Seguridad electrónica en la gestión de información

MARCOS GESTAL, JUAN LUÍS PÉREZ
Departamento de Tecnologías de la Información y las Comunicaciones
Facultad de Informática – Universidade da Coruña

1. Introducción

La sociedad actual está caracterizada por un amplio uso de las diferentes tecnologías de la información y las comunicaciones. Dichas tecnologías ponen al alcance del usuario un abanico casi infinito de posibilidades para la compartición de documentos, imágenes, etc… Sin embargo, estas ventajas y facilidades, en ocasiones, ocultan los riesgos que una exposición excesiva de dicha información puede provocar.

En este capítulo trata de darse una visión global que permita al usuario conocer el tipo de riesgos, amenazas,… a los que se expone y una serie de herramientas a su alcance para enfrentarse a ellos.

2. Seguridad

La seguridad de las redes y de la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles. A continuación se explican en mayor detalle cada uno de estos conceptos.

2.1. Requisitos de seguridad

Los requisitos generales de seguridad de las redes, tanto públicas como privadas, y los sistemas de información presentan las siguientes características generales interdependientes:

✔ ***Confidencialidad (secreto)***

Protección de las comunicaciones o de los datos almacenados contra su interceptación y lectura por parte de personas no autorizadas. Requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, por ejemplo mediante cifrado.

En el secreto no sólo se incluye la privacidad de los datos, sino también el flujo de información, es decir, se debe proteger la identidad del origen y destino(s) del mensaje, por ejemplo enviando los datos confidenciales a muchos destinos además del verdadero, así como el volumen y el momento de tráfico intercambiado, por ejemplo produciendo una cantidad de tráfico constante al añadir tráfico espurio al significativo, de forma que sean indistinguibles para un intruso. La desventaja de estos métodos es que incrementan drásticamente el volumen de tráfico intercambiado, repercutiendo negativamente en la disponibilidad del ancho de banda bajo demanda.

✔ ***Integridad***

Confirmación de que los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados. Requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos.

La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera, por ejemplo mediante un hash criptográfico con firma, mientras que la integridad de secuencia de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada y que no hay unidades repetidas o perdidas.

✔ ***Accesibilidad (disponibilidad)***

Los recursos del sistema informático han de estar disponibles a las entidades autorizadas cuando éstas los necesiten. Se han de proporcionar mecanismos que impidan el acceso a las entidades no autorizadas y mecanismos para que las entidades autorizadas puedan disponer de los recursos.

✔ ***Autenticidad***

Requiere una identificación correcta del origen del mensaje, asegurando que la entidad emisora no es falsa. Se distinguen dos tipos: de entidad, que asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares; y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.

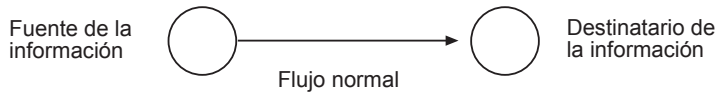
La autenticación debe contemplar la posibilidad de mantener el anonimato, dado que muchos servicios no necesitan la identidad del usuario.

✔ ***Imposibilidad de rechazo (no-repudio)***

Ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin.

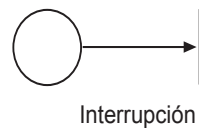
2.2. Amenazas

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario.



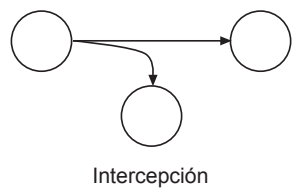
Un ataque no es más que la realización de una amenaza. Las cuatro categorías generales de amenazas o ataques son las siguientes:

✔ ***Interrupción***



Un recurso del sistema es destruido o se vuelve no disponible, de manera temporal o permanente. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

✔ ***Intercepción***



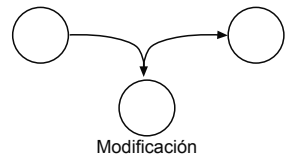
Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son *pinchar* una línea para hacerse con datos que circulen por la red (que es lo que realizan los programas denominados *sniffers*) y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

Al no producirse, por lo general, una alteración de los datos del sistema su detección se hace realmente complicada.

✔ ***Modificación***

Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar líneas de código de un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

✔ ***Fabricación o generación***



Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información.

Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad**: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos

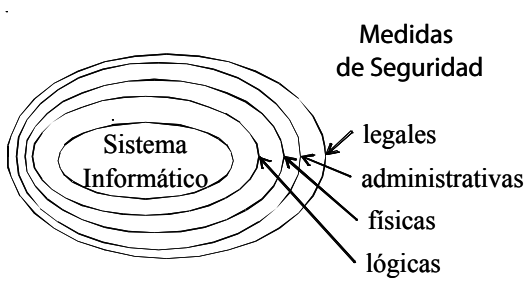
privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

- **Reactuación**: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
- **Modificación de mensajes**: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesetas en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesetas en la cuenta B".
- **Degradación fraudulenta del servicio**: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

Es preciso tener en cuenta todos los factores que pueden amenazar la seguridad, y no únicamente los de carácter malintencionado. Desde el punto de vista de los usuarios, los peligros derivados de los incidentes del entorno o de errores humanos que alteren la red pueden ser tan costosos como los ataques malintencionados.

3. Medidas de seguridad

Las medidas de seguridad que se deben establecer en un sistema se muestran en la figura de la derecha. Son de cuatro tipos: medidas de seguridad lógica, medidas de carácter físico; medidas de carácter administrativo y, por último, medidas de carácter legal.



3.1. Medidas físicas

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas – técnicas de protección – ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del espacio físico en el que se ubican los activos de un sistema informático, así como a los medios de acceso al mismo y desde el mismo. Las principales amenazas que se prevén en la seguridad física de un sistema son:

- ✔ Desastres naturales, incluyendo terremotos, incendios accidentales, tormentas…
- ✔ Amenazas ocasionadas por el hombre.
- ✔ Disturbios, sabotajes internos y externos.

A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento de datos, sala de commutación de una red local, etc. junto con una serie de acciones encaminadas a prevenir, reducir y recuperar los errores ocasionados.

Incendios

Son una de las principales amenazas contra la seguridad. Puede originarse por múltiples causas: fallo en las instalaciones eléctricas, fallos o sobrecalentamiento en los equipos…

Deben observarse una serie de medidas de seguridad para prevenir, o al menos mitigar, los daños causados: existencia de falso piso en el que aislar la conducción eléctrica, impermeabilidad del espacio físico en el que se encuentren los equipos, mantenimiento de la temperatura entre unos márgenes adecuados, existencia de equipos extintores…

Inundaciones

Junto con los incendios son una de las principales causas de situaciones de desastre en los sistemas informáticos a nivel físico. Pueden deberse a fenómenos naturales (tormentas, riadas…) o estar provocadas por las actuaciones de sofoco de un incendio, rotura de conducción de aguas…

Son aplicables la mayoría de medidas de seguridad que en el caso de los incendios: impermeabilización, doble piso, etc.

Instalación eléctrica

Debe tenerse en cuenta que todo sistema de información depende de una manera total de la existencia de fluido eléctrico. Por lo tanto, deberá prestarse especial atención a este apartado. Las amenazas a la seguridad de un sistema pueden darse por varios motivos. Uno de los más comunes son los picos y ruidos electromagnéticos, que aparte de interferir en la calidad de los datos, favorecen la escucha electrónica. Se suelen emplear SAI – siglas de sistema de alimentación ininterrumpida, UPS en inglés – que, además de filtrar la señal eléctrica, poseen un conjunto de baterías que les permite mantener en funcionamiento los equipos durante un tiempo razonable ante una caída del suministro eléctrico. Este tiempo ha de ser al menos suficiente para poder apagar con seguridad los equipos.

Cableado de red

El cableado de red también puede ser blanco de ataques o fuente de problemas. Se pueden realizar monitorizaciones del tráfico de red, inducción de interferencias accidental (producidas por fuentes electromagnéticas próximas) o provocada (para degradar la calidad del servicio), realizar conexiones no autorizadas a la red de la organización… Para reducir los peligros se utilizan diversas técnicas: empleo de cables de fibra óptica (que son inmunes a las interferencias provocadas por campos electromagnéticos), utilización de cableado apantallado (minimiza el impacto de los campos electromagnéticos en los cables metálicos) hasta el empleo de cableado de alta seguridad. Éste último se emplea únicamente en organizaciones en las que la seguridad de la información es de vital importancia, por ejemplo, el ejército. El objetivo que se persigue con la utilización de este tipo de cableado es impedir la posibilidad de filtraciones o monitorización de la información que circula por el cable. Éste consta de un sistema de tubos cerrados herméticamente por el que circula aire a presión y el propio cable de red. A lo largo de estos tubos existen sensores conectados a una computadora que dispara un sistema de alarma cuando se detecta algún tipo de variación en la presión del aire.

3.1.1. Control de accesos físicos

El control de accesos no sólo requiere la capacidad de identificación, sino también asociar dicha capacidad a la apertura o cierre de puertas, al permiso o denegación del acceso basado en restricciones de tiempo, área o privilegios.

Personal de seguridad

Quizás el método más común de control de acceso físico consiste en la utilización de personal o guardias de seguridad. A cualquier personal ajeno al sistema que se desea proteger se le requerirá completar un formulario con sus datos personales, los motivos de la visita, la hora de llegada y de salida, etc.

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz de la entrada y salida de personal en los diferentes sectores de la organización que se protege.

En este caso cada una de las personas se identifica por algo que posee, por ejemplo una tarjeta de identificación. Cada una de estas tarjetas tiene un PIN (Personal Identification Number) único, siendo éste el que se almacena en una BD para su posterior seguimiento, en caso de que fuese necesario. El mayor inconveniente es que estas tarjetas pueden ser copiadas, robadas, etc. permitiendo el acceso a cualquier persona que la posea.

Las personas también pueden acceder mediante algo que saben (por ejemplo un número de identificación o una clave de acceso) que se solicitará a su entrada en la zona de acceso restringido. Al igual que en el caso de identificación, los datos aportados por el personal se contrastarán contra una BD en la que estarán almacenados los datos de las personas autorizadas. Como principales desventajas de este sistema tengamos presente que generalmente se eligen identificadores sencillos – con lo que es fácil que pueda acceder al sistema una persona no autorizada – o que estas identificaciones se olvidan.

Sistemas biométricos

La principal desventaja de la utilización de personal de guardia reside en el hecho de *quién vigila al vigilante*. Es decir, se corre el riesgo de que ante situaciones de amenaza, soborno, etc. una persona pueda acceder a aquellos sectores a los que no esté autorizada. Otra posibilidad es que el propio personal de se-

guridad acceda de manera fraudulenta a los sistemas de la organización. Ante situaciones de este estilo se recomienda el uso de sistemas biométricos para el control de accesos.

La biometría es la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos. La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una BD. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas, digitales, voz, etc.)

Utilizando la biometría se elimina la necesidad de poseer una tarjeta identificadora. Aunque su coste se ha visto considerablemente reducido, el verdadero beneficio de su eliminación reside en la reducción del trabajo concerniente a su administración. Utilizando un dispositivo biométrico los costes de administración son menores, únicamente se necesita realizar el manteniendo del lector biométrico y mantener la BD actualizada. Además, y lo que es más importante, las características biométricas de una persona son intransferibles.

Entre los sensores biométricos más empleados se encuentran los sensores de emisión de calor, el análisis de huellas dactilares, analizadores de voz y verificadores de patrones oculares.

Los sensores de emisión de calor miden la emisión de calor del cuerpo (termograma), realizando un mapa de valores sobre la forma de cada persona. Además de para la identificación de personas, estos sensores también pueden utilizarse para verificar que una estancia se encuentre vacía.

Basados en el principio de que no existen dos huellas dactilares iguales, los sensores dactilares se vienen utilizando desde tiempo atrás con excelentes resultados. Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc., llamados minucias, características. La posición relativa de cada una de ellas se analiza para establecer la identidad de una persona. Diversos estudios han establecido que dos personas no tienen más de ocho minucias iguales, y que cada persona posee más de 30, lo que hace este método sumamente interesante.

Los analizadores de voz comparan ciertos parámetros de la voz obtenida de la persona que desea acceder al sistema (entonación, diptongos, agudeza, timbre, etc.) con la dicción de un fragmento previamente grabado y almacenado en la

BD. Este sistema es muy sensible a factores externos como pueden ser el ruido ambiental, el estado de ánimo de la persona que desea acceder, enfermedades, envejecimiento, etc.

Los modelos de verificación de patrones oculares están basados en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (sobre una población de 200 millones de personas, la probabilidad de coincidencia es prácticamente nula).

Verificación automática de firmas

En este caso lo que se considera es lo que el usuario es capaz de hacer. Los sistemas verificadores de firmas también podrían encuadrarse dentro de las verificaciones biométricas.

Para cualquier técnica de falsificación es extremadamente complejo reproducir las características dinámicas de una persona, como pueda ser la firma. La verificación automática de firmas, usando emisiones acústicas, toma datos del proceso dinámico de firmar o escribir. La secuencia sonora de estas emisiones generadas por el proceso de escribir constituye un patrón que es único para cada individuo.

Protección electrónica

Se denomina así a la detección de robos, intrusión, incendios, etc. mediante la utilización de sensores conectados a centrales de alarmas. Cuando uno de estos sensores detecta una situación de riesgo, trasmite aviso a la central; ésta procesa la información recibida y alerta al personal de seguridad de la situación de emergencia.

Entre los elementos de protección electrónica se encuentran las barreras de infrarrojos y microondas. Estas barreras están compuestas por un receptor y un transmisor entre los que se emiten haces, codificados para evitar sabotajes, de luces infrarrojas y de microondas respectivamente. Cuando este haz se interrumpe, se activa el sistema de alarma. Estas barreras son inmunes a la luz ambiental, movimientos de masas de aire, etc. Las barreras infrarrojas pueden cubrir áreas de hasta 150 metros de longitud y reflejar sus rayos por medio de espejos para cubrir con una misma barrera diferentes sectores. Una ventaja de las barreras de microondas con respecto a las infrarrojas reside en su capacidad de atravesar ciertos materiales (vidrio, plástico, madera, hormigón, …).

Los detectores ultrasónicos utilizan ultrasonidos para crear un campo de ondas. Cualquier movimiento que se realice dentro del espacio protegido generará una perturbación en dicho campo que accionará las alarmas.

3.2. Medidas lógicas

Una vez visto como un sistema puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de proceso de datos (CPD) no serán sobre los medios físicos sino contra la información almacenada y procesada en él.

El activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la asegure. Estas técnicas las brinda la seguridad lógica. Este tipo de seguridad consiste en la *aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo*.

En la seguridad informática existe una regla no escrita que dicta que *todo lo que no está permitido hacer debe estar prohibido*; esto es lo que debe asegurar la seguridad lógica. Los objetivos que se plantean son:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los empleados puedan trabajar sin una supervisión minuciosa y que no puedan modificar programas ni archivos que no les corresponda.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos, según un procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada.
5. Que la información recibida sea la misma que se ha transmitido.

3.2.1. Controles de acceso lógico

Este tipo de controles pueden implementarse en el sistema operativo, sobre las propias aplicaciones, BD, paquetes específicos de seguridad… Constituyen una importante ayuda para proteger al sistema operativo y demás software, reguardar la información confidencial de accesos no autorizados…

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relativos al procedimiento que se lleva a cabo para determinar si un usuario puede acceder a un determinado recurso del

sistema. Al respecto se han definido los siguientes estándares de seguridad que indican los requisitos mínimos de seguridad en cualquier sistema:

3.2.1.1. Identificación y autenticación

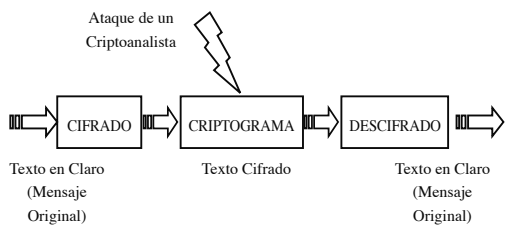
Se trata de la primera línea de defensa en la mayoría de los sistemas y es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios, siendo por lo tanto de las primeras medidas de seguridad que han de tomarse encaminadas a securizar estos aspectos.

Se denomina identificación al momento en el que el usuario se da a conocer en el sistema, y autenticación a la verificación que realiza el sistema sobre esta identificación.

Al igual que se consideró para la seguridad física, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad de un usuario.

- Algo que solamente el usuario conoce, por ejemplo un password de acceso, una clave criptográfica, un número de identificación personal…
- Algo que el usuario posee, por ejemplo una tarjeta magnética.
- Algo que el usuario es y que lo identifica de manera unívoca, por ejemplo las huellas dactilares.
- Algo que el individuo es capaz de hacer, por ejemplo los patrones de escritura.

3.2.2. Cifrado



Se trata, sin lugar a dudas, de la técnica que más ampliamente se emplea para dotar de seguridad a un sistema. Etimológicamente la palabra criptología significa *arte de escribir de un modo enigmático*. Es decir, consiste en transformar un mensaje inteligible en otro que no lo es (mediante claves que sólo el emisor y destinatario conocen) para después volverlo a su forma original, de tal manera que cualquiera que tenga acceso al mensaje cifrado –denominado criptograma– sea capaz de descubrir su significado.

Se pueden diferenciar dos tipos principales de sistemas de cifrado, o criptosistemas, que a continuación se describen brevemente:

- Simétricos o de clave privada: se emplea una misma clave K para que cifre el emisor y descifre el destinatario, por lo tanto ambos han de poseer dicha clave. El mayor inconveniente que presentan es que se debe contar con un canal seguro para la transmisión de dicha clave.

  Los sistemas criptográficos clásicos son de este tipo: sustitución simple (cifrado tipo CESAR), sustitución homofónica (uno de los sistemas de este tipo más característicos es el de Beale: el alfabeto del cifrado lo representan los números enteros que indican la posición de una palabra en la declaración de independencia de los EEUU cuya primera letra se corresponde con la que letra que se desea cifrar), substitución polialfabeto… También son de este tipo cifrados más complejos como el DES.

  Todos estos sistemas se basan en la aplicación de 2 operaciones básicas: la substitución (que en términos de la teoría de la información e Shannon busca la confusión del mensaje original) y la transposición (que busca la difusión del mensaje original)

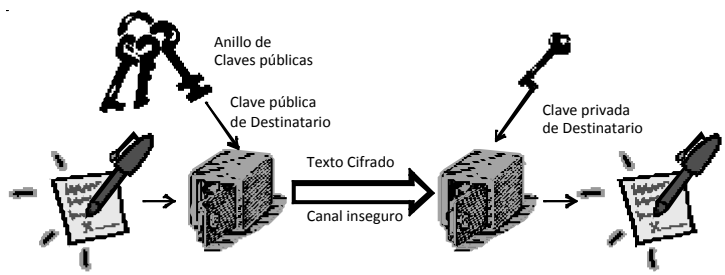
  La fortaleza de cualquier algoritmo de cifrado de clave privada se basa en el secretismo bajo el que se mantenga la referida clave, pues el algoritmo y su funcionamiento han de ser públicos, según postula el principio de Kerckhoff.

- Asimétricos o de clave pública: se emplea una doble clave, pública y privada. Una de ellas se utiliza para el cifrado y otra para el descifrado de mensajes. En muchos de los sistemas existentes los papeles de estas claves son intercambiables, es decir, si utilizamos una de las claves para cifrar se utiliza la otra para descifrar y viceversa.

  Cifrados de este estilo son los exponenciales, el RSA (basado en la teoría de los números primos)… Este último cifrado también se utiliza para la firma electrónica (invierte el papel de las claves: cifra con la clave privada y descifra con la pública).

  Haciendo una analogía, el cifrado de clave pública equivaldría a que cada entidad participante en una comunicación dispusiese de un contenedor va-

cío (o un buzón de correo) del que sólo su legítimo propietario dispone de la llave para su apertura. Este contenedor sería de acceso público, es decir, no existiría la obligación de mantenerlo en secreto. Cada vez que alguien quisiese establecer un canal de comunicación seguro necesitaría solicitar el contenedor o buzón de la persona destinataria (es decir, su clave pública). El destinatario del mensaje procedería a enviar al destinatario uno de sus buzones abierto. Una vez ésta estuviese en poder de la entidad que desea iniciar la comunicación, podrá introducir en dicho buzón su mensaje y, a continuación cerrarlo. Desde ese mismo instante, la única manera de acceder al contenido del mensaje es a través de la llave que abre el buzón (la clave privada), que únicamente se encuentra en poder del propietario del buzón. Se garantiza de éste modo que únicamente el destinatario legítimo tiene acceso a la información.



Aún así, este esquema presenta una fuerte debilidad. ¿Quién garantiza que el buzón que se envía a una entidad se corresponde realmente a ella (autenticidad) y no se trata de una usurpación de identidad? De esta manera, el origen de la comunicación podría pensar que está comunicándose con un receptor dado, cuando la realidad posiblemente fuese otra. Para solucionar este aspecto basta hacer uso de una Autoridad de Certificación, que garantice de alguna manera que el buzón que cada entidad tiene expuesto (su clave pública) es realmente de dicha entidad. Esta certificación puede realizarse a través de certificados digitales que, a grandes rasgos, contienen la identificación personal de una entidad dada, su clave pública y una firma digital del mismo.

Bajo este esquema (origen A cifra de un mensaje con la clave pública del destinatario B) se obtiene un sistema que ofrece las siguientes características:

- A puede enviar un mensaje cifrado a B utilizando la clave pública de B
- B puede descifrar el mensaje utilizando su clave privada
- Únicamente el destinatario podrá descifrar el mensaje (puesto que sólo él posee la clave privada)

De esta manera, se proporcionan las siguientes características a la transmisión de información:

- Confidencialidad: sólo el usuario legítimo podrá leer el mensaje
- Integridad: si el mensaje cifrado se altera no se podrá descifrar en el destino.

Sin embargo, tal y como se comentó anteriormente, las claves suelen ser intercambiables. Es decir, todo lo que se cifre con una de las claves (pública o privada) puede ser descifrado con la otra. Así, otra opción sería cifrar con la clave privada del origen el mensaje, en vez de iniciar una comunicación cifrando el contenido de un mensaje con la clave pública del destinatario. De esta manera, el sistema resultante ofrecería las siguientes características:

- Cualquier usuario (que disponga de la clave pública del origen de la comunicación) podrá descifrar el mensaje
- Por lo tanto, no proporciona confidencialidad
- Sin embargo sí proporciona:
    - Integridad: si el mensaje es alterado no se podrá descifrar, con lo que se tiene la certeza de que el documento recibido es exactamente el mismo que el que se cifró.
    - autenticidad del emisor: sólo el emisor puede haber cifrado el mensaje con su clave privada, ya que sólo él tiene esa clave. De esta manera se atribuye de forma irrefutable la procedencia del documento.
    - no repudio: el emisor no puede negar que haya sido él quien cifró el mensaje.

Este es el mecanismo que posibilita el funcionamiento de la firma digital.

A nivel comparativo entre ambos tipos de cifrado, la principal ventaja que aporta el cifrado simétrico (o de clave privada) sobre el cifrado asimétrico es la mayor rapidez y eficiencia a la hora de cifrar. Por el contrario, se trata de métodos menos seguros (dependiendo evidentemente de la longitud de la clave) y tienen otro punto débil en el elevado número de claves que se necesita generar para garantizar la existencia de comunicaciones seguras en escenarios con múltiples escenarios (en concreto si existen N usuarios, cada uno de ellos ha de poseer N-1 claves diferentes para poder comunicarse con el resto). Al contrario, empleando una arquitectura de clave pública se tiene una mayor seguridad y se necesita generar únicamente un par de claves (pública/privada) para cada usuario, a costa de sacrificar la velocidad de cifrado.

3.2.3. Firma digital

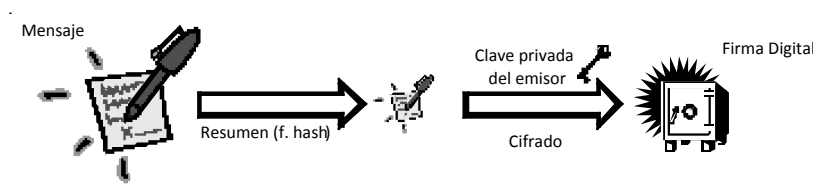
La firma digital trata de trasladar al ámbito informático las mismas propiedades de las que dispone la firma manuscrita. Así, tal y como se comentó anteriormente, cifrando un documento con la clave privada del autor de la firma consigue dotarse al citado documento de integridad, autenticidad y no repudio.

No obstante, tal y como se ha comentado con anterioridad, el cifrado mediante algoritmos simétricos es altamente ineficiente, con lo que no es una opción viable cifrar todo el contenido de un documento con la clave privada del emisor para proceder a su firma. Para solventar este inconveniente, la firma digital hace uso de las llamadas *funciones hash* o funciones unidireccionales de resumen.

Básicamente, una función hash lo que hace es generar un resumen de tamaño fijo a partir de un documento N (idealmente utilizando la totalidad del documento original). Será este resumen lo que posteriormente se cifre empleando la clave privada del emisor.

Por lo tanto, el proceso de firma digital podría resumirse en los siguientes puntos:

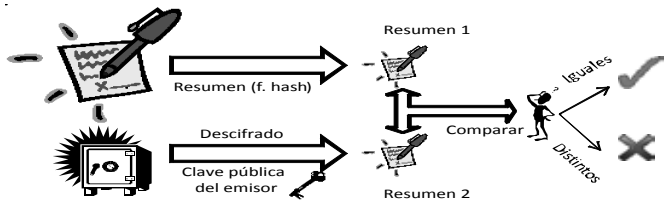
- Se genera un resumen del documento (empleando una función hash conocida)
- El resumen se cifra empleando la clave privada emisor
- Se envía al destinatario el documento original y el resumen firmado (opcionalmente puede adjuntarse la clave pública del remitente para facilitar la validación de la firma)



Una vez que el destinatario recibe el mensaje, para comprobar su validez ha de realizar los siguientes pasos:

- Generar un resumen del documento recibido, usando la misma función unidireccional de resumen.
- Descifrar con la clave pública del origen el resumen firmado.

• Si el resumen firmado coincide con el resumen que él ha generado, la firma es válida, en caso contrario será errónea.



3.2.4. Certificados digitales

La seguridad de la firma digital se basa en un aspecto clave: la confianza en la clave pública del emisor. Esta confianza se garantiza mediante un certificado digital: un documento firmado electrónicamente que acredita la clave pública contenida en el certificado del emisor.

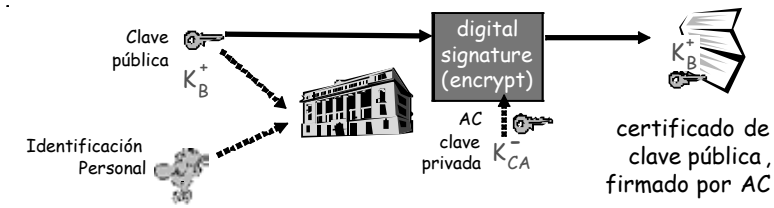
Para lograr esto, los certificados digitales han de ser emitidos por un organismo (la Autoridad de Certificación, p.e. Fábrica Nacional de Moneda y Timbre) en la que confíen ambas partes involucradas en la comunicación. Este organismo firma digitalmente la información con su clave, de ahí que sea de vital importancia la confianza de todas las partes.

Como norma general, los certificados expedidos por una autoridad de certificación incluyen la siguiente información:

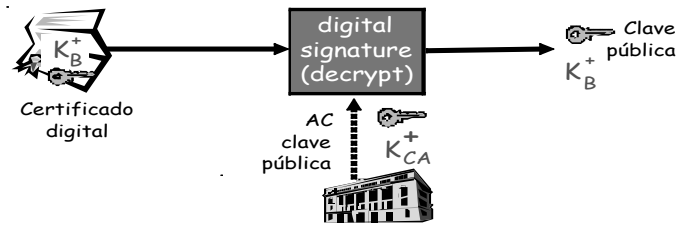
• Identificación del propietario del certificado
• Clave pública [puede incluirse también la privada]
• Fecha de expedición y periodo de validez
• Identificación de la Autoridad de Certificación
• Firma digital del certificado

La obtención de un certificado digital ha de requerir, por lo tanto, algún mecanismo que permita acreditar la identidad del solicitante ante la autoridad de certificación, por ejemplo a través de la asistencia en persona ante la autoridad de certificación.

Una vez comprobada la identidad, la Autoridad de Certificación podrá generar el certificado digital, simplemente mediante la firma digital de la clave pública del solicitante, empleando para ello la clave privada de la propia Autoridad de Certificación.



A partir de este instante la clave pública de un usuario podrá obtenerse de forma segura a través de su certificado digital. Bastará para ello aplicar la clave pública de la Autoridad Certificadora (en la que, recuérdese, todos los participantes han de confiar) al certificado digital.



3.3. Medidas organizativas

3.3.1. Políticas de Seguridad

El término política de seguridad se suele definir como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales qué está y qué no está permitido en el área de seguridad durante la operación general de dicho sistema. Al tratarse de 'términos generales', aplicables a situaciones o recursos muy diversos, suele ser necesario refinar los requisitos de la política para convertirlos en indicaciones precisas de qué es lo permitido y lo denegado en cierta parte de la operación del sistema, lo que se denomina política de aplicación específica.

Una política de seguridad puede ser prohibitiva, si todo lo que no está expresamente permitido está denegado, o permisiva, si todo lo que no está expresamente prohibido está permitido. Evidentemente la primera aproximación es mucho mejor que la segunda de cara a mantener la seguridad de un sistema; en este caso la política contemplaría todas las actividades que se pueden realizar en los sistemas, y el resto – las no contempladas – serían consideradas ilegales.

Cualquier política ha de contemplar seis elementos claves en la seguridad de un sistema informático: disponibilidad, utilidad (la información almacenada por el sistema ha de ser útil), integridad, autenticidad, confidencialidad, posesión (los propietarios de un sistema han de ser capaces de controlarlo en todo momento)

Análisis de riesgos

El término análisis de riesgos hace referencia al proceso necesario para responder a tres cuestiones básicas sobre la seguridad: ¿qué se quiere proteger? ¿contra quién o qué protegerse? ¿cómo se protege?

Tras conocer y evaluar los riesgos a los que se enfrenta un sistema se podrán implementar las soluciones prácticas – los mecanismos – para minimizar sus efectos.

Identificación de recursos

Deberán identificarse todos los recursos cuya integridad pueda ser amenazada de cualquier forma:

- Hardware: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, ordenadores personales, impresoras, unidades de disco, líneas de comunicación, servidores, routers…
- Software: códigos fuente y objeto, utilidades, sistemas operativos, …
- Información: En ejecución, en comunicación, BD...
- Personas: Usuarios, operadores…
- Accesorios: Papel, cintas, tóners…

Aparte del recurso en sí (algo tangible, como un router) se ha de considerar la visión intangible de cada uno de estos recursos (por ejemplo, la capacidad para seguir trabajando sin ese router). Es difícil generar estos aspectos intangibles de los recursos, ya que es algo que va a depender de cada organización, su funcionamiento, sus seguros, sus normas... No obstante, siempre se han de tener en cuenta algunos aspectos comunes: privacidad de los usuarios, imagen pública de la organización, …

Con los recursos correctamente identificados se ha de generar una lista final, que ya incluirá todo lo que se necesite proteger de una organización.

Identificación de amenazas

Una vez conocidos los recursos que se deben proteger hay que identificar las vulnerabilidades y amenazas que se ciernen contra ellos. Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Se suelen dividir las amenazas que existen sobre los sistemas informáticos en tres grandes grupos, en función del ámbito o la forma en que se pueden producir:

- Desastres del entorno: Dentro de este grupo se incluyen todos los posibles problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Por ejemplo, se han de tener en cuenta desastres naturales (terremotos, inundaciones...), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico, y peligros relacionados con operadores, programadores o usuarios del sistema.
- Amenazas en el sistema. Bajo esta denominación se contemplan todas las vulnerabilidades de los equipos y su software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, medidas de protección que éste ofrece, fallos en los programas, copias de seguridad...
- Amenazas en la red: Cada día es menos común que una máquina trabaje aislada de todas las demás; se tiende a comunicar equipos mediante redes locales, intranets o la propia Internet, y esta interconexión acarrea nuevas amenazas a la seguridad de los equipos, peligros que hasta el momento de la conexión no se suelen tener en cuenta. Por ejemplo, es necesario analizar aspectos relativos al cifrado de los datos en tránsito por la red, a proteger una red local del resto de internet, o a instalar sistemas de autenticación de usuarios remotos que necesitan acceder a ciertos recursos internos a la organización.

Algo importante a la hora de analizar las amenazas a las que se enfrenta un sistema es analizar los potenciales tipos de atacantes que pueden intentar violar nuestra seguridad. Es algo normal que a la hora de hablar de atacantes se piense en hackers. No obstante, la inmensa mayoría de problemas de seguridad vienen dados por atacantes internos a la organización afectada.

No siempre se han de contemplar las amenazas como actos intencionados contra un sistema: muchos de los problemas pueden ser ocasionados por accidentes, desde un operador que derrama una taza de café sobre una terminal hasta un usuario que tropieza con el cable de alimentación de un servidor y lo desconecta de la línea eléctrica, pasando por temas como el borrado accidental de datos o los errores de programación; decir 'no lo hice a propósito' no ayuda nada en estos casos.

Medidas de protección

Tras identificar todos los recursos que se desean proteger, así como las posibles vulnerabilidades y amenazas a que los que se está expuesto y los potenciales atacantes que pueden intentar violar la seguridad del sistema, se ha de estudiar cómo proteger dichos sistemas, sin ofrecer aún implementaciones concretas para protegerlos (esto ya no serían políticas sino mecanismos).

Esto implica en primer lugar cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades de que una amenaza se pueda convertir en realidad. Este cálculo puede realizarse partiendo de hechos sucedidos con anterioridad en la organización, aunque por desgracia en muchos lugares no se suelen registrar los incidentes acaecidos. En este caso, y también a la hora de evaluar los daños sobre recursos intangibles, existen diversas aproximaciones como el método Delphi, que básicamente consiste en preguntar a una serie de especialistas de la organización sobre el daño y las pérdidas que cierto problema puede causar; no obstante, la experiencia del administrador en materias de seguridad suele tener aquí la última palabra a la hora de evaluar los impactos de cada amenaza.

La clasificación de riesgos de cara a estudiar medidas de protección suele realizarse en base al nivel de importancia del daño causado y a la probabilidad aproximada de que ese daño se convierta en realidad; se trata principalmente de no gastar más dinero en una implementación para proteger un recurso que lo que vale dicho recurso o lo que nos costaría recuperarnos de un daño en él o de su pérdida total.

Se llama *Ri* al riesgo de perder un recurso i (es decir, a la probabilidad de que se produzca un ataque), y se le asigna un valor de 0 a 10 (valores más altos implican más probabilidad); se define también de 0 a 10 la importancia de cada recurso, *Wi*, siendo 10 la importancia más alta. La evaluación del riesgo es enton-

ces el producto de ambos valores, llamado peso o riesgo evaluado de un recurso, WRi, y medido en dinero perdido por unidad de tiempo (generalmente, por año): WRi = Ri * Wi

De esta forma se podrán utilizar hojas de trabajo en las que, para cada recurso, se muestre su nombre y el número asignado, así como los tres valores anteriores. Evidentemente, los recursos que presenten un riesgo evaluado mayor serán los que más medidas de protección deben poseer, ya que esto significa que es probable que sean atacados, y que además el ataque puede causar pérdidas importantes. Es especialmente importante un grupo de riesgos denominados inaceptables, aquellos cuyo peso supera un cierto umbral.

Una vez conocido el riesgo evaluado de cada recurso es necesario efectuar lo que se llama el análisis de costes y beneficios. Básicamente consiste en comparar el coste asociado a cada problema (calculado anteriormente, WRi) con el coste de prevenir dicho problema. El cálculo de este último no suele ser complejo si se conocen las posibles medidas de prevención disponibles: por ejemplo, para saber lo que cuesta prevenir los efectos de un incendio en la sala de operaciones, no se tiene más que consultar los precios de sistemas de extinción de fuego. No sólo se ha de tener en cuenta el coste de cierta protección, sino también lo que puede suponer su implementación y su mantenimiento.

Ha de tenerse presente que los riesgos se pueden minimizar, pero nunca eliminarlos completamente, por lo que será recomendable planificar no sólo la prevención antes de un problema sino también la recuperación si el mismo se produce; se suele hablar de medidas proactivas (aquellas que se toman para prevenir un problema) y medidas reactivas (aquellas que se toman cuando el daño se produce, para minimizar sus efectos).

Estrategias de respuesta

¿Qué hacer cuando la política de seguridad ha sido violada? La respuesta a esta pregunta depende completamente del tipo de violación que se haya producido, de su gravedad, de quién la haya provocado, de su intención... Si se trata de accidentes o de problemas poco importantes suele ser suficiente con una reprimenda verbal o una advertencia; si ha sido un hecho provocado, quizá sea conveniente emprender acciones como la clausura de las cuentas de forma temporal o pequeñas sanciones administrativas. En el caso de problemas graves que hayan sido intencionados interesará emprender acciones más duras, como

cargos legales o sanciones administrativas firmes. La política de seguridad ha de establecer el tipo de castigo para cada una de las infracciones.

Existen dos estrategias de respuesta ante un incidente de seguridad: *"Proteger y proceder"* y *"Perseguir y procesar"*. La primera de estas estrategias se suele aplicar cuando la organización es muy vulnerable o el nivel de los atacantes es elevado; la filosofía es proteger de manera inmediata la red y los sistemas y restaurar su estado normal, de forma que los usuarios puedan seguir trabajando normalmente. Seguramente será necesario interferir de forma activa las acciones del intruso para evitar más accesos, y analizar el daño causado. La principal desventaja de esta estrategia es que el atacante se da cuenta rápidamente de que ha sido descubierto, y puede emprender acciones para evitar ser identificado, lo que incluso conduce al borrado de logs o de sistemas de ficheros completos; incluso puede cambiar su estrategia de ataque a un nuevo método, y seguir comprometiendo al sistema. Sin embargo, esta estrategia también presenta una parte positiva: el bajo nivel de conocimientos de los atacantes en sistemas habituales hace que en muchas ocasiones se limiten a abandonar su ataque y dedicarse a probar suerte con otros sistemas menos protegidos en otras organizaciones. La segunda estrategia de respuesta, perseguir y procesar, adopta la filosofía de permitir al atacante proseguir sus actividades, pero de forma controlada y observada por los administradores, de la forma más discreta posible. Con esto, se intenta guardar pruebas para ser utilizadas en la segunda parte de la estrategia, la de acusación y procesamiento del atacante (ya sea ante la justicia o ante los responsables de la organización, si se trata de usuarios internos). La parte positiva de esta estrategia es, aparte de la recolección de pruebas, que permite a los responsables conocer las actividades del atacante, saber qué vulnerabilidades de la organización se han aprovechado para atacarla, cómo se comporta una vez dentro, etc. De esta forma se aprovecha el ataque para reforzar los puntos débiles del sistema de seguridad.

Una forma de monitorizar las actividades de una organización sin comprometer excesivamente su integridad es mediante un proceso denominado jailing o encarcelamiento: la idea es construir un sistema que simule el real, pero donde no se encuentren datos importantes, y que permita observar al atacante sin poner en peligro los sistemas reales. Para ello se utiliza una máquina, denominada sistema de sacrificio, que es donde el atacante realmente trabaja, y un segundo sistema, denominado de observación, conectado al anterior y que permite analizar todo lo que esa persona está llevando a cabo. De esta forma se consigue que

el atacante piense que su intrusión ha tenido éxito y continúe con ella mientras se monitorizan sus acciones.

4. Referencias

- W. Stallings: Cryptography and Network Security: Principles and Practice, Fourth Edition; Prentice Hall. 2006.

- S. Garfinkel, G. Spafford, A. Schwartz: Practical UNIX and Internet Security. O'Reilly 2003.

- J. Ramió: Aplicaciones Criptográficas. Universidad Politécnica, Escuela Universitaria de Informática, 1999.

- M. J. Lucena: Criptografía y seguridad en Computadores. Libro electrónico disponible en wwwdi.ujaen.es/~mlucena

- The Standard of good Practice for Information Security. Information Security Forum. Disponible en línea en www.isfsecuritystandard.com