el uso de herramientas de detección de esteganografía y técnicas de análisis forense.

Conclusión.

En esta actividad pude tener mas conocimiento de algunos conceptos que pueden llegar a ser más técnicos en el tema de sistemas operativos, pero así mismo te ayudan a entender un poco mas del cómo es que funcionan los sistemas operativos y todo la organizan y situaciones que tienen que llegar a contemplar. Tanto la criptografía como la esteganografía son técnicas fundamentales en la seguridad informática y se utilizan en los sistemas operativos para proteger la información confidencial. La criptografía se enfoca en cifrar la información para que solo las personas autorizadas puedan acceder a ella, mientras que la esteganografía se enfoca en ocultar la información dentro de otra información para que no sea detectada. Los sistemas operativos modernos incluyen herramientas y características de seguridad, como la encriptación de archivos y discos duros, la autenticación de usuarios, la prevención de intrusiones y la detección de virus y malware, que hacen uso de la criptografía y la esteganografía para mantener la información segura.

Bibliografía

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

González, A. (2021, 16 marzo). *Esteganografía. Definición, técnicas y usos frecuentes*. Ayuda Ley Protección Datos. https://ayudaleyprotecciondatos.es/2021/03/17/esteganografia/

GuilleVen. (2022, 24 octubre). *¿Qué es la Criptografía?* Tecnología + Informática. https://www.tecnologia-informatica.com/que-es-la-criptografia/

Hurtado, J. S. (2022, 8 agosto). *Qué es la criptografía y para qué sirve*. Thinking for Innovation. https://www.iebschool.com/blog/que-es-la-criptografia-y-para-que-sirve-finanzas/

Kuksov, I. (2022, 27 marzo). *¿Qué es la esteganografía digital?* https://latam.kaspersky.com/blog/digital-steganography/14859/