Seguridad de la Información

El proporcionar una seguridad real hemos de tener en cuenta múltiples factores, tanto internos como externos. En primer lugar habrá que caracterizar el sistema que va a albergar la información para poder identificar las amenazas, y en este sentido podemos hacer la siguiente subdivisión:

1. Sistemas aislados. Son los que no están conectados a ningún tipo de red. De unos años a esta arte se han convertido en minoría, debido al auge que ha experimentado Internet.

2. Sistemas interconectados. Hoy por hoy casi cualquier ordenador pertenece a alguna red, enviando y recogiendo información del exterior casi constantemente. Esto hace que las redes sean cada día más complejas y supongan un peligro potencial que no puede en ningún momento ser ignorado.

En cuanto a las cuestiones de seguridad que hemos podemos clasificarlas de la siguiente forma:

- Seguridad física. Englobaremos dentro de esta categoría a todos los asuntos relacionados con la salvaguarda de los soportes físicos de la información, más que de la información propiamente dicha. En este nivel están, entre otras, las medidas contra incendios y sobrecargas eléctricas, la prevención de ataques terroristas, las políticas de backup, etc. También se suelen tener en cuenta dentro de este punto aspectos relacionados con la restricción de acceso físico a las computadoras únicamente a personas autorizadas.

2. Seguridad de la información. En este apartado prestaremos atención a la preservación de la información frente a observadores no autorizados. Para ello podemos emplear tanto criptografía simétrica como asimétrica, estando la primera únicamente indicada en sistemas aislados, ya que si la empleáramos en redes, al tener que transmitir la clave por el canal de comunicación, estaríamos asumiendo un riesgo excesivo.

3. Seguridad del canal de comunicación. Los canales de comunicación rara vez se consideran seguros. Debido a que en la mayoría de los casos escapan a nuestro control, ya que pertenecen a terceros, resulta imposible asegurarse totalmente de que no están siendo escuchados o intervenidos.

4. Problemas de autentificación. Debido a los problemas del canal de comunicación, es necesario asegurarse de que la información que recibimos en la computadora viene de quien realmente creemos que viene. Para esto se suele emplear criptografía asimétrica en conjunción con funciones resumen

5. Problemas de suplantación. En las redes tenemos el problema añaadido de que cualquier usuario autorizado puede acceder al sistema desde fuera, por lo que hemos de confiar en sistemas fiables para garantizar que los usuarios no están siendo suplantados por intrusos. Normalmente se emplean mecanismos basados en password para conseguir esto.

Criptografía

Según el Diccionario de la Real Academia, la palabra Criptografía proviene del griego *kryptos*, que significa oculto, y *gráphein*, que significa escritura, y su definicióon es: Arte de escribir con clave secreta o de un modo enigmático". Obviamente la Criptografía hace años que dejó de ser un arte para convertirse en una técnica, o más bien un conglomerado de técnicas, que tratan sobre la protección −ocultamiento frente a observadores no autorizados− de la información. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, la Teoría de Números o Matemática Discreta, que estudia las propiedades de los números enteros, y la Complejidad Algorítmica.

Conviene hacer notar que la palabra Criptografía solo se refiere al uso de códigos, por lo que no engloba a las

técnicas que se usan para romper dichos códigos (Criptoanálisis). El término Criptología, aunque no está recogido aún en el Diccionario, se emplea abitualmente

para agrupar estas dos disciplinas.

Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder esconder el mensaje (lo llamaremos cifrar o encriptar), manda el mensaje por una línea de comunicación que se supone insegura y después solo el receptor autorizado pueda leer el mensaje escondido (lo llamamos descifrar o descencriptar).

CIFRAR ENVIAR DESCIFRAR

Criptosistema

Definiremos un criptosistema como una quíntupla (M; C; K; E; D), donde:

- **M** representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto

plano, o plaintext) que pueden ser enviados.

- **C** representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.

- **K** representa el conjunto de claves que se pueden emplear en el criptosistema.

- **E** es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a

cada elemento de M para obtener un elemento de C. Existe una transformación diferente

- **Ek** para cada valor posible de la clave k.

- **D** es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema ha de cumplir la siguiente condición:

Dk (Ek (m)) = m

es decir, que si tenemos un mensaje m, lo ciframos empleando la clave k y luego lo desciframos empleando la misma clave, obtenemos de nuevo el mensaje original m.

Criptoanálisis.

El criptoanálisis consiste en comprometer la seguridad de un criptosistema. Esto se puede hacer descifrando un mensaje sin conocer la llave, o bien obteniendo a partir de uno o más criptogramas la clave que ha sido empleada en su codificación. No se considera criptoanálisis el descubrimiento de un algoritmo secreto de cifrado; hemos de suponer por el contrario que los algoritmos siempre son conocidos.

Existen dos tipos fundamentales de criptosistemas:

- Criptosistemas simétricos o de clave privada. Son aquellos que emplean la misma clave

k tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en comunicaciones la clave k debe estar tanto en el emisior como en el receptor,

lo cual nos lleva preguntarnos cómo transmitir la clave de forma segura.

- Criptosistemas asimétricos o de llave pública, que emplean una doble clave (kp; kP).

kp se conoce como clave privada y kP se conoce como clave pública. Una de ellas sirve para la transformación E de cifrado y la otra para la transformación D de descifrado.

En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para descifrar y viceversa. Estos criptosistemas deben cumplir además que el conocimiento de la clave pública kP no permita calcular la clave privada kp.

En la práctica se emplea una combinación de estos dos tipos de criptosistemas, puesto que los segundos presentan el inconveniente de ser computacionalmente mucho más costosos que los primeros. En el mundo real se codifican los mensajes (largos) mediante algoritmos simétricos, que suelen ser muy eficientes, y luego se hace uso de la criptografía asimétrica para codificar las claves simétricas (cortas).

Para poder entender un poco de la criptografía, es tiempo de plantear que tipo de problemas resuelve ésta. Los principales problemas de seguridad que resuelve la criptografía son: la privacidad, la integridad, la autenticación y el no rechazo.

La privacidad, se refiere a que la información sólo pueda ser leída por personas autorizadas.

Ejemplos: en la comunicación por teléfono, que alguien intercepte la comunicación y escucha la conversación quiere decir que no existe privacidad. Si mandamos una carta y por alguna razón alguien rompe el sobre para leer la carta, ha violado la privacidad.

En la comunicación por Internet es muy difícil estar seguros que la comunicación es privada, ya que no se tiene control de la línea de comunicación. Por lo tanto al cifrar (esconder) la información cualquier intercepción no autorizada no podrá entender la información. Esto es posible si se usan técnicas criptográficas, en particular la privacidad se logra si se cifra el mensaje con un método simétrico.

La integridad, se refiere a que la información no pueda ser alterada en el transcurso de ser enviada.

Ejemplos: cuando compramos un boleto de avión y están cambiados los datos del vuelo, puede afectar los planes del viajero. Una vez hecho un deposito en el banco, si no es capturada la cantidad correcta causará problemas. La integridad es muy importante en las transmisiones militares ya que un cambio de información puede causar graves problemas.

En internet las compra se puede hacer desde dos ciudades muy distantes, la información tiene necesariamente que viajar por una línea de transmisión de la cual no se tiene control, si no existe integridad podrían cambiarse por ejemplo el número de una tarjeta de crédito, los datos del pedido en fin información que causaría problemas a cualquier comercio y cliente.

La integridad también se puede solucionar con técnicas criptográficas particularmente con procesos simétricos o asimétricos.

La autenticidad, se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mando o que el mensaje recibido es el que se esperaba.

Ejemplo: cuando se quiere cobrar un cheque a nombre de alguien, quien lo cobra debe de someterse a un proceso de verificación de identidad para comprobar que en efecto es la persona quien dice ser, esto en general se lleva a cabo con una credencial que anteriormente fue certifica y acredita la identidad de la persona

que la porta. La verificación se lleva a cabo comparando la persona con una foto o con la comparación de una firma convencional.

Por internet es muy fácil engañar a una persona con quien se tiene comunicación respecto a la identidad, resolver este problema es por lo tanto muy importante para efectuar comunicación confiable.

Las técnicas necesarias para poder verificar la autenticidad tanto de personas como de mensajes usan quizá la más conocida aplicación de la criptografía asimétrica que es la firma digital, de algún modo ésta reemplaza a la firma autógrafa que se usa comúnmente. Para autenticar mensajes se usa criptografía simétrica.

El no rechazo, se refiere a que no se pueda negar la autoría de un mensaje enviado.

Información Segura Persona Autorizada

Cuando se diseña un sistema de seguridad, una gran cantidad de problemas puedes ser evitados si se puede comprobar autenticidad, garantizar privacidad, asegurar integridad y evitar el no−rechazo.

La criptografía simétrica y asimétrica conjuntamente con otras técnicas, como el buen manejo de las claves y la legislación adecuada resuelven satisfactoriamente los anteriormente problemas planteados, como lo veremos en los capítulos posteriores.

Critografía Clásica.

El ser humano siempre ha tenido secretos de muy diversa índole, y ha buscado mecanismos para mantenerlos fuera del alcance de miradas indiscretas. Julio César empleaba un sencillo algoritmo para evitar que sus comunicaciones militares fueran incerceptadas. Leonardo Da Vinci escribía las anotaciones sobre sus trabajos de derecha a izquierda y con la mano zurda. Otros personajes, como Sir Francis Bacon o Edgar Allan Poe eran conocidos por su afición a los códigos criptográficos, que en muchas ocasiones constituían un apasionante divertimento y un reto para el ingenio.

Los mecanismos criptográficos considerados clásico son todos los sistemas de cifrado anteriores a la II Guerra Mundial, o lo que es lo mismo, al nacimiento de las computadoras. Estas técnicas tienen en común que pueden ser empleadas usando simplemente lápiz y papel, y que pueden ser criptoanalizadas casi de la misma forma. De hecho, con la ayuda de las computadoras, los mensajes cifrados empleando estos códigos son fácilmente descifrables, por lo que cayeron rápidamente en desuso.

La transición desde la Criptografía clásica a la moderna se da precisamente durante la II Guerra Mundial, cuando el Servicio de Inteligencia aliado rompe la máquina de cifrado del ejército alemán, llamada ENIGMA.

Todos los algoritmos criptográficos clásicos son simétricos, ya que hasta mediados de los años setenta no nació la Criptografía asimétrica.

Critografía Simétrica

La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

Este tipo de criptografía se conoce también como criptografía de clave privada o criptografía de llave privada.

Existe una clasificación de este tipo de criptografía en tres familias, la criptografía simétrica de bloques (block cipher), la criptografía simétrica de lluvia (stream cipher) y la criptografia simétrica de resumen (hash functions).

Aunque con ligeras modificaciones un sistema de criptografía simétrica de bloques puede modificarse para convertirse en alguna de las otras dos formas, sin embargo es importante verlas por separado dado que se usan en diferentes aplicaciones.

La criptografía simétrica ha sido la más usada en toda la historia, ésta a podido ser implementada en diferente dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.

Aunque no existe un tipo de diseño estándar, quizá el más popular es el de Fiestel, que consiste esencialmente en aplicar un número finito de interacciones de cierta forma, que finalmente da como resultado el mensaje cifrado. Este es el caso del sistema criptográfico simétrico más conocido, **DES**.

Critografía Simétrica

La criptografía asimétrica es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada.

Dependiendo de la aplicación que le demos al algoritmo, la clave pública será la de cifrado o viceversa. Para que estos criptosistemas sean seguros también ha de cumplirse que a partir de una de las claves resulte extremadamente difícil calcular la otra.

Los algoritmos de llave púlica, o algoritmos asimétricos, han demostrado su interés para ser empleados en redes de comunicación inseguras (Internet). Introducidos por Whitfield Diffiey Martin Hellman a mediados de los años 70, su novedad fundamental con respecto a la criptografía simétrica es que las claves no son únicas, sino que forman pares. Hasta la fecha han aparecido multitud de algoritmos asimétricos, la mayoría de los cuales son inseguros.

Otros son poco prácticos, bien sea porque el criptograma es considerablemente mayor que

el mensaje original, bien sea porque la longitud de la clave es enorme. Se basan en general

en plantear al atacante problemas matemáticos difíciles de resolver. En la práctica muy pocos algoritmos son realmente útiles. El más popular por su sencillez es RSA, que ha sobrevivido a multitud de ataques, si bien necesita una longitud de clave considerable.

Otros algoritmos son los de ElGamal y Rabin.

Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos. Por

ejemplo, mientras que para algoritmos simétricos se considera segura una clave de 128 bits, para algoritmos asimétricos se recomiendan claves de al menos 1024 bits.

Además, la complejidad de cálculo que comportan estos últimos los hace considerablemente más lentos que los algoritmos de cifrado por bloques.

En la práctica los métodos asimétricos se emplean únicamente para codificar la clave

Secreta (simétrica) de cada mensaje.

CRIPTOGRAFÍA SIMÉTRICA vs CRIPTOGRAFÍA ASIMÉTRICA

La **Criptografía Simétrica**, es claramente insuficiente para llevar a cabo comunicaciones seguras a través de canales inseguros, debido a que los dos interlocutores necesitan compartir una clave secreta. Dicha clave debe ser transmitida en algún momento desde un extremo a otro del canal de comunicación de forma segura, ya que de ella depende la protección de toda la información que se transmita a lo largo de esa sesión en particular. Necesitamos, pues, un canal seguro para poder crear otro canal seguro.

La **Criptografía Asimétrica** ofrece una salida al problema, proporcionando ese canal seguro de comunicación que va a permitir a los participantes intercambiar las claves de sesión (como se mencionaba anteriormente). Y ésa no es la única ventaja, ya que los algoritmos asimétricos ofrecen mecanismos fiables para que ambos interlocutores se puedan identificar frente al otro de manera segura. La razón por la que no se emplean algoritmos asimétricos todo el tiempo es porque, entre otras ventajas, los criptosistemas simétricos resultan mucho más eficaces y rápidos.

LINEA DE COMUNICACION INSEGURA