GESTIÓN Y SOPORTE DE SEGURIDAD EN HARDWARE Y SOFTWARE

Fundamentos criptográficos

Unidad 2

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yañez

ELABORACIÓN

Experto disciplinar: Felipe Reyes Cáceres

Diseñador instruccional: Antonio Colmenares Prieto

Editora instruccional: María José Fonseca Palacios

VALIDACIÓN

Experto disciplinar:

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Didactic

AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Identifican criptografía en sistemas informáticos vigentes, considerando normativas internacionales.

Introducción

El cifrado es el proceso técnico de convertir información en una contraseña que le permite ocultar los datos que envía, recibe o almacena. Básicamente, se utiliza un algoritmo para cifrar los datos antes de que el destinatario utilice la clave de descifrado para descifrarlos.

En esta ocasión, estudiaremos lo relacionado los fundamentos principales de la encriptación actual.

1. Los fundamentos de la encriptación

El proceso de cifrar un mensaje es diferente al de firmarlo. Ambos procesos se denominan cifrado, pero no son lo mismo.

Los datos transmitidos a través de un canal inseguro como Internet deben mantenerse confidenciales. Cuando los datos están encriptados, se cambian de un texto sin formato a un texto cifrado, o datos enmascarados que solo las personas confiables pueden entender. Al cifrar los datos, se garantiza su confidencialidad independientemente de la naturaleza de la transmisión.

Las firmas digitales o firmas electrónicas son formas modernas de criptografía utilizadas para probar la autenticidad e integridad de la información. También brindan garantías de que el documento no fue alterado o repudiado. Las firmas digitales son similares a las firmas

manuscritas en que prueban la identidad del autor de la firma y confirman la integridad de la información.

Los cuatro pilares de la seguridad son la confidencialidad, la autenticidad, la integridad y el no repudio.

La criptografía moderna requiere la comprensión de los principios básicos. Debido a que estos principios pertenecen a la criptografía, es necesario comprender las firmas electrónicas.

La raíz griega krypto, traducida como criptografía, se refiere a la escritura de información oculta.

Los mensajes confidenciales requieren criptografía para garantizar que solo los destinatarios autorizados puedan entenderlos. Para que ocurra el cifrado, un proceso llamado algoritmo de cifrado necesita convertir el texto de un mensaje que desea proteger en una tontería irreconocible.

Al aprender a realizar un algoritmo de encriptación, los estudiantes primero aprenden los pasos u operaciones. Luego, deben usar una "clave" para revertir el proceso y obtener el texto original.

La Clave determina cómo opera un algoritmo de encriptación, determinando el resultado del proceso. Cambiar las implementaciones clave daría como resultado diferentes textos cifrados si se usan por separado en el mismo texto sin formato.

Los protocolos criptográficos estipulan cómo se utilizan las claves y fórmulas para encontrar los mensajes. El descifrado inverso, que extrae

la clave del criptograma y el texto sin formato, se denomina "extracción de clave". Dado que este proceso se realiza mediante un algoritmo y una clave, es una forma de encriptación.

La criptografía simétrica utiliza la misma clave tanto para el cifrado como para el descifrado.

Transmitir la información presentada en la imagen de la figura requiere procesos de cifrado/descifrado que utilizan componentes de un modelo criptográfico. Estos componentes incluyen las letras del alfabeto latino.

Para cifrar correctamente las letras, primero determine su valor numérico. Luego, suma 5 a ese número y eleva al cuadrado el resultado. Este es un proceso explicado en la oración anterior asociando el número 4 con la letra A. Finalmente, determina el orden del alfabeto aplicando la primera premisa. Esto es equivalente al número entero que comienza en 40000 o "42". Un número derivado de la clave se resta del valor, que luego se calcula en 4 posiciones. Este resultado es equivalente a la posición de la tecla en el alfabeto. Se crea una representación visual del valor utilizando el algoritmo determinado a partir de la clave.

La clave para comprender un criptograma es comprender el algoritmo de cifrado. Una vez que se descubre la clave, es imposible descifrar el mensaje incluso si se conoce el algoritmo de cifrado. Esta es la razón por la cual el cifrado de claves se conoce como criptografía simétrica.

La criptografía simétrica utiliza la misma clave tanto para cifrar mensajes como para descifrarlos. Con este sistema, tanto el remitente como el

receptor deben acceder a la clave antes de cifrar un mensaje y transmitirlo a la otra parte. Una vez recibido, el mensaje se puede descifrar usando la misma clave.

La seguridad del algoritmo radica en la complejidad de la clave y su longitud a longitudes desconocidas. Debido a su naturaleza pública, la longitud de una clave se descubre fácilmente. Las longitudes de clave largas son particularmente seguras. La criptografía de clave pública o asimétrica es un invento más reciente que resuelve el problema de la distribución de claves. Sin embargo, requiere medios de distribución seguros, así como un tiempo considerable para calcular una clave. Con la criptografía simétrica, las claves se pueden calcular rápidamente y al mismo tiempo tener una ventaja significativa sobre la criptografía de clave pública.

Martin Hellman y Whitfield Diffie introdujeron el sistema criptográfico de clave pública después de luchar con el problema de la distribución de claves en el antiguo sistema simétrico. Con la criptografía de clave pública, los usuarios tienen una clave privada para su computadora a la que solo ellos tienen acceso y una clave pública que cualquiera puede usar.

La gente entrega las llaves al mismo tiempo. Estas claves están relacionadas a través de las matemáticas y son compartidas por una persona en particular, el destinatario. Llaman a estas claves claves públicas y están a salvo de miradas indiscretas al almacenarse de forma segura con una clave privada.

Cuando un mensaje se cifra con la clave privada del destinatario, solo ellos pueden leer el mensaje una vez que se ha descifrado. Cualquiera puede cifrar mensajes dirigidos a destinatarios que no poseen una clave privada, porque solo ellos tienen acceso a la clave pública.

Este método requiere más tiempo que el simétrico para cifrar un mensaje y una clave cifrada. Las longitudes de clave también son más largas.

La criptografía simétrica se usa típicamente para el cifrado de mensajes. Esto se debe a que permite procesos de cifrado cortos para mensajes grandes. Sin embargo, como vimos, la criptografía simétrica tiene una debilidad significativa. Esa debilidad es que es necesario un intercambio seguro de claves entre los participantes.

Comparación de claves de criptografía asimétrica y simétrica La criptografía simétrica es más rápida que la criptografía de clave pública, pero requiere un tiempo de procesamiento que la criptografía asimétrica no requiere. La criptografía asimétrica compensa este inconveniente al resolver con éxito el problema del intercambio de claves.

Al combinar ambas formas de criptografía, nuestro mensaje se vuelve seguro utilizando las características de ambos modelos. Utilizamos el uso compartido de claves públicas para compartir la clave que se usará para cifrar datos de forma seudónima.

2. Los métodos de encriptación

La criptografía es el proceso de codificación de datos para una comunicación segura. A menudo se emplea en Internet, ya que es esencial para mantener la seguridad al compartir datos, sitios web y foros. Por eso es importante comprender los conceptos básicos de la criptografía, así como sus diferentes tipos. Este ensayo describe aún más cómo funciona la criptografía en Internet, así como la importancia de hacerlo. La criptografía es la técnica de encriptar información o texto para permitir que solo el remitente y el destinatario lo desbloqueen. Utiliza algoritmos matemáticos complejos para realizar esta tarea en la programación de computadoras.

La criptografía es el uso de la tecnología para proteger la información. Se utiliza un proceso criptográfico para asegurar la información a través de una fórmula matemática. Hay tres categorías principales de criptografía: básica, clave pública y firma digital.

La criptología debe proporcionar cuatro objetivos básicos:

- La confidencialidad o privacidad se refiere a la exclusividad de acceso a la información. Solo aquellas personas a las que se les ha otorgado acceso pueden ver la información.
- Durante su viaje del remitente al receptor, el mensaje debe ser capaz de resistir la alteración.

- Sin garantizar la identidad de la otra parte, no se puede establecer una comunicación segura. Esto se conoce como autenticación.
- Cualquier participante de la conversación no puede negar más tarde haber hablado o transmitido información.

Existen dos tipos de cifrado: **asimétrico y simétrico**. Contienen los dos tipos principales de cifrado.

La criptografía simétrica utiliza la misma clave para cifrar y descifrar un mensaje. Antes de realizar cualquier acción, la clave debe ser compartida entre el remitente y el receptor.

El cifrado asimétrico utiliza diferentes claves para el cifrado y descifrado.

La criptografía asimétrica utiliza dos claves a la vez para realizar su cifrado.

Cualquiera que necesite enviarle información cifrada puede obtener fácilmente la clave pública. Entonces, cualquiera puede cifrar datos usando esta clave. Nunca comparta la información privada.

El cifrado asimétrico utiliza dos claves: una clave pública que se puede compartir con cualquier persona y una clave privada que se mantiene en secreto. La clave pública permite enviar mensajes usando un resumen de mensajes creado usando un algoritmo específico. La clave privada

debe usarse con la clave pública correspondiente para descifrar el resumen del mensaje.

La comunicación confidencial con un colega requiere la distribución de un par de claves. Un par de claves se compone de una clave privada que solo conoce el destinatario y una clave pública que todos conocen. Si tres compañeros de trabajo quieren enviarnos un archivo cifrado, pueden enviarnos su clave pública de forma segura. Esta clave se puede usar para descifrar el archivo cifrado que solo puede leer nuestra clave privada.

Las claves para acceder a una criptomoneda se generan utilizando algoritmos extremadamente complejos que las hacen difíciles de descifrar por parte de los ciberdelincuentes. Esto se debe a que las claves privadas se derivan de las claves públicas.

Confirmar la identidad de alguien junto con el documento firmado es un propósito secundario útil. Mucha gente lo usa para firmar documentos legales. Esto se debe a que se utilizan claves privadas y públicas para firmar y verificar al remitente.

Ya sabemos cómo funciona cada tipo de cifrado. Sin embargo, ¿es uno más eficiente que el otro? Eso requeriría descubrir las ventajas y desventajas asociadas con cada método. Debido a que las ventajas y desventajas provienen de tres perspectivas diferentes, podemos considerar cómo se ve cada categoría a través de tres lentes.

La velocidad se relaciona con el ritmo al que se logra algo. Por ejemplo, un corredor rápido puede recorrer una distancia mayor que uno lento.

La razón principal por la que las personas eligen el cifrado simétrico es porque es rápido y fluido; es la elección perfecta para cifrar grandes cantidades de datos.

El cifrado asimétrico es mucho más rápido que el cifrado asimétrico funcional. Si la velocidad es un factor crítico, el cifrado asimétrico funcional es la mejor opción.

Debido a que el cifrado simétrico es intrínsecamente fácil de descifrar, no es muy seguro. La clave debe ser compartida de una manera muy vulnerable. Encontrar métodos seguros para compartir la clave es crucial.

El cifrado asimétrico permite una comunicación segura que requiere claves públicas. Esto se debe a que los usuarios pueden entregar su clave privada a un tercero, mientras que la clave pública permanece con ellos.

El cifrado asimétrico proporciona beneficios de administración de claves. Solo se necesita un par de claves para cada usuario por mensaje que se debe cifrar. Esto facilita el cifrado de mensajes para múltiples usuarios.

Como vimos con el ejemplo de cifrado simétrico anterior, la cantidad de claves aumenta a medida que aumenta la cantidad de usuarios. El

cifrado se utiliza para proteger nuestros datos en Internet mediante la creación de una red segura con candados cerrados.

El cifrado de datos es esencial cuando usamos nuestras computadoras u otros equipos relacionados. Esto se debe a que el cifrado de datos se utiliza para proteger nuestra privacidad y evitar que la información quede expuesta. Por ejemplo, cuando se usa una computadora, el cifrado de datos se usa para protegerse contra miradas indiscretas.

Una URL que comienza con las letras HTTPS hace que los usuarios de sitios web accedan a sitios web utilizando claves públicas y privadas. Esto permite cifrar los datos. Cuando un usuario accede a un sitio web con una URL HTTPS, el servidor web envía la clave pública al navegador. Esto se llama "apretón de manos SSL" o "hola".

Cuando se establece una conexión segura entre el navegador y el sitio web, se indica con un candado o barra verde. Esto ocurre una vez que el navegador reconoce el enlace como seguro por lo que debemos entender que la principal diferencia entre http y https es su encriptación.

BitLocker es una herramienta integrada en Windows que utiliza métodos de cifrado para cifrar datos en una unidad. Esto evita que cualquier persona acceda a los archivos sin autorización. BitLocker está disponible en las ediciones Windows Education, Enterprise y Pro.

3. Algoritmos de encriptación

RSA, o Rivest, Shamir y Adleman, es un algoritmo de cifrado de clave pública.

La seguridad y utilidad de la factorización radica en su clave pública. Cada clave pública se convierte en una clave privada correspondiente mediante un factor. Los mensajes se expresan numéricamente. El código C++ creado por Sergii Osadchyi utiliza ECC, o RSA ECC, como algoritmo de cifrado.

El algoritmo de Symantec se recomienda para teléfonos inteligentes y otros dispositivos pequeños, como tarjetas inteligentes y chips. Utiliza claves pequeñas para el cifrado y, como resultado, funciona mejor. Este algoritmo fue creado por Code Example C++ de ANSSI France. Su creación fue motivada por DSA (Digital Signature Algorithm) de Code Example en C++ de NSA.

SSL es un algoritmo de cifrado y firma digital utilizado por muchos gobiernos e instituciones, como el Instituto Nacional de Estándares y Tecnología y los Estándares Federales de Procesamiento de la Información. También es importante tener en cuenta que SSL no es solo para personas con conocimientos de tecnología o que entienden términos como RSA, ECC, firmas digitales y más. Actualmente en el mercado tecnológico se pueden encontrar usuarios que no están familiarizados con la tecnología, niños, adolescentes, adultos mayores e incluso usuarios no adultos. Debido a esto, la educación sobre los riesgos

potenciales del uso de la tecnología es necesaria para que los usuarios puedan protegerse independientemente del uso de un antivirus.

4. Protocolos de encriptación

IBM MQ admite protocolos de comunicación seguros como TLS. Esto permite enviar y recibir datos con privacidad e integridad de datos. El protocolo TLS es parte de la capa de transporte de la comunicación basada en SSL.

La confidencialidad, la integridad de los datos y la confirmación de identidad y autoridad se proporcionan a través de ambos protocolos mediante certificados digitales.

Las diferencias entre los dos protocolos son lo suficientemente significativas como para que no se puedan conectar entre sí. Además, las versiones TLS y SSL 3.0 no se pueden conectar entre sí.

La capa segura de comunicación entre dos partes es Transport Layer Security, o TLS. Ofrece una comunicación segura con integridad y confidencialidad de los datos. El protocolo TLS evolucionó a partir del protocolo Netscape SSL 3.0, pero recuerde que TLS y SSL no pueden interactuar.

La comunicación entre un cliente y servidor SSL (Secure Sockets Layer) y un cliente y servidor TLS (Transport Layer, Application Layer) requiere un protocolo de enlace. Este proceso protege los canales seguros de ambas partes.

Al conectarse a un servidor, TLS usa el cifrado para probar la identidad, mantener la confidencialidad y probar la integridad. Cada paso requiere el uso de un algoritmo criptográfico diferente. Durante la autenticación de cliente y servidor, cada usuario debe cifrar sus datos con una clave diferente de un par de claves asimétricas. Luego, tienen que descifrar los datos con la otra clave. Esto es lo que se conoce como resumen de mensaje, que proporciona integridad.

Dentro de cada protocolo criptográfico hay un conjunto de reglas acordadas con respecto a las comunicaciones seguras. Estas reglas se transmiten mediante el uso de CipherSpecs y CipherSuites. Cada protocolo define una combinación específica de algoritmos a la que se adhieren ambas partes.

Las firmas digitales en Secure Sockets Layer y Transport Layer Security se crean cifrando un reflejo de un mensaje que contiene información. Esto se hace con la clave privada del firmante y generalmente usa un resumen de mensaje en lugar del mensaje real.

El gobierno de EE. UU. interactúa con los sistemas de TI y la seguridad de sus ciudadanos. Un método de comunicación con el gobierno es a través del NIST, también conocido como el Instituto Nacional de Estándares y Tecnología. NIST se encarga de publicar consejos técnicos sobre seguridad y protección de los sistemas informáticos. Otra responsabilidad importante del NIST es desarrollar estándares y propuestas que serían implementadas por el gobierno de los Estados

Unidos. Uno de estos estándares es FIPS, o Estándares Federales de Procesamiento de Información.

La Agencia de Seguridad Nacional de los Estados Unidos tiene la tarea de brindar asesoramiento técnico sobre seguridad y encriptación. Lo hacen a través de una integración de múltiples algoritmos criptográficos en la Suite B de su estándar.

5. Normativas de estándares IEEE

IEEE P1363 es un proyecto de estandarización del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) para la criptografía de clave pública . Incluye especificaciones para:

- Criptografía tradicional de clave pública (IEEE Std 1363-2000 y 1363a-2004)
- Criptografía de clave pública basada en celosía (IEEE Std 1363.1-2008) Criptografía de clave pública basada en contraseña (IEEE Std 1363.2-2008)
- Criptografía de clave pública basada en identidad mediante emparejamientos (IEEE Std 1363.3-2013)

El presidente del grupo de trabajo en octubre de 2008 es William Whyte de NTRU Cryptosystems, Inc., que se ha desempeñado desde agosto de 2001.

Los ex presidentes fueron Ari Singer , también de NTRU (1999-2001), y Burt Kaliski de RSA Security (1994 -1999).

La Asociación de Estándares IEEE retiró todos los estándares 1363 excepto 1363.3-2013 el 7 de noviembre de 2019. [1]

Criptografía tradicional de clave pública (IEEE Std 1363-2000 y 1363a-2004).

Esta especificación incluye esquemas de concordancia de claves, firma y cifrado que utilizan varios enfoques matemáticos: factorización de enteros , logaritmo discreto y logaritmo discreto de curva elíptica .

Esquemas de acuerdos clave

DL / ECKAS-DH1 y DL / ECKAS-DH2 (curva elíptica Discrete Logaritmo / Key Acuerdo Scheme, Diffie-Hellman versión): Esto incluye tanto tradicional Diffie-Hellman y curva elíptica Diffie-Hellman .

DL / ECKAS-MQV (Esquema de acuerdo de clave de curva elíptica / logaritmo discreto, versión Menezes-Qu-Vanstone)

Esquemas de firma

- DL / ECSSA (esquema de firma de curva elíptica / logaritmo discreto con apéndice): incluye cuatro variantes principales: DSA , ECDSA , Nyberg-Rueppel y curva elíptica Nyberg-Rueppel.
- IFSSA (Esquema de firma de factorización de enteros con apéndice): incluye dos variantes de RSA , Rabin-Williams y ESIGN,

con varios métodos de codificación de mensajes. "RSA1 con EMSA3" es esencialmente la firma RSA PKCS # 1 v1.5; "RSA1 con codificación EMSA4" es esencialmente RSA-PSS ; "RSA1 con codificación EMSA2" es esencialmente una firma RSA ANSI X9.31.

- DL / ECSSR (esquema de firma de curva elíptica / logaritmo discreto con recuperación).
- DL / ECSSR-PV (esquema de firma de curva elíptica / logaritmo discreto con recuperación, versión Pintsov-Vanstone).
- IFSSR (Esquema de firma de factorización de enteros con recuperación) Esquemas de cifrado IFES (Esquema de cifrado de factorización de enteros): cifrado esencialmente RSA con relleno de cifrado asimétrico óptimo (OAEP).
- DL / ECIES (esquema de cifrado integrado de logaritmo discreto / curva elíptica): Esencialmente, la variante "DHAES" del cifrado ElGamal .
- IFES-EPOC (Esquema de cifrado de factorización de enteros, versión EPOC) Criptografía de clave pública basada en celosía (IEEE Std 1363.1-2008).

Esquema de cifrado NTRU

- Criptografía de clave pública basada en contraseña (IEEE Std 1363.2-2008)

- BPKAS-PAK (Esquema de acuerdo de claves equilibradas y autenticadas con contraseña, versión PAK)
- BPKAS-PPK (versión PPK)
- BPKAS-SPEKE (versión SPEKE)
- APKAS-AMP (esquema de acuerdo de clave autenticado con contraseña aumentada, versión AMP)
- APKAS-BSPEKE2 (versión BSPEKE2)
- APKAS-PAKZ (versión PAKZ)
- APKAS-SRP3 y SRP6 (versión Secure Remote Password (SRP) 3 y 6) APKAS-SRP5 (versión Secure Remote Password (SRP) 5)
- APKAS-WSPEKE (versión WSPEKE) PKRS-1 (Esquema de recuperación de claves autenticadas con contraseña, versión 1)
- Criptografía de clave pública basada en identidad basada en emparejamientos (IEEE Std 1363.3-2013)

Este estándar se publicó el 15 de noviembre de 2013. Incluye técnicas de cifrado basado en identidad, firmas, cifrado de firmas, acuerdo de claves y reencriptación de proxy, todo ello basado en emparejamientos bilineales.

Cierre

Después de estudiado lo correspondiente a la semana, se puede destacar lo siguiente:

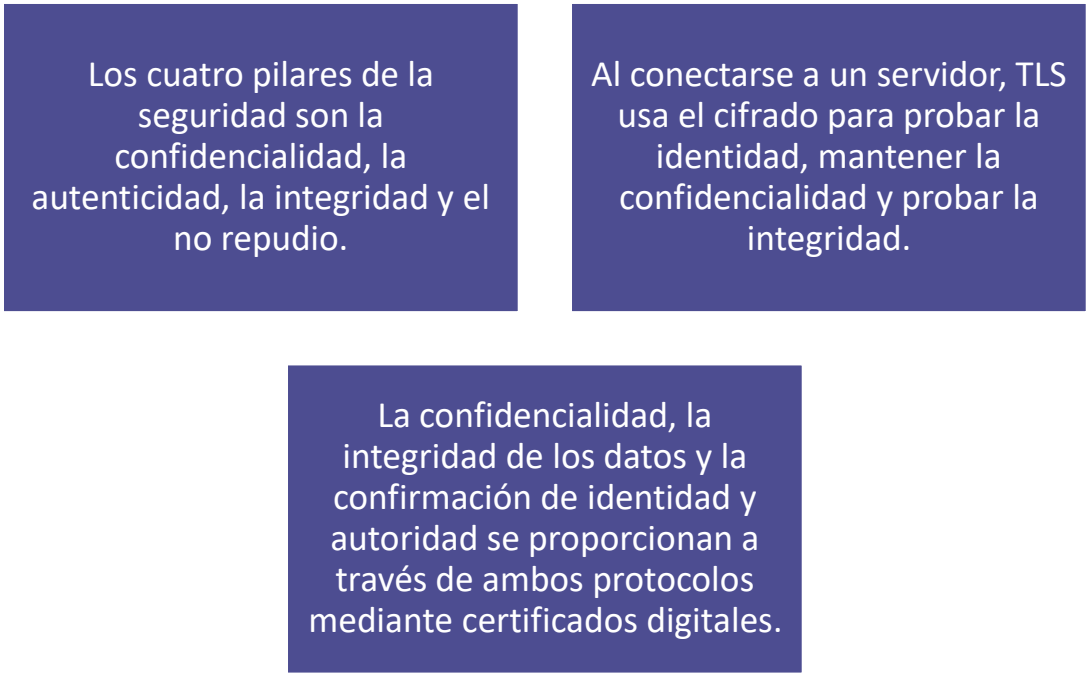

Figura 4. Ideas Claves, semana 4

Fuente: Reyes, F. (2022)

Referencias bibliográficas

CCNA Security 210-260 Official Cert Guide (Santos, Stuppi 2016)