

UNIVERSIDAD DE GUADALAJARA

Centro Universitario de Ciencias Exactas e Ingenierías

Departamento de Ciencias Computacionales

6^{to} semestre

Tema: Criptografía



Materia:

Seminario de Sistemas Operativos

Docente:

Violeta del Rocío Becerra Velázquez

PRESENTA:

Daniel Martínez Martínez

Código:

217565958

Carrera:

Ingeniería en Computación.

Sección:

D02

Fecha de entrega:

Domingo, 07 de Mayo de 2023

Índice

Controladores	2
Discos de estado sólido	2
Seguridad y protección	2
Criptografía	3
Esteganografía	3
Conclusiones	4
Bibliografía	4

Criptografía

Controladores

Los controladores (Drivers en inglés) son todos los programas que emplea un sistema operativo para entablar comunicación con los dispositivos de hardware que se encuentran ligados a la máquina, como lo son el mouse, el teclado, la pantalla, una impresora, etc.

Los controladores de dispositivos son esenciales para que un sistema informático funcione correctamente, porque sin un controlador de dispositivo, el hardware en particular es incapaz de realizar la función para la que fue creado.

Es importante tener los controladores actualizados para asegurarse de que el dispositivo de hardware funcione de manera óptima y se eviten problemas de compatibilidad. Los controladores también pueden solucionar problemas de funcionamiento del dispositivo, como problemas de rendimiento, errores y fallas.

Discos de estado sólido

Son dispositivos de almacenamiento de información que utilizan memoria flash para guardar los datos que el usuario indique. a diferencia de los discos duros mecánicos que usan un cabezal de lectura magnético para realizar operaciones de lectura y escritura, los discos SSD no tienen componentes móviles, sino que usan circuitos integrados para acceder a la información, característica que sirve como principal diferenciador contra los discos duros tradicionales.

Los discos SSD son dispositivos de almacenamiento presentados como una alternativa bastante competitiva al uso de los discos duros tradicionales. Sus principales ventajas están enfocadas a la optimización del acceso a los datos en términos de velocidad, consumo de energía y emisión de ruido, además de que son más resistentes a impactos al carecer de piezas mecánicas frágiles para su funcionamiento.

Considero personalmente que son mejores que los HDD, ya que a pesar de que están en desventaja en aspectos como la capacidad de almacenamiento, la vida útil y el precio, creo que en el futuro las compañías que los fabrican encontrarán vías para posicionarlos por encima de los HDDs, sin perjudicar tanto al consumidor.

Seguridad y protección

Seguridad lo podemos definir como el sentimiento de que nada malo va a suceder a nuestro alrededor, a través de un constante esfuerzo para erradicar todo aquello que pueda poner en peligro nuestra integridad. Si no se hace algo para mantener a raya aquello que representa un riesgo, perdemos el control de aspectos importantes con respecto a nuestra persona y lo que nos rodea, por ejemplo podría verse comprometido nuestro patrimonio, nuestra privacidad, el bienestar de la gente que queremos, etc.

Cuando hablamos de seguridad informática nos referimos a todo aquello que se relaciona al hecho de proteger a los sistemas informáticos de cualquier tipo de amenaza, garantizando la confidencialidad, integridad y disponibilidad de toda la información que se tiene almacenada en dichos sistemas. Dado que el contexto donde se mueve la seguridad informática es muy grande, la podemos subdividir en dos niveles de protección:

- **Nivel físico:** Es el nivel encargado de resguardar la información de todos los factores tangibles que encontramos en el mundo real, es decir, de todo aquello que puede poner en riesgo los recursos físicos usados dentro de un sistema informático.
- **Nivel lógico:** Es el nivel enfocado a la protección de la información de amenazas en el entorno digital. El entorno digital engloba a la manera en la que la información se almacena (serializada, cifrada, en texto plano, etc), como se transporta por la red, que protocolos se siguen para limitar el acceso a los datos, etc.

Criptografía

La criptografía es el estudio y la práctica de técnicas para asegurar la comunicación y la privacidad de la información. Se utiliza para proteger la información confidencial mediante la transformación de los datos originales en una forma codificada, de modo que sólo aquellos que poseen la clave secreta pueden leerlos.

Actualmente, se utilizan una amplia variedad de técnicas criptográficas para proteger la privacidad de la información en sistemas informáticos y de telecomunicaciones. Entre las técnicas criptográficas más comunes se encuentran:

- **Cifrado simétrico:** en el que se utiliza una misma clave para cifrar y descifrar los datos. Es rápido y eficiente, pero presenta el problema de cómo compartir la clave de forma segura.
- **Cifrado asimétrico:** en el que se utilizan dos claves diferentes, una pública y una privada, para cifrar y descifrar los datos. Es más seguro que el cifrado simétrico, pero también es más lento y complejo.
- **Hashing:** en el que se utiliza una función matemática para transformar los datos originales en una cadena de caracteres de longitud fija. Es útil para la verificación de integridad de los datos, pero no es adecuado para la protección de la privacidad.

Esteganografía

La esteganografía es una técnica para ocultar información dentro de otros datos, como imágenes, audio, video o texto. A diferencia de la criptografía, que cifra la información para que no sea legible para aquellos que no tienen la clave de cifrado, la esteganografía oculta la información para que no sea detectable para aquellos que no saben dónde buscarla.

Existen diversas técnicas de esteganografía, como ocultar información en los bits menos significativos de una imagen o en el espacio entre las palabras de un texto. También se puede utilizar la esteganografía para esconder información en imágenes o videos mediante la alteración de los colores o los píxeles.

La esteganografía se utiliza en diversos ámbitos, como la seguridad informática, la protección de la privacidad, la vigilancia y el espionaje. También puede ser utilizada por los artistas digitales y los diseñadores gráficos para ocultar mensajes dentro de sus obras.

Conclusiones

La investigación del día de hoy curiosamente tuvo un enfoque guiado a la seguridad y protección de los datos, ya que son temas que he visto en el curso de seguridad (informática). Es entendible que dichos temas se presenten en una materia aparentemente ajena a la ciberseguridad, ya que las tecnologías que existen actualmente suelen combinarse para crear una experiencia cómoda y segura para los usuarios, sobre todo cuando se trata de procesos que involucran su información personal.

Bibliografía

- GeeksforGeeks. (2022b). Device Driver and It s Purpose. *GeeksforGeeks*. <https://www.geeksforgeeks.org/device-driver-and-its-purpose/>
- Soto, P. (s. f.). conceptos generales de seguridad de la informacion [Diapositivas; Classroom]. classroom. <https://classroom.google.com/u/0/c/NTgzNzExMjAzMTU4?hl=es>
- GeeksforGeeks. (2023d). Cryptography Introduction. *GeeksforGeeks*. <https://www.geeksforgeeks.org/cryptography-introduction/?ref=gcse>
- GeeksforGeeks. (2023f). Difference between Steganography and Cryptography. *GeeksforGeeks*. <https://www.geeksforgeeks.org/difference-between-steganography-and-cryptography/?ref=gcse>