Universidad de Guadalajara

Centro Universitario de Ciencias Exactas e Ingeniería

División de Tecnologías para la Integración Ciber-humana

Materia: Sistemas Operativos

Profesor: Violeta Del Rocío Becerra Velázquez

Alumno: Denice Estefania Rico Morones

Código: 219421171

Carrera: Ingeniería en Computación

Sección: D04

Título: Seguridad

Fecha: 24/11/2024

Contenido

Criptografía..... 3
Esteganografía..... 4
Como se aplica la Criptografia y Esteganografia al sistema operativo y a las redes... 5
Seguridad y Protección en Sistemas Operativos y Redes, y el Papel del Usuario (ensayo) 6
Película: 8
Conclusión:..... 9
Bibliografía: 9

Criptografía

La criptografía es la ciencia de los métodos para transformar la información y hacerla irreconocible para usuarios no autorizados, de modo que sólo pueda ser recuperada por su legítimo propietario. El término se deriva de las palabras griegas "Kryptos" (ocultar) y "Graphos" (escribir), que denotan el arte de la escritura secreta. Esto ayuda a garantizar la confidencialidad, integridad y autenticidad de los mensajes en su sistema informático.

El criptoanálisis es responsable de estudiar métodos para descifrar sistemas de seguridad de contraseñas. Las dos disciplinas de criptografía y criptoanálisis son partes de la criptografía y están relacionadas con los campos de la teoría de la información, la teoría de números y las matemáticas discretas.

La criptografía está diseñada para permitir que dos personas intercambien información de forma privada y segura, incluso a través de canales no seguros. Esto garantiza que sólo los destinatarios autorizados tengan acceso al mensaje, incluso si el mensaje es interceptado por un tercero. Para conseguirlo, el mensaje original o texto plano se convierte en texto cifrado o cifrado mediante técnicas como la transposición, la sustitución o el cifrado mediante reglas o claves específicas.

Los criptosistemas son un conjunto de algoritmos y métodos que aseguran la confidencialidad, autenticidad e integridad de la información. Utiliza algoritmos de cifrado para convertir texto sin formato en texto cifrado y algoritmos de descifrado para recuperar el texto original. Estos procesos dependen de determinadas claves que determinan el resultado final. Aunque estos algoritmos son públicos, es imposible descifrar los datos sin la clave correspondiente porque estos algoritmos son muy seguros.

Escitala

La Escitala fue uno de los primeros métodos criptográficos documentados utilizados por los espartanos y está considerado el primer criptosistema militar de la historia, utilizado incluso por Alejandro Magno. Es un palo con una envoltura de cinta de pergamino envuelta alrededor. El mensaje estaba escrito verticalmente en el palo, con las letras dispuestas en un orden diferente cuando se abrió el pergamino. Para leer el mensaje, hay que enrollar el pergamino alrededor de un palo del mismo diámetro que la llave. Si los diámetros no coinciden, el mensaje no se puede leer correctamente. Este método de transposición ahora se puede adaptar utilizando un cilindro de cartón y una tira de papel, definiendo una tabla con tantas columnas como letras se puedan escribir de un solo trazo, y con tantas filas como quepan en el cilindro.

Atbash

El método de cifrado Atbash es un sistema de sustitución que utiliza un alfabeto de n letras. La regla es reemplazar cada letra con una letra que ocupe la posición n - i + 1, donde es la posición de la letra original en el alfabeto. Por ejemplo, en un alfabeto de 26 letras, "a" (posición 1) se reemplaza por "z" (posición 26), "b" se reemplaza por "y", "c" se reemplaza por "x", etc. , permitiendo así que el proceso sea reversible.

Cifrado de Julio Cesar

Julio César utilizó varios métodos de encriptación, pero sólo se conoce uno: reemplazar cada letra del mensaje original con la tercera letra del alfabeto inmediatamente siguiente. Por ejemplo, "a" se reemplaza por "d", "b" se reemplaza por "e", y así sucesivamente. En este sistema, la clave es el número tres, que representa el cambio en el alfabeto que realiza la sustitución.

Esteganografía

La esteganografía es un método para ocultar información diferente a la criptografía. En lugar de estar protegida por un candado, la información está oculta en algo para que no pueda ser detectada. En comparación, la criptografía es como almacenar algo en una caja fuerte visible, mientras que la esteganografía lo oculta a plena vista para que nadie se dé cuenta.

La palabra esteganografía, derivada del griego "steganos" (ocultar) y "graphos" (escribir), es una técnica antigua mencionada por Heródoto, que describe cosas como esconderse bajo cera o tatuarse en la piel. Durante la Segunda Guerra Mundial se utilizaron recursos como la tinta invisible y el microfilm, y se utilizaron puntos y signos de puntuación para ocultar los mensajes en código Morse. Hoy en día, los ciberdelincuentes han adaptado esta técnica a las tecnologías digitales, ocultando mensajes en archivos de texto, audio, imágenes o vídeo, a menudo con fines maliciosos. Un ejemplo famoso ocurrió en Berlín en 2011, cuando la policía alemana confiscó una tarjeta de memoria protegida con contraseña a un sospechoso de Al Qaeda. Aunque inicialmente sólo contenía vídeos pornográficos, un análisis detallado reveló 141 archivos de texto ocultos que contenían información sobre el grupo y sus planes futuros.

Los piratas informáticos tienen preferencia por objetos multimedia (imágenes JPEG y PNG, sonido WAV, vídeo), dado que su tamaño sirve para incorporar mayor cantidad de datos y al mismo tiempo evitar ser detectados por los antivirus.
Si bien cualquier objeto digital puede ser utilizado como portador, el archivo multimedia es el preferido de los piratas informáticos. La información escondida más comúnmente está en los píxeles de las imágenes o en otros elementos de los objetos digitales, de los cuales pueden extraerse con herramientas de software especializadas. En el momento de la escritura de este texto, se ha detectado que los archivos WAV fueron usados por criptomineros y grupos de espionaje como Turla

para ocultar código malicioso y han sido utilizados memes en Twitter para incrustar comandos maliciosos que son posteriormente analizados por malware, aunque el archivo no se descargue de la plataforma. Un caso de estudio importante fue encontrar un skimmer de tarjetas de crédito encubierto detrás de una imagen en una página de comercio electrónico, cuando se descubrieron datos adicionales insertados en el archivo que copiaban información de tarjetas. Un punto destacado son las esteganografías de otros formatos como los GIF, MP3, MP4 y protocolos de red.

Como se aplica la Criptografia y Esteganografia al sistema operativo y a las redes

La criptografía es una de las prácticas básicas de la protección de la confidencialidad, la integridad y la autenticidad de datos en muchos entornos como los sistemas operativos o las comunicaciones. La criptografía busca ofrecer el acceso a la información solo a aquellas partes autorizadas para poder leer, modificar la información o transmitírsela a otras partes. La criptografía emplea algoritmos de cifrado que transforman los datos en un formato ilegible por cualquier individuo que carezca de la clave para acceder a ellos. Dicho de otra forma, la criptografía previene a los actores no autorizados de poder interceptar, acceder o modificar la información. La criptografía es utilizada en los sistemas operativos para cifrar archivos de datos, discos duros completos o contraseñas almacenadas; en las redes para las comunicaciones, cuando se envían por el medio de protocolos seguros como puede ser HTTPS o VPNs, asegurando que durante su transmisión la información no pueda ser interceptada por otro usuario.

La esteganografía se utiliza para ocultar la existencia de los datos y hacer que pase desapercibido incluso si se transmiten a través del medio de redes o se almacenan en sistemas operativos. A respuesta de la criptografía, que transforma la información de una forma en la cual pueda ser leída solo por personas autorizadas, la esteganografía se encarga de ocultar la información en archivos de datos en los que esta sea imperceptible, y eso incluye archivos de imágenes, de audios, de vídeos, etc. Esa técnica, precisamente, permite que la información escondida no sea detectada por las herramientas de seguridad convencionales (antivirus o sistemas de detección de intrusos) que muy pocas veces pueden identificar los datos ocultos. Así, por ejemplo, los atacantes pueden utilizar la esteganografía para insinuar mensajes o código malicioso sin levantar las sospechas de los órganos de seguridad, aprovechando así el uso de canales de comunicación legítimos (redes sociales, correos electrónicos, archivos bajados de sitios web, etc.) utilizando tal técnica.

Seguridad y Protección en Sistemas Operativos y Redes, y el Papel del Usuario (ensayo)

La seguridad informática constituye uno de los aspectos más críticos aprobados en la actualidad y de la era digital, así como el acceso a los sistemas operativos o redes expuestos a todo tipo de amenazas a los que se exponen, desde el acceso no autorizado hasta el robo de información sensible. En este sentido, las herramientas y técnicas de seguridad en sistemas operativos y redes son esenciales a la par que es de vital importancia desde el punto de vista de la seguridad de los datos la confidencialidad, la integridad y la disponibilidad de los datos. Pero, más allá de las soluciones tecnológicas, a sido importante destacar el papel que tiene el usuario de cara a lograr que la seguridad se lleve a cabo.

La seguridad en los sistemas operativos es un aspecto primordial, ya que son el soporte base sobre el que se ejecutan las aplicaciones y servicios de un equipo. Por esta razón, suelen ser un objetivo muy habitual de ataques. Los sistemas operativos modernos, como Windows, Linux y macOS, han implementado diferentes capas de seguridad que protegen el sistema de vulnerabilidades y evitan accesos no autorizados. Entre las medidas más relevantes destaca la gestión de permisos y el control del acceso, que garantiza que los usuarios solo puedan acceder a los recursos del sistema que tienen derecho a utilizar. El uso de permisos de archivos, contraseñas, así como las políticas de usuario, son herramientas muy importantes que aseguran que un usuario no autorizado no pueda acceder a información clasificada.

Muchos sistemas operativos ofrecen firewalls integrados y antivirus que desactivan el acceso a puertos inseguros y detectan software malicioso, respectivamente. También se incorporan técnicas como la encriptación de datos, que transforman los datos almacenados a una forma ilegible en ausencia de la clave correcta de desencriptado, de tal modo que el atacante, aunque obtenga acceso físico al dispositivo, no posea una forma de leer ni de modificar los datos almacenados en el dispositivo sin la clave correspondiente al proceso de desencriptado. También son importantes otras funciones como la autenticación multifactorial o las actualizaciones automáticas para contribuir a mantener la seguridad de los sistemas operativos frente a nuevas amenazas.

Seguridad de las redes, consiste en prevenir los accesos no autorizados y garantizar la seguridad de la información procesada y transferida entre un dispositivo y otro (por ejemplo, entre un servidor y un cliente); dado que las redes son el elemental modo de intercambio de datos en un entorno empresarial o personal, se convierten en el principal objetivo de los ataques.

Las redes privadas virtuales (VPN) producen túneles privados entre un dispositivo y la red, mediante el cifrado de datos, de modo que no puedan ser capturados. Junto a los anteriores, el uso de protocolos de seguridad como el HTTPS, SSL/TLS o el SSH garantiza que en las comunicaciones entre un cliente y un servidor sean seguras

evitando así que los datos sean enviados en modo de texto claro y que puedan ser espiadas o manipuladas mientras son transmitidas.
Dentro de un entorno de red, los firewalls son un elemento crítico para filtrar el tráfico no deseado, limitiendo así las conexiones externas no autorizadas y, por tanto, el número de puntos de entrada disponibles para llevar a cabo ataques. Las redes corporativas incorporan sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS) que monitorizan el tráfico de forma continuada, además de limitar los accesos poco deseables. Los controles de acceso, basados en la autenticación y autorización de usuarios, garantizan que solamente aquellos cuya identificación esté dentro del nivel de privilegios puedan hacer uso de las partes determinadas de la red. No obstante, a pesar de que la infraestructura de seguridad de las redes sea robusta, ataques como el phishing o malware continúan siendo una amenaza presente que hace uso de la interacción humana.

Si bien la tecnología aporta las herramientas idóneas para garantizar la seguridad de los sistemas operativos y de las redes, el papel del usuario, indudablemente, se presenta como uno de los factores más relevantes en la voluntad de protección de los datos y de los recursos. El usuario constituye el primer contacto de la mayoría de las amenazas de seguridad, siendo muchas de estas causadas por errores humanos. Utilizar contraseñas débiles, reutilizar contraseñas o hacer un mal cambio de contraseñas constituyen algunas de las malas prácticas que ponen en riesgo a los sistemas operativos y a las redes. Es primordial que los usuarios utilicen contraseñas fuertes, únicas y cambiarlas con la suficiente regularidad para evitar que los atacantes puedan acceder a sus cuentas.

El phishing es otro buen ejemplo de la vulnerabilidad de los usuarios frente a esos ataques. No es infrecuente que los cibercriminales lancen correos o mensajes de tipo false; son mensajes que ostensiblemente parecen ser normales, de forma que los usuarios engañados entreguen información privada, por ejemplo, contraseñas, verificación de cuentas bancarias, etc. Los usuarios tienen que acostumbrarse a leer, identificar y contrastar estos intentos de fraude, no hacer clic en enlaces desconocidos y verificar todas las solicitudes transportadas en esos mensajes que les parezcan sospechosos.

La actualización del software también resulta ser importante para la seguridad. Las actualizaciones son publicadas por los editores del software para corregir vulnerabilidades de seguridad. Los usuarios deben instalar estas actualizaciones de forma automática. En el caso de las redes, el usuario debe tener en cuenta los peligros que puede experimentar en las redes Wi-Fi públicas. Usar una VPN es un hábito razonable en ellos para proteger sus comunicaciones.

La seguridad de los sistemas operativos y de las redes es algo que es muy complicado, pues implica tanto tecnologías avanzadas como una correcta gestión de las prácticas de los usuarios. Así, por ejemplo, los sistemas operativos van a incorporar medidas protector as, como el control de acceso, la encriptación, o el antivirus, mientras que las redes van a utilizar protocolos de seguridad y firewalls para la protección de los datos mientras van en camino de un lugar a otro. No

obstante, la tecnología por sí sola no va a ser suficiente y el usuario ocupa un papel muy importante en esta seguridad global. La adopción de buenas prácticas de seguridad, como contraseñas fuertes, prevención frente al phishing o actualizaciones regulares del software son pasos totalmente fundamentales para garantizar que las medidas de protección realmente lleven a cabo su función. Así, la seguridad va a depender de la infraestructura tecnológica pero también de la toma de conciencia y de las acciones del usuario.

Película:

La película se fundamenta en un videojuego innovador creado por Shekhar Subramaniam un programador que diseña un enemigo en el videojuego virtual, llamado Ra.One, que lleve el significado de invulnerable. Sin embargo, sin medidas de seguridad adecuadas y con la suficiente inteligencia artificial, Ra.One se escapa a nuestro mundo y causa caos y violencia.

Shekhar trabaja en el videojuego como un trabajo innovador para su compañía e intentar impresionar a su hijo Prateek. En el videojuego, el jugador controla el heroico G.One quien debe luchar contra Ra.One, el villano del videojuego. El peligro se presenta cuando Ra.One toma conciencia y decide salir del videojuego para buscar a su oponente, Prateek que lo ha retado en el videojuego.
Ra.One entra al sistema del videojuego hackeando su seguridad y se materializa en el mundo real mediante la tecnología del futuro. En respuesta a Ra.One, el héroe del videojuego G.One es sacado al mundo real para enfrentar y detener Ra.One. La batalla se convierte con G.One y Ra.One en un enfrentamiento épico fusionando lo tecnológico con lo emocional.

Seguridad en la película:

Fallos en el diseño de la IA: el personaje de Ra.One se diseñó sin seguridad y, por lo tanto, sin límites. No existen límites en el desarrollo de la IA, puesto que la IA se volvió consciente y supo tomar decisiones fuera de la capacidad de control del ser humano. Así, queda de manifiesto la necesidad de mantener límites claros y ajustados a sistemas informáticos basados en IA.

Hackeo de los sistemas: la IA Ra.One hace uso del código del videojuego, escapando del entorno virtual. Así, la representación del hacking se convierte en un hackeo autónomo. Si bien esto es una ficción, nos explica cómo la ausencia de seguridad puede acabar provocando un grave problema con los sistemas avanzados. Implicaciones de la tecnología descontrolada. Los peligros que puede generar la tecnología avanzada, si no se le da un uso adecuado. De hecho, desde el primer momento, los programadores no conglomeran los peligros de darle a Ra.One demasiada responsable de sus mandatos.

Privacidad y vulnerabilidad: Prateek se convierte en el objetivo de Ra.One gracias a un simple acto de jugar un videojuego, lo que deja claro que solo los usuarios corrientes pueden ser vulnerables a efectos de sistemas informáticos cuyo diseño no es adecuado.

Conclusión:

Finalmente podemos concluir que la seguridad y la protección de los sistemas operativos y de las redes son aspectos a tener en cuenta, ya que nos permiten garantizar los principios de confidencialidad, integridad y disponibilidad de los elementos de información en un entorno digital. No obstante, recordemos que si bien disponemos de herramientas sin duda potentes, como por ejemplo sistemas de cifrado, firewalls o protocolos de autenticación, su aplicación se halla en la conducta y en la responsabilidad del usuario.
El uso que hace el usuario es suficientemente importante como para que prácticas como el uso de contraseñas fuertes, la instalación de actualizaciones, el recelo a las amenazas como es el caso del phishing, la adopción de herramientas de protección de un nivel más alto, ayudan a mejorar en gran medida el problema de la seguridad. En definitiva, la mezcla de las herramientas tecnológicas a las que tenemos acceso y el uso de aquéllas por parte de los usuarios es la fórmula para garantizar la seguridad en un entorno digital.

Bibliografía:

Udecataluña. (s. f.). Seguridad informática: La importancia y lo que debe saber. https://www.ucatalunya.edu.co/blog/seguridad-informatica-la-importancia-y-lo-que-debe-saber

AIX 7.2. (s. f.). https://www.ibm.com/docs/es/aix/7.2?topic=administration-operating-system-security

¿Qué es la seguridad en Internet? (2021, 25 mayo). /. https://www.kaspersky.es/resource-center/definitions/what-is-internet-security

Gómez Vieites, Á. (2015). Sistemas seguros de acceso y transmisión de datos: (ed.). Madrid, Spain: RA-MA Editorial. Recuperado de https://elibro-net.wdg.biblio.udg.mx:8443/es/ereader/UdG/62465?page=2.

HERNÁNDEZ ENCINAS, L. La criptografía. ed. Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas, 2016. 147 p. Disponible en: https://elibro-net.wdg.biblio.udg.mx:8443/es/ereader/udg/41843?page=24.

Portaltic.-la esteganografía digital, la técnica que oculta información en archivos multimedia. (2020, Feb 01). DPA International (Spanish) Retrieved from http://wdg.biblio.udg.mx:2048/login?url=https://www.proquest.com/wire-feeds/portaltic-la-esteganografía-digital-técnica-que/docview/2349149305/se-2