



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

Índice Tema 8

1. La seguridad en redes.
2. Control de accesos.
3. Técnicas criptográficas.
4. Mecanismos de firma digital.
5. Intrusiones. Cortafuegos.





CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

TEMA 8

La seguridad en redes. Control de accesos. Técnicas criptográficas. Mecanismos de firma digital. Intrusiones. Cortafuegos.

1. LA SEGURIDAD EN REDES.

Se entiende por seguridad (o sistema de seguridad) de los sistemas de información al conjunto de funciones, servicios y mecanismos que permitan garantizar las siguientes premisas:

- Autenticación. Se define como la característica de dar y reconocer la autenticidad de ciertas informaciones del Dominio y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de esas cuestiones.
- Confidencialidad. Se define como la «condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados».
- Integridad. Se define como la «condición de seguridad que garantiza que la información es modificada, incluyendo su creación y destrucción, sólo por el personal autorizado».
- Disponibilidad. Se define como el «grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un Sistema de Información en un período de tiempo considerado aceptable». Se asocia a menudo a la fiabilidad técnica (tasa de fallos) de los componentes del sistema de información.

Además de satisfacer los anteriores requisitos, los sistemas de seguridad pueden proporcionar una serie de servicios entre los que destacan:

- Servicios de no-repudiación. Impiden que un usuario pueda negar haber recibido un documento electrónico.
- Reclamación de origen. Constituye la contrapartida del servicio anterior, en el sentido de que permite probar quién es el creador de un determinado documento.

- Reclamación de propiedad. Este servicio permite probar que un determinado documento electrónico es de propiedad de un usuario particular. Se usa en transacciones mercantiles, donde la posesión de un documento concede determinados derechos a su poseedor.
- Accesibilidad. En su sentido más general, éste es el servicio cuyo objetivo es el de permitir que ciertos datos sólo sean accesibles por personas autorizadas.
- Intercambio equitativo de valores. Este servicio es importante en todas aquellas operaciones comerciales o mercantiles en las que la cesión de un documento por una de las partes implicadas supone la recepción de otro documento a cambio, como en el intercambio de contratos y en la realización de pagos. El servicio garantiza que la transacción se realiza en los términos acordados o que, en caso contrario, la parte en desacuerdo recuperará los documentos que haya entregado.
- Certificación de fechas. En las comunicaciones electrónicas este servicio es el equivalente al certificado de fecha y/u hora a la que se ha realizado o entregado un determinado documento.

El sistema de seguridad requerido por un SI o una organización variará dependiendo de una serie de factores, entre los que pueden destacarse los siguientes:

- Localización geográfica de los usuarios.
- Topología de la red de comunicaciones.
- Instalaciones o salas donde residen los equipos físicos.
- Equipo físico que soporta el SI.
- Configuración del equipo lógico básico.
- Tipo y estructura de las bases de datos.
- Forma de almacenamiento de los datos.
- Número y complejidad de los procesos a realizar.

Las funciones, servicios y mecanismos de seguridad requieren, en general, el concurso de una serie de medidas que podríamos clasificar como:

- Medidas administrativas/organizativas de los sistemas. Publicación de normas de uso adecuado, u otros métodos apropiados. Deben definirse claramente las áreas de responsabilidad de usuarios, administradores y directivos.
- Medidas legislativas: deben preverse sanciones en aquellos en que la prevención no sea técnicamente posible o conveniente. Puede además darse el caso de que algunos aspectos de la política de seguridad tengan implicaciones legales (por ejemplo, el seguimiento de líneas).
- Medidas técnicas: son, esencialmente, la criptografía y los productos certificados.

La generalización del uso de las tecnologías de la información y de las comunicaciones es potencialmente beneficiosa para los ciudadanos, las empresas y la propia Administración Pública, pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en su utilización.

Internet es una red de redes independiente de cualquier tipo de control gubernamental, privado, local o central. Esta característica la convierte también en un entorno en el que el control de acceso y la seguridad de los recursos conectados a la red, están abiertos a determinados niveles de intrusismo.

En este sentido, la Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones públicas (MAGERIT) es un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

MAGERIT ha sido elaborada por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, SSITAD, del Consejo Superior de Informática.

Los objetivos de MAGERIT son:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.
- Como objetivo a más largo plazo, MAGERIT prepara su lógica articulación con los mecanismos de evaluación, homologación y certificación de seguridad de sistemas de información (ITSEC, Criterios Comunes de Evaluación de la Seguridad de los Productos y Sistemas de Información).

• ESTRATEGIAS DE SEGURIDAD A NIVEL DE RED.

A) Cortafuegos.

De todos los sistemas de seguridad de Internet, el más efectivo es el cortafuegos. En un sistema tradicional, todos los ordenadores de la red local tienen acceso directo a Internet y son igualmente vulnerables a todo tipo de ataques provenientes del exterior. Resulta complejo proteger un sistema abierto como éste de posibles ataques del exterior. Un ordenador no seguro puede permitir a un intruso el acceso no autorizado a la red local, pero además resulta muy difícil detectarlo. Los cortafuegos intentan paliar esto interponiendo un ordenador especialmente configurado, entre el mundo exterior (Internet) y la red local que se quiere proteger (una Intranet, por ejemplo).

Los cortafuegos son sistemas que controlan el acceso a las redes prohibiendo el tráfico directo entre la red local y el exterior y obligando a que todo el tráfico de datos pase primero por el ordenador cortafuegos donde una serie de programas determinan si se permite a los datos seguir su camino o si son rechazados.

De este modo, en vez de proteger con sistemas de seguridad cada uno de los ordenadores de la red local, el esfuerzo se centra sobre el cortafuegos. La región que se encuentra fuera del control del cortafuegos se denomina «zona no cubierta».

Los cortafuegos pueden tener distintas formas, como filtrador de paquetes, cortafuegos a nivel de circuitos y a nivel de aplicación.

– Filtrador de Paquetes.

Pueden filtrar paquetes de información y así discriminar el tráfico en base a unas reglas definidas. Es decir, dejan pasar a su través paquetes y pueden filtrar el tráfico en función de direcciones IP, tanto fuente como destino, protocolos y números de puertos TCP, en cuyo caso se podrán filtrar los servicios a los que se les permite el paso. El filtrador de paquetes puede ser bien un Router o bien un ordenador con dos tarjetas de red, una conectada a la red interna y la otra a la red externa.

– Cortafuegos a nivel de aplicación.

Estos cortafuegos están conectados a la red interna y a la red externa, no permiten el paso de paquetes IP a su través, permiten el tratamiento de los servicios por separado sin necesidad de manipular complicadas listas de acceso y centralizan en un solo punto la gestión de los servicios, de cara a la red externa y también de cara a la red interna.

– Cortafuegos a nivel de circuitos.

Habitualmente se trata de un ordenador con dos interfaces de red operando a modo de pasarela que realiza tareas de filtrado de paquetes y además puede incorporar funcionalidades adicionales como el control de acceso mediante palabras de paso. Por un lado reciben las peticiones de conexión a un determinado puerto TCP y por otro establecen la conexión con el destinatario deseado si se han superado las comprobaciones.

A cambio de una mayor seguridad, el cortafuegos trae consigo también una mayor incomodidad ya que los ordenadores de la red local no tienen acceso directo a Internet, a menos que se tomen medidas especiales en el cortafuegos.

B) Servidores Proxy.

La función de un servidor Proxy es actuar de pasarela (gateway) entre los ordenadores de una red local e Internet. Normalmente se usan para llevar las peticiones del cliente a través de un cortafuegos. El Proxy espera a una petición desde dentro del cortafuegos y la expide al servidor remoto en el exterior del cortafuegos, lee la respuesta y la envía de vuelta al cliente.

En la práctica todos los clientes en una subred salen a través del mismo Proxy. Es por ello que también sirven para prestar servicios como caché de documentos que son pedidos por muchos clientes. De esta forma se reduce el coste de tráfico de red, ya que a menudo gran cantidad de documentos son recuperados desde el caché local una vez que la petición inicial ha sido hecha.

Las llamadas entrantes generalmente no son permitidas por el Proxy a través del cortafuegos. Esto hace que para los usuarios de la red interna el cortafuegos se comporte como un espejo unidireccional: pueden ver hacia fuera, pero el resto del mundo no les puede ver a ellos.

Una función que realiza el Proxy en una red interna es la de crear direcciones IP dinámicas para los equipos de la red que deseen realizar una conexión con Internet. Esto se usa cuando no se tienen suficientes direcciones IP reales contratadas para todos los equipos de la red. En ese caso (cuando los

equipos de una red interna no tienen todos una dirección IP fija asignada) lo que hace el Proxy es, cuando un ordenador demanda información a Internet, realmente lo que hace es pedírsela al Proxy; éste le asigna al ordenador de forma temporal (mientras dure la conexión) una IP que esté libre en ese momento (IP dinámica) y se realiza la conexión a Internet como si el equipo dispusiera de su propia IP real. Una vez concluida la conexión, la dirección IP asignada queda libre para ser asignada de nuevo a cualquier equipo que desee realizar una conexión a Internet.

• ESTRATEGIAS DE SEGURIDAD A NIVEL DE APLICACIÓN. CRIPTOGRAFÍA.

La criptografía es el proceso por el cual unos mecanismos lógicos o físicos hacen ininteligible un documento digital para garantizar la confidencialidad de información sensible que pudiera contener el documento y que pudiera ser vulnerable a acceso no autorizado en comunicaciones o soportes de almacenamiento.

Los distintos métodos de criptografía que existen tienen las siguientes características:

- Proporcionan comunicaciones seguras a través de canales que no lo son.
- Permiten que la comunicación privada entre dos entidades no pueda ser interceptada por una tercera persona que pueda estar a la escucha.
- Garantiza la protección de información si el sistema se ve comprometido, ya que puede borrarse la información, pero no alterarse su contenido.
- Protege los datos que se encuentren en un soporte que pueda ser robado.

La criptografía trabaja acumulando información de forma no visible, utilizando un algoritmo para cifrar la información y utilizando claves para descifrarla.

Los navegadores de WWW más extendidos del mercado utilizan métodos de cifrado para sus comunicaciones a través de Internet.

A) Transacciones seguras.

Existen dos protocolos que se han creado para seguridad en transacciones en la WWW. Éstos son:

- SSL (Secure Socket Layer): éste es un protocolo que define la comunicación segura entre aplicaciones cliente y servidor. Utiliza algoritmos de encriptación basados en DES y RSA con claves de 40 ó 128 bits. Este protocolo está presente en navegadores de WWW.
- S-HTTP (Secure HTTP): éste es un conjunto de protocolos basados en HTTP, con los que se pretende conseguir confidencialidad, integridad y autenticación en transacciones HTTP.

Además de estos dos protocolos existe una solución que se ha desarrollado expresamente para transacciones financieras. Se trata del protocolo SET (Secure Electronic Transactions) y consiste en una especificación basada en cifrado de tipo RSA, desarrollado conjuntamente por dos compañías de tarjetas de crédito, para la realización de transacciones electrónicas seguras a través de la WWW.

Existen organizaciones que trabajan continuamente en mejorar el protocolo HTTP para aumentar la seguridad de las transacciones a través de la Web.

B) Seguridad en Correo Electrónico.

En el ámbito del correo electrónico donde se han impuesto los protocolos SMTP para el transporte y POP3/IMAP4 para la entrega, la seguridad y autenticación la proporcionan los protocolos PGP y S/MIME.

S/MIME es un protocolo que proporciona seguridad en el intercambio de mensajes por correo electrónico. Fue desarrollado por varias empresas de software que se unieron para crear esta especificación y su objetivo era que fuera fácilmente integrable en las aplicaciones de correo electrónico y que proporcionara de una forma sencilla protección a los mensajes para evitar su interceptación por extraños.

PGP es una técnica de cifrado de mensajes que se basa en un algoritmo de clave pública, el cual usa dos claves: una clave es la clave pública que se disemina entre todos aquellos usuarios de los que se quiere recibir mensajes, y una clave privada, que se usa para descifrar los mensajes recibidos. El programa de cifrado PGP es gratuito y se puede obtener de distintos servidores de Internet.

2. CONTROL DE ACCESOS.

El control de acceso es un servicio de seguridad que asegura que cada persona o entidad sólo pueda tener acceso a la información que está autorizado. Puede ser discrecional, por necesidad de conocer, o por mandato, por disponer del nivel de habilitación acreditado. Como mecanismo de seguridad que presta dicho servicio incluye diversos procedimientos que lo aseguran (listas de personal, a qué está autorizado, contraseñas, tiempo de intento de acceso, ruta de intento de acceso, duración del acceso).

El control de acceso implica resolver las cuestiones ligadas a la identificación y a la autenticación: la identidad de los actores, la aprobación del uso de cada sistema y conocimiento de los usuarios, asegurando que cada identificador de usuario es único y sólo puede ser asociado a una persona; la autenticidad de los activos del dominio de tipo información y de los actores de tal forma que se asegure que un usuario es quien dice ser cuando accede al sistema y la autorización por parte de los autorizadores. La autenticación del usuario habitualmente se basa en algo que el usuario tiene (tarjeta, llaves), algo que el usuario sabe (una palabra de paso), algo que el usuario es (constantes biométricas).

Para implementar el control de acceso se dispone de los siguientes dispositivos o mecanismos técnicos: contraseñas o palabras de paso, constantes biométricas, sistemas de retrollamada o callback, cifrado, tarjetas y cortafuegos. Estos dispositivos o mecanismos permiten la identificación sobre la persona o sistema remoto, la autorización, determinando la autoridad de la persona o sistema remoto para ejecutar cada tipo de acción posible, la protección contra el robo de claves o la suplantación de personalidad, la protección contra la modificación de datos, de la copia, etc., calificar un recurso o una unidad de datos con sus atributos de seguridad, así un sistema típico de esta naturaleza tiene una clasificación jerárquica (libre, restringida, protegida, confidencial), la utilización de características biométricas tales como el reconocimiento de la voz, retina ocular, huellas digitales, etc.

Nos vamos a centrar en los aspectos más técnicos del control de acceso, no obstante hay un conjunto de aspectos organizativos ligados al control de acceso a los que se deberá prestar atención: ges-

ción del acceso de usuarios. Gestión de identificadores de usuario. Registro de usuarios y comprobación de acceso. Gestión de privilegios. Revisión de los derechos de acceso de los usuarios. Responsabilidades del usuario en el acceso, Sistema de gestión de contraseñas. Equipamiento desatendido asignado al usuario. Conservación de la información en los puestos de trabajo. Control de Accesos frente a terceras partes.

• CONTRASEÑAS O PALABRAS DE PASO.

La contraseña o palabra de paso de cada usuario es la base de validación de cada operación de acceso que proporciona el propio usuario a los servicios del Sistema de Información. La contraseña es un mecanismo de salvaguarda que asegura la autenticación del usuario y permite que la máquina compruebe o valide las autorizaciones de acceso a los servicios informáticos que proporciona.

Algunas aplicaciones requieren que las contraseñas sean asignadas por una autoridad independiente. Pero en la mayoría de los casos, son los propios usuarios quienes seleccionan y mantienen sus contraseñas. Debe establecerse un procedimiento seguro para controlar el establecimiento y cambio de estas claves de acceso, exigiendo a los usuarios:

- El compromiso con su firma de mantener el secreto de sus claves personales y de las que compartan con otros miembros de un grupo.
- El acuse de recepción de la clave de acceso temporal enviada por conducto seguro, no mediante terceros ni por correo (electrónico) no cifrado.

Los sistemas de gestión de contraseñas deberían controlar la calidad de las mismas. Un buen sistema de gestión de contraseñas debería tener las siguientes características:

- Siempre que sea posible, el sistema forzará el uso de contraseñas individuales a efectos de la contabilización y seguimiento de los accesos.
- Si procede, el sistema permitirá a los usuarios que seleccionen sus contraseñas. Pero les obligará a usar contraseñas de longitud mínima (seis a ocho caracteres), promoverá un proceso de confirmación de las contraseñas para evitar errores al teclearlas. Se evitarán contraseñas deducibles de fechas o series regulares (planetas, días de la semana, meses), nombres de la familia, direcciones, teléfonos, matriculas de coche, nombres de la organización, productos comerciales y similares, identificador de usuario, de grupo u otros identificadores de sistema, números o letras únicamente, o repetición de caracteres seguidos.
- Si los usuarios pueden cambiar sus contraseñas, el sistema les forzará a cambiarlas a intervalos regulares. El sistema obligará a cambiar las contraseñas temporales (dadas por la Administración de Seguridad) en la primera conexión válida que realicen (la clave de acceso inicial dada por la Administración también será temporal, permitirá sólo la primera conexión al sistema y requerirá su cambio inmediatamente después) o si el usuario olvida la suya.
- El sistema exigirá cambiar las contraseñas de usuarios privilegiados con mayor frecuencia que a los demás usuarios.
- El sistema mantendrá registro de las últimas contraseñas (por ejemplo, de las usadas durante los últimos doce meses) para impedir que los usuarios las vuelvan a utilizar.

- El sistema evitará mostrar las contraseñas en la pantalla cuando se estén tecleando.
- El sistema almacenará mediante algoritmos de cifrado las contraseñas en archivos distintos de los que contienen datos.
- Se debe mantener la confidencialidad de la contraseña (por ejemplo no escribirla en un papel si no existe forma segura de guardarlo), cambiar la contraseña si se tiene algún indicio o posibilidad de que su confidencialidad pueda verse comprometida.
- No se debe incluir la contraseña en ningún procedimiento automático de conexión o que requiera un cambio de identificador de usuario (por ejemplo en «scripts» o «guiones» macros, teclas de función, etc.).

En el caso de usuarios que necesiten acceso a múltiples plataformas y tengan que mantener varias contraseñas, se permitirá establecer una misma contraseña para todos los servicios siempre que se pueda garantizar el almacenamiento de todas con condiciones mínimas de seguridad (el nivel de protección recomendado para almacenar las contraseñas de usuarios implica usar al menos algoritmos de cifrado unidireccionales).

• CONSTANTES BIOMÉTRICAS.

Los sistemas de identificación y autenticación basados en constantes biométricas se basan en atributos físicos únicos del individuo. Se pueden clasificar de la siguiente forma:

- Fisiológicas: reconocimiento facial, huellas dactilares, geometría de la palma de la mano, patrón de vasos sanguíneos de la retina, DNA.
- De conducta: ritmo de pulsaciones del teclado, reconocimiento de la voz, análisis de la firma manuscrita, olor.

Una desventaja, por el momento, de los sistemas basados en el reconocimiento de constantes biométricas es el tiempo de respuesta, sobre todo en el caso de que la base de datos de usuarios sea grande. Algunos sistemas para reducir este tiempo de respuesta combinan el reconocimiento de constantes biométricas con la introducción de palabras de paso. De esta manera el sistema sólo compara el patrón capturado con el almacenado en la base de datos.

No obstante, los sistemas de identificación y autenticación basados en constantes biométricas son reconocidos como sistemas de futuro para aplicaciones en multitud de áreas desde los servicios públicos a los servicios bancarios y financieros pasando por la telefonía, el control de acceso físico, etc.

• SISTEMAS DE RETROLLAMADA O «CALLBACK».

Los sistemas de retrollamada son una forma común de controlar el acceso remoto vía redes conmutadas utilizando modems. En un sistema de este tipo el modem receptor solicita la identificación del modem que llama, desconecta la llamada, comprueba la identidad de quien llama en un directorio y llama al modem autorizado según el número que casa con la identificación del llamante. De esta forma se asegura que la comunicación sólo tiene lugar entre dispositivos autorizados.

- **CIFRADO.**

Como se ve en el apartado de técnicas criptográficas o en el de tarjetas, el cifrado es un componente importante en la implementación de mecanismos de control de acceso.

- **TARJETAS.**

La identificación y autenticación personal ante el sistema que se va a utilizar exige dar respuestas a cuestiones del tipo ¿cómo se identifica a sí misma la persona que va a utilizar el sistema?, ¿puede memorizar el usuario claves de una cierta longitud, complejos algoritmos o incluso varias páginas de texto sin errores? La respuesta parece ser negativa. Es necesaria la ayuda de algún dispositivo, terminal u ordenador que realice la función de agente de seguridad en las relaciones con otros sistemas. Entre el agente de seguridad y el sistema remoto se pueden establecer procedimientos de autenticación sistema a sistema, sin embargo permanece el problema de la identificación personal del usuario.

La solución tradicional a los problemas de identificación personal se ha orientado a asegurar el sistema tanto desde el punto de vista físico como del lógico, por ejemplo, colocando el agente de seguridad en una habitación cerrada, de forma que sólo pueda tener acceso la persona que tenga la llave de la cerradura. Una vez conseguido el acceso a esta habitación el usuario debe proporcionar su identidad y su palabra de paso al agente de seguridad o en su caso, a un terminal para autenticación ante un host. En caso de que el agente sea un simple terminal no proporciona mayor seguridad que su localización en una habitación cerrada en una dirección de red fija que permite una función de callback.

La autenticación del usuario se realiza directamente ante el host, con el riesgo, por ejemplo, de que se envíe la palabra de paso como texto claro. Un agente de seguridad más adecuado debe disponer de capacidad de proceso de tal forma que su papel sea autenticar al usuario inicialmente y asegurar con posterioridad, en cualquier momento, la identidad del usuario hasta que la sesión concluye y actuar en nombre del usuario para asegurar los intercambios o transacciones con sistemas remotos y que el usuario sea consciente de todas las acciones que se realizan en su nombre.

La autenticación del usuario se puede basar en algo que tiene (una llave) y que se aplica directamente al agente de seguridad, en lugar de a una puerta. Esta llave puede consistir, por ejemplo, en una tarjeta con una banda magnética. Además, la tarjeta puede almacenar no sólo la clave para acceder al agente de seguridad sino también las claves utilizadas para acceder a sistemas remotos en nombre del usuario. Este enfoque permite la movilidad del usuario, puesto que las claves son portátiles (en la tarjeta con banda magnética) y no se encuentran fijas en un determinado sistema. Así, el papel del agente de seguridad se orienta a ejecutar algoritmos y procedimientos pero no almacenar datos secretos tales como claves.

- **TARJETAS DE BANDA MAGNÉTICA.**

La capacidad de almacenamiento de una tarjeta de banda magnética se basa en la capacidad de la propia banda adherida a la tarjeta. Según la norma ISO 7811 que especifica posición, tamaño y características de la banda magnética, esta banda se divide en tres pistas. Las dos primeras pistas almacenan información que sólo puede ser leída, a saber, 79 caracteres numéricos de 7 bits la primera y 40 caracteres numéricos de 5 bits la segunda. La tercera banda es la que se usa para las transacciones y tiene una capacidad de 107 caracteres numéricos de 5 bits que se vuelven a escribir cada vez que la tarjeta es utilizada.

Un sistema típico de control de acceso puede estar basado en un usuario que dispone de una tarjeta con banda magnética que almacena las claves cifradas, un número de identificación personal (PIN) y un teclado que permite la introducción del PIN en el sistema. La tarjeta contiene, por ejemplo, los siguientes datos en modo sólo lectura:

- Identidad del propietario de la tarjeta (ID), cifrada con una clave secreta compartida por todos los agentes autorizados, de forma que puedan descifrar de nuevo ID.
- Una versión hashed del PIN, de la palabra de paso (PW) y de la identidad H (ID, PIN, PW). El hashing es irreversible y en consecuencia el PIN y la palabra de paso no pueden ser recuperados.
- Las claves del usuario cifradas que utilizará el agente de seguridad para comunicaciones remotas.

El procedimiento de utilización puede ser tal como sigue:

- El usuario coloca la tarjeta en el lector e introduce su PIN y su palabra de paso. Disponer a la vez de un PIN y de una palabra de paso proporciona una cierta flexibilidad, así, por ejemplo, el PIN puede ser estrictamente secreto y personal mientras que la palabra de paso puede ser un secreto compartido por un conjunto de usuarios autorizados.
- El agente (terminal, PC) lee la tarjeta y descifra la identidad del usuario.
- El agente calcula el hash en base a las tres entradas de las que dispone (ID, PIN, PIN) y lo compara con el valor almacenado en la tarjeta.
- Si las dos versiones coinciden, el agente concluye que el PIN y la palabra de paso introducidas por el usuario son compatibles con la información almacenada en la tarjeta, es decir que el usuario y el propietario de la tarjeta son una y la misma persona y que el usuario/propietario de la tarjeta está autorizado para acceder al sistema, puesto que la identidad descifrada es también compatible.
- El agente lee, descifra y utiliza las claves en nombre del usuario.

Según este procedimiento el agente no dispone de una lista de usuarios autorizados ni de palabras de paso. Simplemente comprueba que el propietario de la tarjeta y el usuario son la misma persona y confía en el descifrado con éxito de la identidad para comprobar su autorización. Este procedimiento se puede alterar fácilmente para que el valor hash H (ID, PIN, PW) se almacene en el agente y no en la tarjeta. El PIN introducido por el usuario se usaría como un índice para acceder a una tabla. Pueden existir otras variantes con el objetivo de asegurar, que el usuario y el propietario de la tarjeta son una y la misma persona, que el usuario propietario está autorizado para utilizar el agente, que si la tarjeta es robada, que no pueda revelar ni la identidad del propietario, ni sus claves (que están cifradas), ni su palabra de paso, ni su PIN (que no se encuentra en la tarjeta, salvo en forma hashed).

Las tarjetas de sólo lectura utilizadas para identificación habitualmente contienen otras informaciones además de las claves cifradas y del PIN en modo hashed. Así, pueden almacenar, por ejemplo, la fecha de expiración de la tarjeta. Si la unidad lectora comprueba que la fecha ha expirado, simplemente rechaza la tarjeta. También se pueden almacenar horas y días de validez.

• TARJETAS INTELIGENTES O TARJETAS CHIP.

Las posibilidades de la tarjeta se pueden ampliar mediante la capacidad de escritura. Esto generalmente implica que la tarjeta incorpora un microprocesador con memoria y una interfaz serie para interactuar con el dispositivo de lectura y escritura de la tarjeta. El protocolo de interfaz puede incorporar el cifrado de toda la información en tránsito entre la tarjeta y el dispositivo. La norma ISO 7816 describe este tipo de tarjetas. Una tarjeta inteligente puede realizar funciones completas de seguridad. Si estas funciones se realizan dentro de la tarjeta las claves no necesitan abandonarla nunca. En un caso extremo la tarjeta podría desempeñar el papel de un agente, ya que de hecho son pequeños microcomputadores a los que sólo les falta la fuente de alimentación, el teclado y el monitor. Se pueden caracterizar de la siguiente forma:

- Tarjetas con memoria de acceso libre: poseen un circuito con memoria que no se encuentra protegido por ninguna unidad de control de acceso. Generalmente se comunican en modo síncrono con un dispositivo externo para operaciones de lectura/escritura.
- Tarjetas de memoria protegida: son de tipo síncrono y tienen un cierto control de acceso. En las tarjetas con memoria EPROM dividida en zonas después de escribir la información restringida se quema un pequeño fusible que impide el acceso en modo escritura a esa zona. Las tarjetas con lógica de acceso poseen un dispositivo que compara un código introducido con el grabado en la tarjeta para poder leer o escribir. Existen tarjetas combinadas en las que se almacena el código en una zona protegida mediante un circuito de fusible.
- Tarjetas con microprocesador: el microprocesador dispone de un sistema operativo con un juego de instrucciones grabado en memoria ROM y permite la gestión de memoria del mismo de forma similar a un disco de ordenador pudiéndose crear ficheros y directorios.

La comunicación con el exterior se realiza de forma asíncrona. El microprocesador es capaz de bloquear la tarjeta y la memoria en situaciones dudosas. Las tarjetas criptográficas son un tipo particular de las tarjetas con microprocesador que incorpora un coprocesador matemático optimizado para aritmética modular que permite realizar algoritmos complejos de cifrado con clave asimétrica.

La tarjeta inteligente habitualmente sirve como un medio combinado de identificación, procesador de seguridad y almacenamiento seguro de claves personales. Se utiliza con un sistema que dispone de una unidad lectora, que da soporte a aplicaciones y a gestión de ficheros y que proporciona la manera de controlar la tarjeta vía teclado y pantalla. Entre las funciones se encuentran, por ejemplo, las siguientes:

- Identificación segura del usuario. Implica dos pasos: la comprobación por la propia tarjeta de que el usuario y el propietario de la tarjeta son una y la misma persona, comprobación por el agente de que el usuario/propietario está autorizado para utilizarla. En el primer paso el usuario introduce su identificador y su PIN, preferentemente en el teclado de la unidad lectora. Dentro de la propia tarjeta se compara el valor hash del ID y del PIN con el valor almacenado en la misma. Si el resultado es positivo se procede con el segundo paso. A continuación el usuario introduce su palabra de paso por medio del teclado del agente. El agente realiza un hash sobre la palabra de paso y sobre el ID (leído cifrado de la tarjeta) utiliza el resultado como un índice a una tabla de usuarios autorizados. Esta tabla contiene entre otras informaciones un número específico de usuario N que se compara con el valor almacenado en la tarjeta. Sólo si ambos pasos tienen resultado positivo el usuario es reconocido como genuino y autorizado.

- El acceso seguro sistema a sistema en nombre del usuario se realiza en base a las claves almacenadas en la tarjeta.
- Cifrado y descifrado de información por la tarjeta. El agente le proporciona los datos junto con los parámetros que indican las claves a utilizar.
- Generación y autenticación de MACs (controles de integridad basados en criptografía o Message Authentication Checks) y/o firmas digitales por la tarjeta. El agente proporciona los datos junto con los parámetros que indican las claves a utilizar.

Un ejemplo típico es el de una tarjeta previamente adquirida por el usuario que viene precargada con una cantidad límite. Cada vez que se utiliza la tarjeta esta cantidad va disminuyendo hasta que finalmente alcanza el valor cero en cuyo momento debe ser bien recargada o bien desechada.

• TARJETAS ÓPTICAS.

Utilizan una tecnología similar a la de los CDs de audio y funcionan en modo Write Once Read Many. Para escribir se utiliza un diodo láser con potencia suficiente para crear un hueco de unas micras en la superficie. Un bit se representa por la existencia o ausencia de un hueco en la superficie. La lectura de la información se realiza mediante un diodo de baja potencia. Con esta técnica se consiguen capacidades de almacenamiento de hasta 6Mb, que debido a los códigos de corrección de error, se ven reducidas en un 30 por 100. Su alta capacidad de almacenamiento las hace idóneas para aplicaciones que manejen gran cantidad de datos.

• CORTAFUEGOS.

Un cortafuegos es un sistema, compuesto generalmente de elementos físicos y lógicos que se utiliza para controlar y limitar el flujo de información y de servicios de aplicación entre dos o más redes contribuyendo fundamentalmente a la prestación del servicio de control de acceso. Adicionalmente y dependiendo de soluciones particulares, pueden prestar servicios de trazabilidad del flujo de comunicaciones, así como servicios de confidencialidad, si bien, en este último caso, habitualmente en un escenario de enlaces entre cortafuegos predeterminados. Adquieren un especial protagonismo en la protección de redes internas corporativas frente a intrusos procedentes de redes externas, como puede ser el caso de Internet. Se pueden caracterizar de la siguiente manera:

- Filtrador de paquetes. Pueden filtrar paquetes de información y así discriminar el tráfico en base a unas reglas definidas y en base a datos manipulados a nivel de capa de red del modelo OSI. El filtrador de paquetes puede ser bien un router o bien un ordenador con dos tarjetas de red, una conectada a la red Internet, la otra a la red externa. Es importante que el cortafuegos basado en router pueda soportar diversos protocolos, así como filtrar las respectivas direcciones y los números de los puertos que se corresponden con diversas aplicaciones. Por ejemplo, dejan pasar a su través paquetes y pueden filtrar el tráfico en función de direcciones IP, tanto fuente como destino, protocolos y números de puertos TCP o UDP, en cuyo caso se podrán filtrar los servicios a los que se les permite el paso. La mayor parte de los cortafuegos basados en router soportan de cientos a miles de filtros, pero hay que tener en cuenta que cada filtro supone la realización de una serie de comparaciones, de tal forma que en la medida que aumente el número de filtros disminuirá el rendimiento del cortafuegos, pudiendo llegar a convertirse en un cuello de botella de la red.

3. TÉCNICAS CRIPTOGRÁFICAS.

Cifrar es transformar una información (texto claro) en otra ininteligible (texto cifrado) según un procedimiento y usando una clave determinados, para que sólo quién conozca dicho procedimiento y clave pueda acceder a la información original. La operación inversa, descifrar, es transformar un texto cifrado en el claro equivalente conociendo el procedimiento y clave de descifrado.

Sea un mensaje en texto claro P entendido como una secuencia de caracteres $P = (P_1, P_2, \dots, P_n)$, de forma similar el texto cifrado se puede expresar como $C = (C_1, C_2, \dots, C_n)$. Formalmente las transformaciones entre el texto claro y el texto cifrado se denotan como $C = E(P)$ y $P = D(C)$, donde C es el texto cifrado, E es el algoritmo de cifrado, P es el texto claro y D es el algoritmo de descifrado. Obviamente se desea un criptosistema tal que $P = D[E(P)]$. Algunos algoritmos de cifrado utilizan una clave K , de tal forma que el mensaje cifrado depende tanto del texto claro original como del valor de la clave, denotándose $C = E(K, P)$. A veces se utiliza la misma clave para cifrado y descifrado, de manera que $P = D[K, E(K, P)]$. Otras veces las claves vienen en pares y se utiliza una de ellas para cifrar y la otra para descifrar. En estos casos la clave de descifrado KD deshace el cifrado de la clave KE , de tal forma que $P = D[KD, E(KE, P)]$.

Básicamente se distinguen dos sistemas de cifrado: simétrico y asimétrico.

- Un criptosistema de clave secreta o cifra simétrica es aquel en el que las claves para cifrar son iguales a las de descifrar. La seguridad del proceso depende del secreto de la clave, no del secreto del algoritmo.
- Un criptosistema de cifra de clave pública o cifra asimétrica es aquel en que las claves para cifrar son distintas a las de descifrar, en el que parte de las claves son conocidas (clave pública de cada usuario) y otra parte permanece en secreto (clave privada de cada usuario).

Se caracterizan por utilizar la misma clave en las transformaciones de cifrado y descifrado.

- El emisor utiliza una clave para cifrar el mensaje.
- El receptor utiliza la misma clave para descifrarlo.

La seguridad del sistema depende de que nadie más conozca la clave. Es necesario por tanto enviar en algún momento la clave al receptor y se corre el peligro de que pueda ser interceptada. La clave debe ser secreta para cualquier otro individuo o entidad distintos del emisor y el receptor.

La criptografía simétrica es mejor para el cifrado de grandes cantidades de información, pues es más rápida. Sin embargo, la clave secreta K se tiene que poner previamente en conocimiento de las dos partes mediante la utilización de un canal seguro, es decir, es necesario que sea distribuida con antelación a la comunicación. Por tanto, el principal problema que plantea la gestión de claves en este tipo de criptosistemas es la salvaguarda del secreto de las claves, que es especialmente delicado en dos momentos, en la generación y almacenamiento de claves y en el transporte de las mismas.

Ejemplos: Data Encryption Standard (DES). Triple DES y variantes. Fast Encryption algorithm (FEAL). International Data Encryption Algorithm (IDEA). RC4 y RC5. Secure and Fast Encryption Routine (SAFER). Skipjack. Software Optimized Encryption Algorithm (SEAL).

Criptosistemas asimétricos: el emisor y receptor tienen cada uno una pareja de claves. En cada par de claves, una de ellas es privada y se debe mantener en secreto, la otra clave es pública y se distribuye a todos los posibles destinatarios. Lo que cifra una clave privada sólo puede ser descifrado por la clave pública correspondiente y viceversa. La clave privada no puede deducirse de la pública por lo que no hay peligro en transmitir las claves públicas por la red.

- El emisor cifra con la clave pública del receptor.
- El receptor descifra con su clave privada.

La criptografía de clave pública no requiere el intercambio de secretos entre los dos comunicantes, es mejor para la gestión de claves y para implementar multitud de protocolos. Sin embargo, los algoritmos de clave pública presentan una baja velocidad de cifrado y sólo se utilizan para cifrar comunicaciones en las que la velocidad no es un requisito crítico. Estos algoritmos son útiles para la transmisión de claves simétricas por canales inseguros entre sistemas que utilicen algoritmos simétricos. Este enfoque permite simplificar la gestión de claves minimizando el número de claves que deben ser gestionadas y permitiendo su distribución a través de canales inseguros. En una red con n usuarios, si se usa cifrado de clave simétrica se precisa $n(n-1)/2$ claves, mientras que si se utiliza cifrado de clave asimétrica bastan $2n$ claves.

La clave privada se debe almacenar en un soporte protegido tal como una tarjeta inteligente. Este tipo de soporte permite una operativa en la que la clave nunca abandona la tarjeta y en la que se dificulta cualquier intento de copia de la misma. Las tarjetas inteligentes pueden estar protegidas mediante un número de identificación personal (PIN) o bien mediante un sistema de reconocimiento de huella digital.

La separación entre las claves de cifrado y de descifrado permite que los usuarios integrados en un determinado sistema de comunicación puedan publicar sus claves públicas junto con sus datos a modo de listín telefónico o directorio. Un usuario puede enviar un mensaje a otro simplemente buscando su clave pública en el directorio y utilizándola para cifrar el mensaje. Sólo el propietario de la clave privada correspondiente podrá descifrar y leer el mensaje. Un usuario puede firmar un mensaje cifrándolo con su propia clave privada. Cualquier otro usuario con acceso a la clave pública correspondiente puede verificar que se ha cifrado con la clave privada del par. Por esta razón los algoritmos asimétricos también se denominan algoritmos de clave pública.

Ejemplos: RSA, Diffie-Hellman, ElGamal.

• FUNCIÓN RESUMEN O «HASH».

Una función hash o función resumen es una función de un solo sentido que calcula a partir de una cadena de bits de longitud arbitraria otra, aparentemente aleatoria, de longitud fija. Las funciones hash se aplican a unos datos para obtener un resumen que se utiliza en la firma digital. Estas funciones transforman unos datos de longitud variable en una cadena de longitud fija de tal manera que es extremadamente difícil encontrar otros datos que den lugar a una cadena igual. Se puede considerar que el resultado de aplicar la función es una huella digital de los datos originales. El resumen o huella del texto original tiene siempre la misma longitud. Características de las funciones hash:

- Se obtiene un resultado unidireccional e irreversible.
- No hace falta una clave pues el texto cifrado depende exclusivamente del texto claro original.

- El texto cifrado normalmente es de longitud fija y mucho mas corto que cualquier mensaje típico. Se trata de una función libre de colisiones en sentido estricto. Es muy difícil encontrar un par de mensajes cuyo cifrado sea equivalente. Dada una función hash que genera cadenas fijas de 128 bits, el número posible de cadenas diferentes es 2^{128} y la probabilidad de que dos mensajes den lugar a la misma cadena es 2^{-64} .
- Cualquier alteración del mensaje original por pequeña que sea genera un mensaje cifrado completamente distinto.
- La seguridad de una función hash radica en su carácter unidireccional.

Ejemplos: MD2, MD5, SHA1, RIPE-MD

4. MECANISMOS DE FIRMA DIGITAL.

La firma digital sirve para probar la autenticidad y la integridad de los datos. Una firma digital segura consta de dos partes, en primer lugar de un método para firmar un mensaje o documento de forma no falsificable, en segundo lugar, de un método para comprobar que la firma fue generada por aquel a quien representa. Los protocolos de autenticación pueden estar basados en criptosistemas de clave pública o asimétricos puesto que estos sistemas también se pueden utilizar para autenticar al emisor. Si el emisor cifra un mensaje con su clave privada, no lo está protegiendo pues cualquiera que tenga su clave pública puede descifrarlo, pero sí que está garantizando su identidad, ya que nadie más tiene su clave privada. Este procedimiento se puede combinar con el de cifrado del mensaje para autenticarlo y protegerlo a la vez.

Así, una firma digital es una cadena de datos cifrada con una clave privada. Se puede utilizar la clave pública para verificar que la firma se generó utilizando la clave privada correspondiente. La firma se debe crear de tal manera que sea imposible generarla sin conocer la clave privada. La cadena de datos en la que se basa la firma puede incluir el nombre o pseudónimo del emisor. Además, puede llevar un sellado o estampilla de tiempo para testificar que el mensaje existía en un determinado momento. La firma digital también se puede utilizar para certificar que una determinada clave pública pertenece a una cierta persona.

El emisor aplica al mensaje una función hash que da lugar a un resumen o huella del mismo. A diferencia del proceso en el que se cifran los datos para preservar la confidencialidad, el emisor cifra el resumen del mensaje junto con otra información adicional, como lugar y tiempo, con su clave privada y no con la clave pública del receptor. Así la clave no se utiliza para cifrar el texto claro del mensaje sino para cifrar la firma digital que se anexa al mensaje.

El receptor utilizando la clave pública del emisor puede determinar si el mensaje ha sido alterado. En primer lugar, se utiliza la clave pública del emisor para descifrar la firma digital y obtener el resumen del mensaje descifrado. En segundo lugar, a partir del texto claro del mensaje recibido se obtiene el resumen aplicando la misma función hash. En tercer lugar, se comparan ambos resúmenes. El menor cambio en los datos daría lugar a dos resúmenes diferentes y sería prontamente detectado. Así, el receptor del mensaje puede estar seguro de que no ha sido alterado y de que la clave pública y privada del emisor constituyen el par correspondiente.

Para soslayar la dificultad de enviar un mensaje a un número de receptores y la baja velocidad de los algoritmos asimétricos, se usa la criptografía asimétrica y la criptografía simétrica combinadas, de tal forma que el texto claro del mensaje se cifra con una clave simétrica, denominada de sesión que se distribuye cifrada con la clave pública para cada uno de los receptores (lo que se repite es el cifrado de la clave simétrica, una cadena corta y no el cifrado del mensaje para todos los receptores).

• PROCEDIMIENTO DE LA FIRMA DIGITAL.

Cada usuario dispone de un par de claves asimétricas bien porque se le han entregado o bien porque las ha generado él mismo.

El emisor:

- Prepara el mensaje.
- Aplica al mensaje una función hash segura para obtener un resumen del mensaje de longitud fija.
- Cifra el resumen con su clave privada para obtener la firma digital.
- Adjunta la firma digital al mensaje o bien la envía por separado.
- Envía por medios electrónicos la firma y el mensaje que puede ir o no cifrado.

El receptor:

- Utiliza la clave pública del emisor para verificar la firma digital que ha recibido. Esta verificación prueba que los datos vienen de quien dice ser el emisor.
- Aplica la misma función hash segura al mensaje para obtener el resumen del mensaje o huella.
- Compara los dos resúmenes del mensaje, si ambos son Certificaciones iguales sin el bit de certificación de diferencia el receptor sabe que los datos no se han alterado.
- Obtiene un certificado de una autoridad de certificación (o del emisor del mensaje). El certificado confirma la firma digital realizada sobre el mensaje. El certificado contiene la clave pública el nombre o pseudónimo del emisor todo ello firmado certificación por la Autoridad de Certificación.

Las claves privadas no se revelan, se deben conservar en secreto. La clave simétrica de sesión se transmite una sola vez cifrada. Pero las claves públicas, por definición se encuentran a disposición de todo el mundo y su distribución no presenta ningún riesgo ya que no revela nada sobre la clave privada, sin embargo, es importante garantizar la autenticidad y propiedad de la clave pública por su legítimo propietario mediante la certificación de claves públicas.

Si «A» quiere mandar un mensaje firmado y protegido a «B». «A» firma el mensaje con su clave privada y lo cifra con la clave pública de «B». «A» sabe que sólo «B» puede descifrar ese mensaje y «B» sabe que sólo «A» ha podido mandarlo. Eso es cierto si la clave pública de «B» en posesión de «A» es la auténtica y viceversa.

Supongamos que «C» hace pública una clave que en apariencia pertenece a «A» y «B» la acepta como válida. Eso significa que «C» puede suplantar a «A» mandando a «B» mensajes aparentemente firmados por «A». Además, «C» podrá descifrar cualquier mensaje que «B» dirija a «A» cifrado con esta clave. Esto es en el fondo un problema de autenticación similar al de garantizar la identidad de los usuarios. En este caso, se trata de garantizar la identidad de las claves públicas, o más propiamente de asociar éstas a usuarios. Podemos resolver este problema usando las mismas técnicas que para autenticar usuarios, criptografía y firma digital, que aplicadas a las claves públicas y a una descripción del usuario, en vez de a los mensajes, dan lugar a los certificados de claves públicas mediante el pro-

ceso de certificación llevado a cabo por las Autoridades de Certificación. Los criptosistemas asimétricos requieren la presencia de una infraestructura sólida de certificación de claves. La certificación es un aspecto esencial de cualquier proceso de comunicaciones seguro, ya que de una buena estructura de certificación depende la validez de las claves empleadas para autenticar y cifrar las transacciones.

Una Autoridad de Certificación es una autoridad en la que confían uno o más usuarios y cuya responsabilidad principal es la certificación de la autenticidad de los usuarios. En ella confían los usuarios para la creación y firma de certificados. La Autoridad de Certificación firma digitalmente con su clave privada la información del certificado. Esta firma digital por la Autoridad de Certificación da lugar a tres elementos de confianza: primero, por definición, una firma digital de un certificado es una garantía de la integridad del certificado. Segundo, puesto que la autoridad de certificación es la única entidad con acceso a su clave privada, cualquiera que verifique la firma digital de la autoridad de certificación tiene la garantía de que sólo dicha autoridad puede haber creado y firmado el certificado en cuestión. Tercero, puesto que sólo la Autoridad de Certificación tiene acceso a su clave privada, no puede denegar que haya firmado el certificado. Por otra parte, la Autoridad de Certificación emite periódicamente listas de certificados revocados (CRLs). Un certificado puede ser revocado porque la información en el mismo ya no es válida, porque la clave privada asociada al mismo se ha perdido, o simplemente ha caducado su período de validez.

Un certificado es un documento electrónico firmado digitalmente por una Autoridad de Certificación para hacerlo infalsificable que proporciona confirmación independiente de la relación entre una clave pública de un usuario y un determinado conjunto de atributos, es decir, asocia un nombre único de una entidad con su clave pública además de con alguna otra información. Un certificado identifica a la Autoridad de Certificación que lo ha emitido, incluye algún nombre identificador o atributos del propietario de la clave pública y contiene la clave pública que se certifica. Un certificado se puede utilizar para enviar datos cifrados al propietario del certificado o bien para verificar la firma digital del citado propietario.

ESTRUCTURA DE UN CERTIFICADO SEGÚN LA ESPECIFICACIÓN DE LA NORMA ITU- X.509

PARTE	INFORMACIÓN QUE CONTIENE
Versión	Número de versión
Número de serie	Identificador único para cada certificado generado por el emisor
Firma	Identificador del algoritmo utilizado para firmar y parámetros requeridos
Emisor	Nombre de la autoridad de certificación que ha emitido el certificado
Validez	Intervalo de fechas durante las que el certificado es válido. No antes y no después
Sujeto	Nombre del sujeto para el que se emite el certificado
Información de clave pública del sujeto	Algoritmo de firma del sujeto y clave pública del mismo
Identificador único del emisor	Información adicional para identificación de autoridades de certificación
Identificador único del sujeto	Información adicional del sujeto
Extensiones	Otras informaciones opcionales
Firma del emisor	Firma digital con la clave secreta de la autoridad certificadora

La definición del nombre mediante «nombres distinguidos» X.500 facilita el uso del directorio como medio de difusión de claves, con independencia de que se puedan usar otros medios como el correo electrónico o el WWW. La recomendación X.509 de la ITU-T (antiguo CCITT) es parte de las recomendaciones X.500 que definen un servicio de directorio. El directorio está constituido por un servidor o un conjunto distribuido de servidores que mantienen una base de datos de información sobre usuarios. La información incluye una correspondencia entre nombre de usuario y dirección de red, así como otros atributos e información sobre los usuarios. X.509 define un esquema para la provisión de servicios de autenticación por medio del directorio X.500 a sus usuarios. El directorio puede servir como un repositorio de certificados de clave pública. Además X.509 define protocolos de autenticación basados en los certificados de clave pública.

El funcionamiento de la Autoridad de Certificación implica la definición de unos procedimientos para todas las tareas, es decir, debe haber unos protocolos de calificación que articulen, por ejemplo, qué formato tiene una petición de certificado, cómo se envía la respuesta, qué datos van en una lista de revocación de certificados y que aseguren la interoperabilidad con otras Autoridades de Certificación. Una de las soluciones es el conjunto de especificaciones PKCS (Public Key CryptoSystem) de RSA:

- PKCS = 1. Define mecanismos y firma digital mediante el algoritmo RSA.
- PKCS = 3. Define mecanismos de intercambio de clave mediante Diffie-Hellman.
- PKCS = 5. Como cifra mediante una clave secreta obtenida de una contraseña.
- PKCS = 6. Define el formato de los certificados.
- PKCS = 7. Define una sintaxis genérica para mensajes que incluyan mejoras criptográficas, tales como firma digital y/o cifrado.
- PKCS = 8. Define el formato de las claves privadas.
- PKCS = 9. Define diversos tipos de atributos que son usados en toda la serie.
- PKCS = 10. Define la sintaxis de una petición de certificado.
- PKCS = 11. Define una interfaz de programación independiente de la tecnología de base para utilizar objetos inteligentes como medio de autenticación.

Las Autoridades de Certificación no operan de forma aislada, sino que habitualmente pertenecen a una comunidad homogénea en cuanto a sus necesidades de certificación y en la que existen varias Autoridades de Certificación, siguiendo para su infraestructura modelos de arquitectura jerárquicos, en red o combinados. Una infraestructura de clave pública (PKI) establece una jerarquía de autoridades con diferentes tipos de responsabilidades dependiendo de sus respectivos niveles en la jerarquía:

- PAA – Policy Approving Authority. Crea y emite políticas generales para toda la infraestructura y aprueba políticas para las diferentes PCA.
- PCA – Policy, Certification Authority. Establece una política que ha de ser seguida por todas las entidades de su dominio. La PCA certifica las Autoridades de Certificación pertenecientes a ese dominio.

- CA – Certification Authority. Sigue las políticas impuestas por una PCA y su principal responsabilidad es certificar usuarios.
- ORA – Organizational Registration Authority. Su principal responsabilidad es identificar correctamente al usuario final y registrarlo en la CA.
- Usuarios.

Las políticas de certificación se refieren a temas tales como qué tipos de certificados se emiten, quiénes pueden recibir un certificado, qué prueba de identidad se considera aceptable, qué medidas de seguridad protegen los datos de los usuarios, qué procedimientos garantizan que estas normas se cumplan, cuál es la responsabilidad de la Autoridad de Certificación en caso de no ser así, etc.

5. INTRUSIONES. CORTAFUEGOS.

A) Protección de la Infraestructura.

Existen poderosas razones para proteger las redes. Por ejemplo, un intruso puede desviar el tráfico de la red hacia una máquina en el exterior con el objetivo de examinar los datos (p. ej., en busca de contraseñas). Además en el concepto infraestructuras se incluye más que las redes y los routers que las interconectan. Se incluye la gestión de red (p. ej., SNMP), los servicios (p. ej., NFS, NTP, WWW), y la seguridad (p. ej., la autenticación de los usuarios y las restricciones de acceso).

La infraestructura requiere también de protección contra los errores humanos. Cuando un administrador comete un error en la configuración de una determinada máquina, puede degradarse el servicio que ofrece esa máquina. Esto sólo afecta a los usuarios que necesitan ese ordenador, y, a menos que sea un servidor importante, el número de usuarios afectados será, por tanto, limitado. En cambio, si el error se comete en la configuración de un router, todos los usuarios que requieran de la red se verán afectados. Evidentemente, el número de usuarios es mayor que los que dependen de una sola máquina.

B) Protección de la Red.

Hay diversos problemas a los cuales son vulnerables las redes. El problema clásico es el de los «ataques de denegación de servicio». Se trata de llevar la red a un estado en el que ya no pueda procesar de modo adecuado los datos de los usuarios legítimos. Hay principalmente dos modos de hacer esto: atacando los routers y saturando la red con tráfico extraño. Nótese que el término «router» en este apartado hace referencia a un conjunto más amplio de dispositivos activos de interconexión de redes, como cortafuegos, servidores proxy, etc.

El ataque a un router se diseña con el objetivo de que éste no pueda seguir redirigiendo paquetes, o para que los redirija de modo indebido. Esto puede deberse a una configuración errónea, la inyección de información espuria sobre actualización de rutas, o un «ataque de flujo» (el router se bombardea con paquetes imposibles de encaminar, causando una degradación del rendimiento). Un ataque de flujo sobre una red es similar al ataque de flujo sobre un router, excepto que los paquetes del flujo normalmente llevan la dirección de multidifusión (broadcast) en la dirección de destino. Un ataque de flujo ideal sería el que introdujera en la red un único paquete que obligara a todos los demás nodos de la red a retransmitirlo o a generar paquetes de error, cada uno de los cuales fuera leído y retransmitido por todos los demás nodos. Un ataque de este tipo bien diseñado puede generar una explosión exponencial de transmisiones.

Otro problema clásico es el del «spoofing», o suplantación de direcciones. En este caso, se envía a uno o varios routers información trucada sobre actualización de tablas de encaminamiento. La diferencia con los ataques de denegación de servicio está en el propósito de la ruta espuria. En la denegación de servicio se pretende inutilizar el router; un estado que sería detectado de inmediato por los usuarios de la red. En el «spoofing», la ruta falsa introducida hace que los paquetes sean dirigidos a un ordenador en el que un intruso puede inspeccionar los datos de los paquetes. Luego los paquetes son reencaminados hacia sus destinos correctos. Además, el intruso ha podido alterar el contenido de los paquetes.

La solución a la mayoría de estos problemas pasa por proteger los paquetes de actualización de rutas enviados por los protocolos en encaminamiento (por ejemplo RIP-2 o OSPF). Existen tres niveles de protección: contraseñas «en claro», sumas de verificación criptográficas, y cifrado. Las contraseñas proporcionan sólo una protección mínima frente a los usuarios que no tengan acceso directo a las redes físicas.

La ventaja de las contraseñas es que la sobrecarga que producen es muy pequeña, tanto en ancho de banda como en consumo de CPU. Las sumas de verificación ofrecen protección contra la inyección de paquetes espurios, aun cuando el intruso tenga acceso directo a la red física. Combinadas con un número de secuencia, u otro tipo de identificador único, pueden proteger frente a ataques de retransmisión, en los que un paquete viejo (pero válido sólo en su momento) es retransmitido por un intruso o por un router comportándose incorrectamente. El mayor nivel de seguridad se consigue con el cifrado completo de la actualización de rutas. Esto impide que un intruso pueda determinar la topología de la red. La desventaja del cifrado es la sobrecarga que lleva consigo.

RIP-2 y OSPF contemplan las contraseñas «en claro» en su especificación básica. Además, existen extensiones a ambos protocolos para que soporten cifrado MD5. Desafortunadamente, no existe protección posible frente a los ataques de flujo. Nada puede impedir que un ordenador o u router inunden la red. Afortunadamente, este tipo de ataque se manifiesta de inmediato y normalmente puede ser abortado de modo relativamente simple.

C) Protección de los Servicios.

Hay gran variedad de servicios, y cada uno de ellos tiene sus propios requerimientos de seguridad. Estos requerimientos variarán según el uso que se pretenda hacer del servicio en cuestión. Por ejemplo, un servicio que sólo deba ser utilizado internamente (por ejemplo, NFS) puede requerir diferentes mecanismos de protección que un servicio que se ofrezca para su utilización desde el exterior. Puede ser suficiente proteger el servidor interno del acceso desde el exterior. No obstante, un servidor WWW que ofrece información en Internet para ser vista por cualquiera, requiere una protección propia. Es decir, el servicio, el protocolo y el servidor deben proporcionar las medidas de seguridad necesarias para prevenir el acceso o la modificación no autorizados a la base de datos del servidor Web.

Los servicios internos, es decir, los servicios que se pretende se utilicen sólo por los usuarios internos, y los servicios externos, aquellos que se ofrecen deliberadamente al exterior, tendrán requisitos de protección que variarán como se ha descrito anteriormente. Por tanto, es deseable aislar los servicios internos a un conjunto de máquinas y los servicios externos en otro grupo diferente. Es decir, que no coexistan servidores internos y externos en un mismo ordenador. De hecho, muchas organizaciones tienen un grupo de subredes (o incluso diferentes redes) accesibles desde el exterior, y otro grupo al que sólo se puede acceder desde el interior. Por supuesto, habitualmente existe un cortafuegos que conecta esas particiones. Debe ponerse un gran cuidado en asegurar que dicho cortafuegos funciona correctamente.

Existe un interés creciente en el uso de intranets para conectar diferentes partes de una organización (por ejemplo, divisiones de una compañía). Mientras que este documento generalmente diferencia entre externo e interno (público y privado), debe advertirse que cuando se utilicen intranets es necesario considerar tres separaciones y tomar las medidas oportunas cuando se diseñen y se ofrezcan servicios. Un servicio ofrecido en una intranet no es ni público ni tan privado como el ofrecido a una única unidad organizativa. Por tanto, dicho servicio precisará de su propio sistema de soporte, separado tanto de las redes y servicios internos como externos.

Hay un tipo de servicio externo que requiere una atención especial: el acceso anónimo (o invitado). Es el caso del FTP anónimo o el login como invitado a un determinado sistema. Es extremadamente importante que los servidores de FTP anónimo y los identificadores de los usuarios invitados sean cuidadosamente aislados de cualquier máquina o sistema de archivos de los que se deba mantener alejado a los usuarios del exterior. Otro asunto al que prestar especial atención es el relativo al derecho de escritura anónimo. Una organización puede ser responsable de la información que ponga a disposición del público en general, por lo que se recomienda una cuidadosa monitorización de la información depositada por usuarios anónimos.

A continuación consideraremos algunos de los servicios más populares: servicios de nombres, servicios de contraseñas/claves, servicios de autenticación/proxy, correo electrónico, WWW, transferencia de archivos, y NFS. Ya que éstos son los servicios más utilizados, son los puntos más obvios de ataque. Desde luego que un ataque con éxito sobre uno de estos servicios puede producir un desastre totalmente desproporcionado a la «inocencia» del servicio básico.

D) Servidores de Nombres [DNS y NIS(+)].

Internet utiliza el Sistema de Nombres de Dominio (DNS) para realizar la traducción entre nombres de máquinas y de redes y sus correspondientes direcciones. El Servicio de Información de Red (NIS y NIS+) no es utilizado globalmente en Internet, pero está sujeto a los mismos riesgos que un servidor DNS. La traducción nombre-a-dirección es crítica para el uso seguro de la red. Un atacante que pueda controlar con éxito o «despersonalizar» un servidor DNS puede reencaminar el tráfico y subvertir las protecciones. Por ejemplo, el tráfico puede ser desviado a un sistema comprometido o monitorizado; o los usuarios pueden ser engañados para que proporcionen secretos relacionados con la autenticación. Una organización debe crear sistemas bien protegidos que actúen como servidores secundarios de nombres y proteger sus servidores principales DNS de ataques de denegación de servicio, mediante la utilización de routers con capacidad de filtrado de paquetes.

Tradicionalmente, el DNS no ha tenido ninguna característica de seguridad. En particular, no se puede examinar si la información devuelta tras una interrogación ha sido modificada, ni verificar si dicha información procede del servidor de nombres en cuestión. Se está trabajando en la incorporación de firmas digitales al protocolo, lo que permitirá que la integridad de la información sea verificada utilizando técnicas criptográficas.

E) Servidores de Contraseñas/Claves [NIS (+) y KDC].

Los servidores de contraseñas y claves protegen generalmente su información vital (contraseñas y claves) mediante algoritmos de cifrado. No obstante, incluso una contraseña cifrada mediante un algoritmo de un solo sentido puede ser descubierta mediante un «ataque de diccionario», en el que se cifran palabras comunes para ver si coinciden con la palabra cifrada almacenada. Por tanto, es necesario que dichos servidores no sean accesibles desde aquellos sistemas que no los utilicen para dicho servicio, e incluso los sistemas que utilicen este servicio sólo deben ser capaces de utilizar éste. Es decir, no deben permitirse otros servicios comunes, como Telnet o FTP, salvo quizá para los administradores.

F) Servidores de Autenticación/Proxy (SOCKS, FWTK).

Un servidor proxy proporciona gran número de funciones de seguridad. Permite concentrar servicios a través de una máquina específica para permitir la monitorización, ocultar la estructura interna, etc. Esta concentración de servicios crea un objetivo atractivo para un intruso potencial. El tipo de protección requerida para un proxy depende del protocolo que se utilice y de los servicios que el proxy concentre. La regla general de limitar el acceso a aquellas máquinas que necesitan los servicios, y limitar el acceso desde esas máquinas a esos servicios exclusivamente, es un buen punto de partida.

G) Correo Electrónico.

Los sistemas de correo electrónico han sido durante mucho tiempo una gran fuente de intrusiones debido a que los protocolos de correo se encuentran entre los servicios más antiguos y más ampliamente extendidos. Además, por su naturaleza, un servidor de correo necesita que pueda accederse desde el exterior; la mayoría de los servidores de correo aceptan conexiones desde cualquier procedencia. Un servidor de correo electrónico generalmente está formado por dos partes: un agente de envío/recepción y un agente de procesamiento. Puesto que se entrega correo a todos los usuarios y es lógico que sea privado, el agente de procesamiento debe contar con los privilegios de super-usuario (root) para entregar el correo. La mayoría de las implementaciones realizan ambas partes del servicio, lo que significa que el agente de recepción también disfruta de esos privilegios. Esto plantea bastantes problemas de seguridad que no se describen en detalle en este documento. Existen algunas implementaciones que permiten una separación de ambos agentes y que son consideradas más seguras, pero siguen requiriendo una instalación muy cuidadosa para evitar crear un problema de seguridad.

H) World Wide Web (WWW).

La «Web» está creciendo en popularidad de modo exponencial debido a su facilidad de uso y su potente capacidad para concentrar servicios de información. La mayoría de los servidores WWW aceptan algún tipo de interacción por parte de las personas que acceden a sus servicios. El ejemplo más común es aceptar una solicitud del usuario remoto y pasar la información proporcionada a un programa que se ejecuta en el servidor para que procese dicha solicitud. Algunos de estos programas no están escritos pensando precisamente en la seguridad y pueden plantear problemas en este terreno. Si un servidor Web está disponible para toda la comunidad Internet, es especialmente importante que no exista en ese mismo servidor información confidencial. De hecho se recomienda que sea un servidor dedicado y que en ningún caso se declare como servidor «de confianza» en ninguna otra máquina interna.

Muchas organizaciones ubican conjuntamente su servicio FTP y su servicio WWW. Esto sólo debería ocurrir con servidores de FTP anónimo que sólo suministren información (get). Si se permite que el usuario suministre archivos (put) y existe un servidor Web en la misma máquina, puede ser bastante peligroso (por ejemplo, podría traducirse en una alteración de la información que la organización publica en el Web).

I) Transferencia de Archivos (FTP, TFTP).

Tanto FTP como TFTP permiten a los usuarios recibir y enviar ficheros electrónicos de un modo punto-a-punto. Sin embargo, FTP requiere autenticación, mientras que TFTP no. Por este motivo los servicios TFTP deben ser evitados en lo posible.

Los servidores FTP mal configurados pueden permitir a los intrusos copiar, reemplazar y borrar ficheros en cualquier área del servidor, por lo que es muy importante configurar este servicio correctamente. El acceso a las contraseñas cifradas y las informaciones sensibles, así como la introducción de caballos de Troya, son algunos de los peligros potenciales para la seguridad que pueden darse cuando el servicio no es configurado correctamente. Los servidores FTP deberían residir en una máquina dedicada. En ocasiones se opta por ubicar conjuntamente un servidor FTP con un servidor Web, ya que ambos protocolos participan de una concepción común de la seguridad. Sin embargo, se desaconseja esta práctica, especialmente cuando el servidor FTP permite el depósito de ficheros (véase la sección WWW anterior). Asimismo, si se ofrece un servicio FTP para usuarios internos y otro para el exterior, deberían residir en sistemas distintos.

TFTP no contempla las mismas funcionalidades que FTP, y no considera en absoluto la seguridad. Este servicio sólo debería considerarse para uso interno, y debería configurarse para acceder únicamente a un conjunto predeterminado de ficheros, y no a cualquier fichero del sistema con permisos de lectura. Probablemente, el uso más común de TFTP sea para cargar en un router los ficheros de configuración del mismo. En caso de utilizar TFTP, debe dedicársele una máquina, que en ningún caso sea compartida por un servicio Web o FTP accesible desde el exterior.

J) NFS.

El Sistema de Ficheros de Red permite que distintas máquinas compartan discos. Se utiliza frecuentemente por parte de estaciones de trabajo sin disco que dependen de un servidor de disco para todas sus necesidades de almacenamiento. Desafortunadamente, NFS no tiene en sí mismo ninguna función de seguridad. Es preciso que el servidor NFS sea accesible única y exclusivamente por parte de aquellas máquinas que utilicen este servicio. Esto se consigue especificando a que sistemas se exporta el sistema de archivos y de qué modo (por ejemplo, sólo-lectura, o lectura-escritura). No deben exportarse sistemas de ficheros fuera de la red local, ya que esto requeriría que el servicio NFS fuera accesible desde el exterior. Lo ideal sería que el acceso externo a un servicio NFS fuera convenientemente detenido por un cortafuegos.



