Universidad de Guadalajara

CUCEI (Ciencias Exactas e Ingenierías)

Departamento de ciencias computacionales

Materia: Sistemas operativos

Profesor: Violeta del Rocío Becerra Velazquez

Gómez Rubio Alexia

Código:219551644

Carrera: Ingeniería en computación

Sección: D04

Tarea 7

Tema: Seguridad

Fecha: 24 Noviembre 2024

La **criptografía** en los sistemas operativos es un proceso que se utiliza para codificar u ocultar información para que solo las personas autorizadas puedan leerla. Se basa en el uso de algoritmos criptográficos, o cifrados, que se integran en protocolos y se escriben en software. La criptografía es una técnica que permite codificar un objeto de forma que su cifrado no sea obvio, es decir, puede convertir un objeto original en un objeto cifrado aplicando una función de encriptado.

Algunos de los casos más comunes en la criptografía son:

- Para validar la autenticidad de las contraseñas y también para proteger las contraseñas almacenadas. De esta manera, los servicios pueden autenticar contraseñas sin necesidad de mantener una base de datos de texto simple de todas las contraseñas que puedan ser vulnerables a los hackers.
- Las criptomonedas como Bitcoin y Ethereum se basan en complejos sistemas de cifrado de datos que requieren grandes cantidades de potencia de cálculo para descifrarlos. A través de estos procesos de descifrado, se “acuñan” nuevas monedas y entran en circulación. Las criptomonedas también se basan en la criptografía avanzada para salvaguardar las criptocarteras, verificar las transacciones y evitar el fraude.
- Protege a los usuarios de los ataques de intermediario y los protocolos Secure Sockets Layer (SSL) y Transport Layer Security (TLS) se basan en criptografía de clave pública para proteger los datos enviados entre el servidor web y el cliente y establecer canales de comunicación seguros.
- Las firmas electrónicas se utilizan para firmar documentos importantes en línea y suelen aplicarse por ley. Las firmas electrónicas creadas con criptografía se pueden validar para evitar fraudes y falsificaciones.

La **esteganografía** digital consiste en esconder datos dentro de archivos aparentemente inofensivos, como imágenes, vídeos o audios, sin alterar de forma visible o auditiva el contenido original. Se puede utilizar para proteger datos sensibles, mantener la confidencialidad de la información o transmitirla de manera discreta.

Algunas de las técnicas mas utilizadas son:

- Least Significant Bit (LSB): Consiste en modificar el bit menos significativo de cada píxel de una imagen o muestreo de audio. Este cambio es imperceptible para el usuario, pero permite almacenar datos sin alterar el contenido visible o audible.
- Codificación de redundancia: Esta técnica utiliza datos redundantes o espacio disponible dentro de un archivo para insertar información oculta. Por ejemplo, en un archivo de audio, se pueden utilizar segmentos de silencio o tonos muy ligeros para incluir mensajes.

Ensayo

En el mundo digital actual, la información se ha convertido en uno de los recursos más valiosos para la sociedad. Las empresas, gobiernos y en general las personas realizan tareas diarias que involucran él envió en información, y como ya sabemos hoy en día existen muchas amenazas, como el robo de datos, espionaje o duplicado de archivos.

El cifrado o criptografía en los sistemas operativos y en redes son de gran ayuda para los ataques cibernéticos, de modo que la criptografía asegura que la información no pueda ser leída por terceros que no tienen autorización, protegiendo archivos sensibles o garantizando comunicaciones seguras mediante los protocolos SSL/TLS. Y por otra parte la esteganografía complementa la seguridad al ocultar la existencia de datos.

La criptografía es una disciplina que tiene sus raíces en la antigüedad, cuando se utilizaban códigos simples para proteger mensajes. En la actualidad, se ha convertido en una herramienta importante, con algoritmos avanzados que protegen información sensible, su principal objetivo es garantizar la confidencialidad, integridad, autenticidad de los datos.

En los sistemas operativos, la criptografía juega un papel clave en la protección de archivos y datos personales. Por ejemplo, tecnologías como BitLocker en Windows o FileVault en macOS cifran el contenido del disco duro, impidiendo el acceso no autorizado. Asimismo, contraseñas y credenciales almacenadas en sistemas operativos modernos están protegidas mediante técnicas de hashing, que dificultan su descifrado incluso si son robadas.

En redes, la criptografía es esencial para garantizar que las comunicaciones entre usuarios y servidores sean seguras. Protocolos como SSL/TLS, que sustentan el uso de HTTPS, cifran los datos transmitidos, evitando que puedan ser interceptados por atacantes. También se emplea en tecnologías como redes privadas virtuales (VPN), que permiten a los usuarios navegar por internet de forma segura, incluso en redes públicas.

Mientras que la criptografía busca proteger la información mediante el cifrado, la esteganografía tiene un enfoque diferente: ocultar la existencia de los datos. Esta técnica consiste en incrustar información dentro de archivos aparentemente inofensivos, como imágenes, videos o audios, haciendo que los datos sean imperceptibles para terceros.

En redes, la esteganografía es empleada para transmitir información de forma discreta. Esto puede ser útil en contextos donde la censura o la vigilancia son comunes, permitiendo a los usuarios compartir datos sin ser detectados. Sin embargo,

al igual que en los sistemas operativos, esta técnica también puede ser usada para actividades ilegales, como el tráfico de información confidencial.

La seguridad en sistemas operativos y redes, es responsabilidad de muchas personas como por ejemplo de los desarrolladores de software, los administradores de sistema y los usuarios finales. Se ha demostrado que la criptografía y la esteganografía son muy eficiente, pero depende de como se implementan y de como el usuario las utilicen.

Desde mi punto de vista considero que los desarrolladores deben diseñar sistemas más seguros, las empresas deben invertir en tecnologías y capacitación, y los usuarios deben adoptar una actitud proactiva hacia la protección de sus datos. Solo con esta colaboración será posible garantizar un entorno digital más seguro en un mundo cada vez más interconectado.

Desde el punto de vista del usuario, se destaca que la falta de buenas prácticas, como el uso de contraseñas débiles, la apertura de enlaces sospechosos o la descarga de archivos no confiables, puede comprometer incluso los sistemas más avanzados de seguridad.

Es crucial que los usuarios adopten una actitud proactiva hacia la protección de sus datos, lo cual incluye:

- Educación constante: Conocer los riesgos y mejores prácticas de seguridad.
- Uso de herramientas adecuadas: Adoptar medidas como gestores de contraseñas, autenticación de dos factores y cifrado de datos personales.
- Conciencia situacional: Reconocer intentos de phishing, evitar redes Wi-Fi públicas inseguras y no compartir información sensible en plataformas no seguras.

En el mundo cada vez más interconectado de hoy, la seguridad digital no es solo un aspecto técnico, sino un esfuerzo colectivo. Si bien la criptografía y la esteganografía son herramientas poderosas para proteger la información, el verdadero eslabón fuerte en la cadena de seguridad es el usuario. Sin el compromiso de los usuarios finales para implementar buenas prácticas, incluso los sistemas más seguros pueden ser vulnerables. La colaboración entre desarrolladores, empresas y usuarios es esencial para garantizar un entorno digital confiable y seguro en el que la información pueda fluir sin riesgos indebidos.

Resumen de la película: Matrix

La película presenta un mundo virtual (la Matrix) creado por máquinas, donde los humanos están conectados sin saber que viven en una simulación digital. Esto plantea cuestiones sobre la seguridad y el control de sistemas avanzados. Los protagonistas, como Neo y Trinity, son hackers que intentan liberar a la humanidad de la opresión de las máquinas. La película utiliza conceptos de hacking para romper las barreras de la simulación.

Matrix narra la aventura de Neo, un joven hacker que es convocado por el movimiento de resistencia liderado por Morfeo, que lucha contra la dominación de los seres humanos por las máquinas. Morfeo le ofrece dos pastillas de diferentes colores: con una continuará en la ilusión, con la otra descubrirá la verdad.

El protagonista escoge la píldora roja y despierta en una cápsula, de esta manera descubre que la raza humana está dominada por la inteligencia artificial, y vive atrapada en un programa de ordenador y sirve solo como una fuente de energía. Neo se da cuenta de que la resistencia cree que él es el Elegido, un mesías que liberará a la humanidad de la esclavitud de Matrix.

Aunque dude de su destino a lo largo de todo el camino, aprende a superar las reglas de simulación. Consigue salvar a Morfeo, que había sido secuestrado, y derrota al agente Smith tras un duelo en el que demuestra su valía como guerrero y confirma que es el Elegido.

Referencias Bibliográficas

¿Qué es la criptografía? (2024, July 18). *Ibm.com*. https://www.ibm.com/mx-es/topics/cryptography

Informàtica, C. I. S. (2024, September 18). *¿Qué es la Esteganografía?¿Qué representa por la Ciberseguridad?* CIS Informàtica. https://www.cisinformatica.cat/es/que-se-la-esteganografia-en-ciberseguridad/

Sanchis, E. (2021, August 2). Estenografía: Descubre su Historia, Técnicas y Aplicaciones. *Peritos Informaticos*. https://peritos-informaticos.com/blog/que-es-la-estenografia/

de Lorenzo, M. (2011, December 27). ¿Qué es Matrix? *Jot Down Cultural Magazine*. https://www.jotdown.es/2011/12/manuel-de-lorenzo-que-es-matrix/