Infraestructura I
Profesor: David Pignalberi

Módulo 5: Cierre de la materia

Sesión 25: Criptografía
Abril 25 de 2022

Criptografía
Es una técnica tiene por objetivo cifrar, codificar o encriptar datos y/o mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Para lograr esconder un mensaje son necesarios dos componentes: un algoritmo y una clave:

Algortimo:
Es una secuencia de instrucciones a las que será sometido el mensaje para cifrarlo o codificarlo.

Clave:
Es una variable que se inserta en el algoritmo, para lograr el resultado deseado. Un mismo mensaje, tratado con un mismo algoritmo, pero codificado con dos claves distintas, debería producir dos resultados diferentes.

Tipos de algoritmos criptográficos

Transposición
Es un algoritmo que se basa en dividir un mensaje, cifrarlo en columnas y luego transcribirlo usando el nuevo orden de los caracteres dado por esas columnas. La cantidad de columnas es la clave que se utiliza para codificar y decodificar el mensaje.

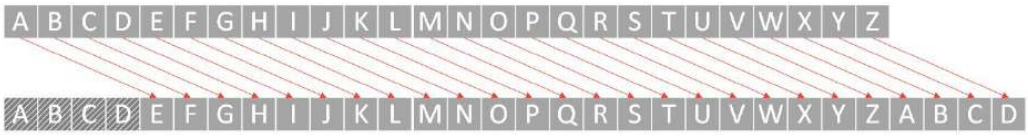
Mensaje a cifrar: "Este mensaje es secreto". **Clave:** Utilizar una matriz de 5x4.

Mensaje codificado: "EEEC SNER TSSE EAST MJEO".

.

Sustitución
La sustitución es un algoritmo criptográfico que produce un mensaje cifrado a partir del reemplazo de los caracteres de un mensaje por otros. El elemento que establece las reglas para el reemplazo es la clave.
Un ejemplo de sustitución es establecer un desplazamiento de dos caracteres en el alfabeto. De este modo, todas las letras "A" del mensaje a cifrar se reemplazan por letras "C". Este algoritmo de sustitución se lo conoce como **cifrado César** o **cifrado por desplazamiento**.

Mensaje a cifrar: "Este mensaje es secreto".
Clave: Desplazamiento de 4 caracteres.



Mensaje codificado: "IWXI QIRWENI IW WIGVIXS".

Ocultación
En el caso de la ocultación, el objetivo es esconder el mensaje en otro mensaje u objeto. La clave en este caso son las indicaciones que permiten al individuo encontrar el mensaje.

Mensaje a cifrar: "Este mensaje es secreto"
Clave: La primera letra de cada oración contendrá el mensaje.
Mensaje codificado: "Elefantes fueron avistados por primera vez en la costa de Nairobi. Sumamente sorprendidos, los conservacionistas se acercaron para observarlos. Tímidos, pero no asustados, los elefantes mantuvieron su posición. El más pequeño de la manada jugaba cerca del agua. Mientras tanto, el elefante que lideraba la familia se aseguraba de que haya una distancia prudencial entre los científicos y su familia. En algunas oportunidades los científicos pudieron acercarse. No podían determinar cuánto tiempo los elefantes estaban allí, de modo que querían aprovechar el tiempo. Subidos a los árboles, algunos científicos pudieron tomar fotografías panorámicas. A la distancia podía observarse una segunda manada aproximándose. Jugaban. Elefantes pequeños. Elefantes grandes. Sorprendidos los científicos decidieron alejarse. Sabían que lo que habían presenciado era un evento único. En tanto el gobierno lo permita, los científicos volverán al sitio. Cuando sea posible volveremos, dijo el jefe de la expedición. Rara vez puede uno ser testigo de un evento como este. Elefantes volviendo a un área donde se los creía extintos. Todos celebraron el evento. Otra parte del equipo prefirió quedarse documentando el suceso para no perder detalles del mismo".

Esteganografía
La esteganografía es una forma de ocultación, de uso habitual para el cifrado de mensajes. Consiste en ocultar un mensaje dentro de un archivo de datos —imagen, audio— sin alterar el contenido original del archivo.

La Criptografía en la Historia

Esparta, s. VII a.C.: Escílata.

Roma, s. I a.C.: Julio César utiliza algoritmo de sustitución por desplazamiento.
Edad Media. Departamento de claves y códigos de El Vaticano.
s. XVIII: Cilindro de Jefferson, usado desde la Guerra de Secesión hasta la II Guerra Mundial.
s. XIX: Descubrimiento y desciframiento de la piedra de Rosseta.
II Guerra Mundial: Máquina Enigma para encriptación de mensajes (Alemania). Alan Turing construyó la máquina Bombe para decodificar dichos mensajes.

Criptografía en los sistemas

Cuando se habla de seguridad informática, los distintos conceptos, estrategias y técnicas para proteger un sistema o una red se construyen sobre tres pilares que se conocen por su sigla en inglés CIA:

- Confidentiality (confidencialidad):
Se refiere a la protección de los datos, recursos y sistemas de accesos no autorizados.

- Integrity (integridad):
Se refiere a la protección de los datos, recursos y sistemas de cambios no autorizados y así asegurar su confiabilidad.

- Availability (disponibilidad):
Se refiere a garantizar que aquellos usuarios autorizados tengan acceso a los datos, recursos y sistemas que necesitan.

La criptografía como vector de ataque

Un **ransomware** es un software que encripta la información de un individuo u organización con propósitos extorsivos. Es decir, mediante el uso de la criptografía, los archivos en cuestión son cifrados utilizando un algoritmo complejo y una clave conocida únicamente por el autor del ataque. Finalmente, se indica al usuario qué operación financiera deberá realizar para el pago del rescate. El ámbito de ataque puede limitarse a una computadora en particular o a toda una red.

Una vez que el ransomware comienza a ejecutarse en el dispositivo, localiza los archivos que está programado para encriptar. Para cumplir con los propósitos extorsivos, el software encripta archivos con extensiones conocidas y que pueden ser de valor para el usuario, pero deja intactos los archivos del sistema operativo. De esta manera, permite al usuario descubrir los efectos del ransomware y acceder a la información necesaria para realizar el pago (si así lo deseara).

Usando la Criptografía para generar Confidencialidad

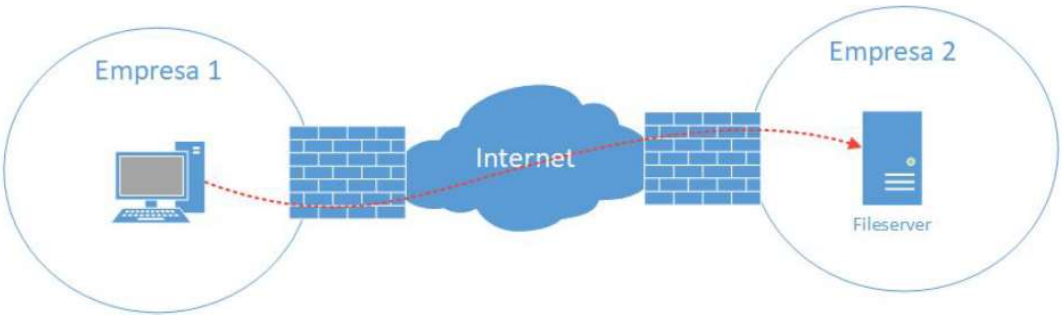
Uno de los usos principales de la criptografía es habilitar la confidencialidad; en otras palabras, mantener datos o información ininteligibles a ojos no autorizados.

Los datos pueden estar en tres estados: at rest, in transit, in use. En los tres casos se debe garantizar su seguridad física y lógica:

	Seguridad Físico	Seguridad Lógico
Data at rest	• Controles de acceso físicos • Camaras de seguridad	• Implementar ACLs para reforzar el principio de 'Least Privilege'. • **Implementar mecanismos de encriptación en los file systems.**
Data in transit	• Evitar redes wifi y priorizar redes cableadas • Encriptación de dispositivos de almacenamiento removibles	• Implementar una VPN (Virtual Private Network) • **Encripción de los datos en tránsito (con TLS / SSL)**
Data in use	• Limitar el acceso a los áreas de trabajo a sólo personal autorizado	• **Encripción de los datos en memoria.** • RBAC (Role Based Access Control) en los sistemas de usuario. • Un sistema de gestión de identidades robusto

Protección de datos en tránsito

Criptografía simétrica:



Las empresas 1 y 2 están conectadas por medio de una VPN. Una computadora en la Empresa 1 necesita acceder a un recurso en la Empresa 2.
Ambas empresas se ponen de acuerdo en el algoritmo a utilizar y la clave que utilizarán.
Por cada mensaje que la Empresa 1 envíe, se produce un paquete cifrado, utilizando el algoritmo definido, la clave compartida y los datos a intercambiar.

Cuando la Empresa 2 recibe el mensaje cifrado, utiliza el mismo algoritmo y clave para realizar la operación inversa y así obtener el mensaje original.

Repositorio Java: Stationary

https://github.com/Juanesp1990

Criptografía asimétrica
En contraste con la criptografía simétrica donde se usa una misma clave para codificar los mensajes entre todas las partes, en la criptografía asimétrica se hace uso de dos claves.
Ambas claves son generadas matemáticamente y en conjunto. De este modo, los mensajes que son codificados con la clave 1, pueden ser decodificados con la clave 2 y viceversa.
En los pares de claves, una se conoce por el nombre de clave pública mientras que la otra se conoce por el nombre de clave privada.

Certificados
Un certificado contiene los siguientes datos:
- Una forma de identificación del sitio que implementa el certificado (IP o nombre de la página)
- Las fechas entre las cuales será válido el certificado
- La clave pública que se usará para codificar la comunicación
- La firma de la entidad certificante que emitió el certificado
- Otros datos que hacen a la seguridad del certificado

Entidad certificante
También conocidas como CA's o Certification Authorities, son las encargadas de verificar que quien solicita el certificado es realmente quien dice ser.

Certificados Auto-firmados (self-signed)
Existe la posibilidad de generar certificados auto-firmados. Un certificado de este tipo no debe ser usado nunca en un ambiente de producción. Ya que de ser así, el navegador advertirá que el certificado fue emitido por una entidad no confiada.

Paso a paso Criptografía asimétrica
1. El cliente ingresa a la URL del sitio web (ej. un home banking).
2. El servidor envía al cliente el certificado.

3. El navegador en el cliente verifica que el certificado sea válido (firmado por una entidad confiada, que no haya expirado y que la URL que estamos visitando coincida con la especificada en el certificado) . De no cumplirse alguna de estas condiciones el navegador indicará que el certificado no es seguro.
4. Una vez que el navegador tiene el certificado, extrae la clave pública para poder intercambiar mensajes de manera segura con el servidor. Pero no es esta clave la que se va a usar para codificar cada mensaje enviado y decodificar cada mensaje recibido, sino que ahora que pueden establecer una comunicación, lo que hacen es generar y negociar una 'session key'. Y es esa 'session key' la que se utilizará para cifrar el resto de la comunicación.

Usar la Criptografía para validar integridad

La idea de verificar la integridad de un dato usando la criptografía es sencilla. El dato para el cual queremos validar su integridad es sometido a un algoritmo (los más conocidos para este propósito son SHA y MD5), el resultado es una cadena de caracteres que se conoce como hash.
De alterarse los datos, al volver a calcular el hash, estos producirían un resultado diferente. Al compararlo con el hash original, la diferencia sería evidente.

Integridad para "Data at Rest"

La forma más habitual de garantizar la integridad de los datos "at rest" es calcular y almacenar el hash,. En una instancia posterior cuando el dato deba ser consultado, se puede verificar elhash y así determinar que los contenidos del archivo no fueron alterados.

Hashear archivo con Powershell:
Get-FileHash -Algorithm MD5 -Path <ruta al archivo> | Select-Object -Property Hash

Integridad para "Data in Transit"

Dado un escenario donde 2 computadoras van a intercambiar mensajes, por ejemplo, cuando una computadora se conecta por medio de una VPN a un servidor, mediante la criptografía también es posible verificar la integridad de cada uno de los paquetes que se va a intercambiar. Por cada paquete se va a enviar mediante la red, es posible calcular el hash que le corresponde y agregar el

resultado a uno de los encabezados del paquete. El servidor del otro lado, recibe el paquete, lo somete al mismo algoritmo, y si produce el mismo hash el paquete es íntegro.

HMAC (Hash Message Authentication Code)
HMAC se usa en escenarios de datos en tránsito donde se puede usar una clave simétrica como entrada adicional para el algoritmo de hashing. Es decir que para producir el hash de ambos lados (emisor y receptor) ambos deben conocer la clave. Esto se hace para evitar que un atacante altere los datos, calcule el hash para el nuevo contenido y reemplace el hash original con el nuevo.

Paso a Paso:
1. Acrodar una clave privada.
2. Calcular el hash del paquete.
3. Recibir el paquete.
4. Transmitir el paquete.

Usar la criptografía como Mecanismo de Autenticación

Usar Criptografía Simétrica y/o HMAC
Cuando usamos criptografía simétrica para proteger una comunicación o un mecanismo como HMAC para proteger la integridad de los datos estamos utilizando una clave criptográfica que es secreta y solo conocida por las partes involucradas. De este modo, podemos decir que al utilizar comunicaciones encriptadas de forma simétrica (confidencialidad), con una clave que es solo conocida por los receptores y emisores (autenticación) y sobre la que se monta HMAC (integridad) estamos cumpliendo con el principio de seguridad CIA (asegurar la confidencialidad, verificar la integridad y autenticar a las partes).

Usar Certificados SSL
Para proteger las comunicaciones, las compañías deben hacer uso de la criptografía asimétrica, y el mecanismo de distribución para la clave pública son los ya conocidos certificados. Para que los mismos para que sean confiables, deben ser emitidos por una entidad certificante conocida por nuestras computadoras. Caso contrario, nuestros navegadoresindican que las claves siendo utilizadas por el sitio del banco no fueron generadas por una entidad confiable. Y para que una entidad confiable genere un certificado en nombre de

una compañía, esta debe poder verificar su identidad. De este modo, y por carácter transitivo, podemos decir que los certificados SSL sirven para verificar la identidad de una compañía y así cumplir con el principio de CIA.

Usar pares de claves asimétricas
En los sistemas Linux la manera tradicional de conectarnos de forma remota es utilizando el comando y protocolo SSH (Secure Shell). El administrador debe ingresar el comando ssh usuario@servidor en una consola para conectarse a otro servidor. A continuación, se procederá a pedir al usuario que ingrese su contraseña. Esto quiere decir que en cada servidor al que nos vayamos a conectar tenemos que tener un conjunto de usuario y password. Si se deben administrar varios servidores, se utilizan claves criptográficas asimétricas par autenticación.

Paso a Paso
1. Un administrador de sistemas utiliza los comandos ssh-keygen o openssl, esto producirá un par de claves (pública y privada). La clave privada debe ser mantenida en secreto y no debe compartirse con nadie.

2. El administrador luego distribuye la clave pública a aquellos servidores a los que quiera conectarse utilizando este método.

3. Una vez distribuida la clave, el administrador solo deberá ejecutar desde la computadora en la que tenemos la clave privada ssh usuario@servidor para conectarse sin la necesidad de proveer ningún dato adicional.

Sesión 26. ITSM.
Abril 27 de 2022.

Falta…

Sincrónico