



Universidad
de Huelva

DA
iESI

TERCER CURSO. TECNOLOGÍA DE REDES

Escuela Politécnica Superior
Universidad de Huelva

Tema 5: Seguridad en Redes

Manuel Sánchez Raya
Versión 0.1
5 de Febrero de 2004

ÍNDICE

1. Introducción.....	2
1.1.- Las tres áreas de la seguridad.....	3
1.2.- Políticas de seguridad.....	4
2.- Seguridad de perímetro. Cortafuegos.....	6
2.1.- Introducción.	6
2.2.- Tipos de cortafuegos.	7
2.3.- Topologías de cortafuegos.	8
2.3.1.- Screening Router.....	8
2.3.2.- Bastion Host.	9
2.3.3.- Dual Homed Gateway.	9
2.3.4.- Screened Host Gateway.	10
2.3.5.- Screened Subnets.	10
2.3.6.- Gateways Híbridos.	11
2.4.- Aplicabilidad.	11
3.- Seguridad en el canal.	12
3.1.- Métodos básicos de criptografía.....	13
3.1.1.- Cifrado por sustitución.....	14
3.1.2.- Cifrado por transposición.....	14
3.2.- Criptografía simétrica.....	14
3.3.- Criptografía asimétrica.....	15
4.- Seguridad de Acceso.....	17
4.1.- Autenticación mediante firma digital.	17
4.2.- Autoridades certificadoras.	18
4.2.1.- Distribución de claves en el cifrado simétrico.	19
4.2.2.- Emisión de certificados en el cifrado asimétrico.	20
5.- Seguridad interna.	21
5.1.- Compartimentalización.....	21
5.2.- Monitorización.....	21
5.3.- Seguridad en servidores.	22

BIBLIOGRAFÍA

Apuntes año 2002-2003. Estefanía Cortés Ancos.
Apuntes Universidad de Oviedo. J.A.Sirgo, Rafael C. González
Academia de Networking de Cisco Systems. Guía del Primer Año.
Internetworking with TCP/IP. Vol. I. D.E. Comer.

1. Introducción.

La seguridad en los computadores implica tres exigencias que se extienden al sistema de comunicaciones cuando aquellos se integran en este:

- a) **Secreto:** Acceso a la información y recursos sólo a los entes autorizados.
- b) **Integridad:** Modificación de la información y recursos sólo por entes autorizados.
- c) **Disponibilidad:** La información y recursos deben estar disponibles para los entes autorizados.

La incorporación de un computador en una red informática u otro sistema de comunicaciones añade nuevos aspectos a la seguridad relacionados básicamente con la **identificación** de los interlocutores (denominada también **autenticación o autenticación** según el autor que se consulte). Es decir, que cada una de las dos o más partes que intervienen en una comunicación esté segura de quien o quienes son las otras partes. Algunos de estos aspectos son:

- a) **Control de Acceso:** Autorizando el acceso a través de una comunicación a la información y recursos sólo a los entes autorizados y negándolo a los demás.
- b) **Prueba de Origen:** Asegurar al receptor que un dato recibido proviene en realidad de quien dice ser su emisor.
- c) **Prueba de recepción:** Asegurar al emisor que un dato transmitido ha sido recibido realmente por quien debe ser su receptor.
- d) **No rechazo:** Pruebas más fuertes que las anteriores que impidan que un extremo niegue haber enviado un dato habiéndolo hecho o que el otro niegue haberlo recibido.

Generalmente los **ataques a la seguridad** se dividen en **pasivos** y **activos**. Los ataques pasivos son la *escucha y divulgación de la información* y el *análisis de tráfico*.

Este último no implica que se conozca el contenido de la información que fluye en una comunicación, pero el conocimiento de ese flujo, volumen, horarios o naturaleza, puede ser información útil. Los ataques activos comprenden el *enmascaramiento*, que es la suplantación de un ente autorizado para acceder a información o recursos, la *modificación* que incluye también la posible destrucción y creación no autorizada de datos o recursos, y la *interrupción*, que supone el impedir a entes autorizados su acceso a la información o recursos a los que tienen derecho de acceso.

Las contramedidas se suelen aplicar cuando se ha detectado un ataque, lo cual no suele ser una política adecuada. Los ataques pasivos son difíciles de detectar pero suelen existir contramedidas para prevenirlos. Por el contrario, los ataques activos son más fáciles de detectar pero bastante más complejos de prevenir. En resumen, las contramedidas se suelen concretar en los siguientes aspectos:

- Minimizar la probabilidad de intromisión con la implantación de elementos de protección.
- Detectar cualquier intrusión lo antes posible.

- Identificar la información objeto del ataque y su estado para recuperarla tras el ataque.

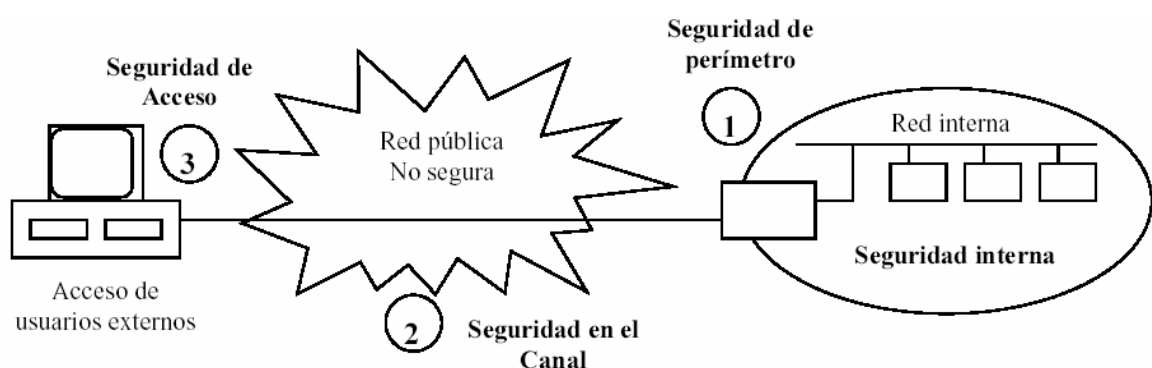
Sería prácticamente interminable el enumerar las posibles formas de ataque que puede sufrir un computador conectado a una red de comunicaciones, bien por intervención física sobre los mismos o vía software. Las **medidas de prevención** son múltiples también, desde la vigilancia física del sistema, por ejemplo, el estado de las líneas de comunicación para detectar posibles pérdidas de potencia en la señal o interferencias atribuibles a intervenciones sobre ellas, hasta el registro de los eventos que se producen en el sistema y la vigilancia de modificaciones en aquellos archivos o procesos que son críticos para la seguridad del mismo.

Todo ello involucra la responsabilidad de los usuarios y del administrador del sistema encargado de establecer las políticas de cuentas de usuario adecuadas y **mantener actualizados los dispositivos y el software** que puedan tener agujeros que comprometan la seguridad.

1.1.- Las tres áreas de la seguridad.

Actualmente, cuando las empresas disponen ya de sus propias redes internas a las que dan acceso a usuarios desde el exterior, los problemas de seguridad se plantean en tres áreas principales:

1. **La seguridad de perímetro:** protección frente ataques del exterior generalmente basada en **Cortafuegos (Firewalls)**.
2. **La seguridad en el canal:** donde hay que proteger los datos frente a escuchas mediante **criptografía**.
3. **La seguridad de acceso:** donde se contemplan tres aspectos, la **identificación** del usuario, la **autorización** del acceso y la **auditoria** de las operaciones realizadas por el usuario.



Sin embargo, se olvida a veces la **seguridad interna** ya que el problema de seguridad puede aparecer dentro de la propia empresa, en su red interna, provocado bien por empleados descontentos de la empresa, o porque la barrera del cortafuegos ha sido insuficiente y el enemigo ya está dentro. En este caso cobran importancia el uso de técnicas como la **compartimentalización** de la red mediante el uso de conmutadores (switches) y repetidores (hubs) con características de seguridad, los sistemas de **monitorización** de la red y la **seguridad en servidores**.

1.2.- Políticas de seguridad.

A la hora de implantar una política de seguridad en la empresa hay que partir de la base de que el sistema o la red 100% segura no existe. Se ha de hacer una valoración de los recursos a proteger, de tal manera que el esfuerzo y coste de la implementación del sistema de seguridad sea proporcional a su valor. Incluso se pueden definir áreas de la red interna de la empresa con información más valiosa o confidencial que deberán ser protegidas con mayor cuidado que otras.

Una técnica que empieza a implantarse en la política de seguridad es la realización de Auditorías de Seguridad. Estas pueden ser llevadas a cabo por personal de la propia empresa o por consultorías externas. Una Auditoría de Seguridad comprende entre otras las siguientes actividades:

- Evaluación de los recursos y la información a proteger.
- Evaluación de los sistemas de seguridad implementados y de aquellos que se podrían implementar.
- Prueba del estado de la seguridad de la red informática en general y de cada uno de los sistemas conectados a ella en particular, mediante la ejecución de programas o el empleo de técnicas que traten de explotar y pongan de manifiesto los posibles agujeros de seguridad. En este último aspecto existen ya aplicaciones informáticas comerciales que permiten detectar la mayoría de los agujeros de seguridad más evidentes de los sistemas operativos y aplicaciones más extendidas.
- Elaborar planes de contingencia y seguridad.

La seguridad de una red informática pasa por involucrar o concienciar a todos los usuarios y administradores de sistemas en los temas de seguridad y las implicaciones legales del uso de una red informática (una referencia a los artículos del código penal relativos se puede encontrar en www2.uniovi.es/wwwd/codigo_penal.html). La formación en estos aspectos es tan fundamental como en cualquier otra actividad de la empresa.

Algunas prácticas habituales de usuarios y administradores comprometen gravemente la seguridad como es el caso de:

- El uso de claves de acceso personales demasiado evidentes.
- La cesión de cuentas de usuarios a terceros.
- El mantenimiento de cuentas de usuario de acceso libre, a grupos o sin clave de acceso.
- La instalación de programas poco conocidos o mal mantenidos que pueden aceptar peticiones de la red.
- La ejecución de programas desconocidos que llegan por correo electrónico, a través de la red o cualquier otro medio.

Cualquier sistema, sobre todo si está conectado a cualquier tipo de red informática, debe de tener asignado un administrador. Se ha de tener especial cuidado si además el sistema es un servidor dentro de la red informática (y téngase en cuenta que cualquier

PC que comparta tan siquiera una impresora o parte de un disco con otros ya es un servidor dentro de la red). Son obligaciones del administrador del sistema las siguientes tareas:

- Instalar el S.O. y el software de aplicaciones del servidor manteniéndolos convenientemente actualizados e instalando los parches que los fabricantes elaboren para corregir los eventuales problemas que tanto de seguridad como de funcionamiento puedan surgir.
- Modificar las claves de acceso tanto del usuario administrador del sistema como de los demás usuarios, según sea necesario para mantener la seguridad del sistema.
- Administrar la seguridad del sistema mediante la instalación de programas que realicen trazas del funcionamiento del servidor o del uso que los usuarios hacen de él, o cualquier otra labor que beneficie la seguridad del sistema.
- Crear estructuras de directorios para programas y datos administrando correctamente los privilegios de acceso de cada usuario o proceso a los directorios o datos.
- Definir y borrar cuentas de usuarios.
- Designar usuarios con privilegios especiales.
- Controlar el rendimiento del sistema.
- Asegurarse de que los datos están convenientemente salvaguardados con políticas de copia de seguridad adecuadas y otros sistemas.
- Arbitrar algún tipo de mecanismo para que en caso de su ausencia temporal o permanente otra u otras personas de confianza puedan acceder a la clave de la cuenta del usuario administrador del sistema en caso de necesidad. (Guardar bajo llave la clave del sistema, dividirla en partes y repartirla entre varias personas de manera que juntándose puedan administrar el sistema, etc.)

2.- Seguridad de perímetro. Cortafuegos.

2.1.- Introducción.

Un cortafuegos es una de las varias formas de proteger una red de otra red no fiable desde el punto de vista de la seguridad. Los mecanismos reales mediante los cuales se implementan las funciones del cortafuegos son muy variados, pero en general, el cortafuegos puede verse como la unión de un mecanismo para bloquear tráfico y otro para permitirlo. Algunos cortafuegos hacen especial hincapié en el primero, mientras que otros se basan fundamentalmente en el segundo.

La razón para la instalación de cortafuegos es proteger una red privada de intrusos, pero permitiendo a su vez el acceso al exterior. En muchos casos, el propósito del cortafuegos es evitar que usuarios no autorizados accedan a los recursos de dicha red, y a menudo, evitar el acceso no autorizado a información. En este segundo caso, podría considerarse que no conectarse a Internet es suficiente. Sin embargo, en una red mal administrada cualquier empleado podría utilizar un módem para hacer una conexión a Internet mediante el protocolo SLIP o PPP y comprometer la seguridad de toda la red.

Por último, un cortafuegos puede actuar como representante de la empresa en Internet ya que muchas compañías usan sus cortafuegos para almacenar información pública sobre los servicios y/o productos que ofrece. Algunos cortafuegos sólo permiten tráfico de correo electrónico a través de ellos, y por lo tanto protegen a la red contra cualquier ataque que no sea a través del servicio de correo. Otros son menos estrictos y sólo bloquean aquellos servicios que se sabe que presentan problemas de seguridad.

En general, los cortafuegos se configuran para proteger contra comunicaciones procedentes del exterior y que no disponen de sistemas de identificación segura del usuario. Cortafuegos más sofisticados bloquean el tráfico procedente del exterior, pero permiten el uso libre de los servicios de red desde el interior. Otra característica importante es que pueden proporcionar un bastión en el que centrar los esfuerzos de administración y auditoría.

Se debe tener claro que un cortafuegos no puede proteger de ataques que no se produzcan a través del mismo. Si una compañía posee información reservada en los ordenadores de su red interna, el cortafuegos no podrá protegerla contra un ataque desde dentro. Por ello, esa parte de la red interna debería estar aislada, o bien contar con medidas extras de protección.

Un cortafuegos tampoco puede proteger contra virus, y en general, contra ataques debidos a los datos que se transfieren. Es responsabilidad final de los usuarios y de los responsables de cada máquina particular, la protección contra este tipo de riesgos. Se debe prestar especial atención a los *troyanos*, a fin de evitar ataques desde el interior. Este tipo de ataques fue bastante frecuente con versiones antiguas de Sendmail.

2.2.- Tipos de cortafuegos.

En la configuración de un cortafuegos, la principal decisión consiste en elegir entre seguridad o facilidad de uso. Este tipo de decisión es tomado en general por las direcciones de las compañías. Existen dos aproximaciones básicas:

- Todo lo que no es expresamente permitido está prohibido.
- Todo lo que no es expresamente prohibido está permitido.

En el primer caso, el cortafuegos se diseña para bloquear todo el tráfico, y los distintos servicios deben ser activados de forma individual tras el análisis del riesgo que representa su activación y la necesidad de su uso. Esta política incide directamente sobre los usuarios de las comunicaciones, que pueden ver el cortafuegos como un estorbo.

En el segundo caso, el administrador del sistema debe predecir que tipo de acciones pueden realizar los usuarios que pongan en entredicho la seguridad del sistema, y preparar defensas contra ellas. Esta estrategia penaliza al administrador frente a los usuarios. Los usuarios pueden comprometer inadvertidamente la seguridad del sistema si no conocen y cumplen unas consideraciones de seguridad mínimas. El problema se magnifica si existen usuarios que tengan cuenta en la propia máquina que hace de cortafuegos. En este tipo de estrategia hay un segundo peligro latente, y es que el administrador debe conocer todos los posibles agujeros de seguridad existentes en los protocolos y las aplicaciones que estén corriendo. El problema se agrava debido al hecho de que los fabricantes no suelen darse prisa en notificar los riesgos de seguridad que presentan sus productos.

Hay muchas formas en las que la seguridad de un cortafuegos puede verse comprometida. Aunque ninguna de estas situaciones es buena, hay algunas que son claramente más peligrosas que otras. Dado que el propósito de muchos cortafuegos es bloquear el acceso externo a una red privada, un claro fallo del sistema es la existencia de algún lazo que permita alcanzar máquinas que se encuentran dentro de la red protegida.

Una situación más peligrosa se produce si alguien es capaz de entrar en la máquina cortafuegos y reconfigurarla de modo que toda la red protegida quede accesible. Este tipo de ataque se suele denominar *destrucción* del cortafuegos. Los daños derivados de este tipo de ataque resultan muy difíciles de evaluar. Una medida importante de cómo un cortafuegos es capaz de soportar un ataque, es la información que almacena para ayudar a determinar cómo se produjo. La peor situación posible es la que resulta de la destrucción de un cortafuegos sin que queden trazas de cómo se perpetró el ataque.

Una forma de ver el efecto del fallo de un cortafuegos es en términos de la *zona de riesgo* que crea su fallo. Si una red se encuentra conectada a Internet directamente, toda la red es susceptible de ser atacada. Eso no significa que la red sea necesariamente vulnerable, sino que es necesario reforzar las medidas de seguridad en todas y cada una de las máquinas que forman la red. Esto es extremadamente difícil a medida que aumenta el número de máquinas y el tipo de servicios de red que estas ofrecen a sus usuarios.

Aplicaciones como *rlogin* representan un peligro potencial, usado habitualmente por los hackers para ir ganando acceso a diferentes máquinas y usarlas como plataformas para nuevos ataques. Un cortafuegos típico reduce la zona de riesgo a la propia máquina, o un reducido subconjunto de nodos de la red, simplificando notablemente el trabajo del administrador. Si el cortafuegos falla, la zona de riesgo puede expandirse hasta alcanzar a toda la red protegida. Si un hacker gana acceso al cortafuegos, puede utilizarlo como plataforma para lanzar ataques contra las máquinas de la red interna, sin embargo, queda la posibilidad de que el atacante deje trazas de su actividad en el propio cortafuegos, que permitan detectarlo y neutralizarlo.

Dado el riesgo que supone el fallo del cortafuegos, es una buena política de seguridad tener definidas políticas de seguridad razonables en los hosts internos para prevenir tales situaciones.

2.3.- Topologías de cortafuegos.

Aunque el propósito de todos los cortafuegos es el mismo, existen diferencias en sus topologías y prestaciones. Se pueden distinguir los siguientes tipos:

- Screening Router
- Bastion Host
- Dual Homed Gateway
- Screened Host Gateway
- Screened Subnet
- Proxy o Gateway a nivel de aplicación
- Gateway Híbrido

2.3.1.- Screening Router

Son un componente básico de la mayor parte de los cortafuegos. Pueden ser un router comercial o basado en una estación, con capacidad para filtrar paquetes. Muchos tienen la capacidad para bloquear el tráfico entre redes o nodos específicos basándose en direcciones y puertos TCP/IP. Algunos cortafuegos sólo consisten en un screening router entre la red privada e Internet.

En general permite la comunicación entre múltiples nodos de la red protegida y de Internet. La zona de riesgo es igual al número de nodos de la red protegida y el número y tipo de servicios para los que se permite el tráfico. Para cada servicio proporcionado en forma conexiones directas entre entidades homólogas, el tamaño de la zona de riesgo se incrementa rápidamente. Es difícil controlar los daños que pueden producirse dado que el administrador de la red debe examinar regularmente cada host para buscar trazas de ataques.

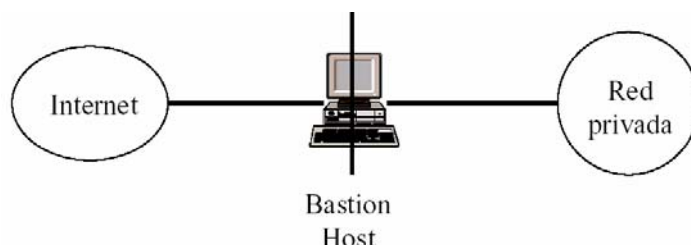
Es casi imposible reconstruir un ataque que haya llevado a la destrucción del cortafuegos, e incluso puede ser difícil detectar la propia destrucción. En general responden a configuraciones en las que lo que no está expresamente prohibido, está permitido. No son la solución más segura, pero son muy populares dado que permiten un acceso a Internet bastante libre desde cualquier punto de la red privada.

2.3.2.- Bastion Host.

Son sistemas identificados por el administrador de la red como puntos clave en la seguridad de la red. En general, tienen un cierto grado de atención extra por parte del administrador en cuanto a su seguridad. Son auditados regularmente y pueden tener software modificado para trazar las comunicaciones y reparar fallos de seguridad del sistema.

2.3.3.- Dual Homed Gateway.

Algunos cortafuegos son implementados sin necesidad de un screening router. Para ello se conecta un bastion host a la red que se quiere proteger y a Internet, desactivando las funciones de reenvío TCP/IP. Los hosts de la red privada pueden comunicarse con el gateway, al igual que los nodos de Internet, pero el tráfico directo entre ambos tipos de nodos está bloqueado.



Esta estructura de cortafuegos es empleada habitualmente debido a que es fácil de implementar. Al no reenviar el tráfico TCP/IP, bloquea completamente la comunicación entre ambas redes. Su facilidad de uso depende de la forma en la que el administrador proporciona el acceso a los usuarios:

- Proporcionando pasarelas para las aplicaciones.
- Proporcionando cuentas a los usuarios en el bastion host.

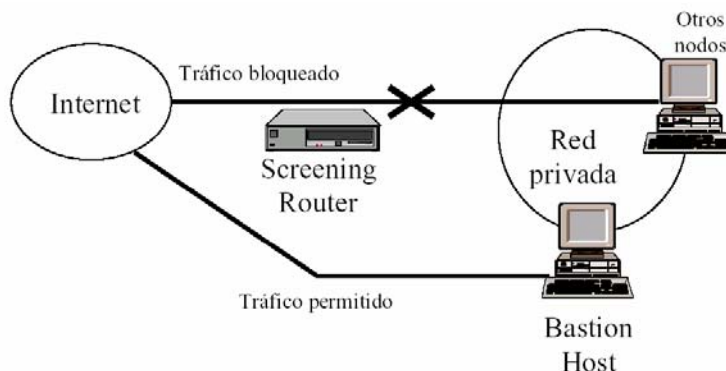
En el primer caso se está en una situación en la que lo que no está explícitamente permitido, está prohibido. En el segundo caso, el acceso de los usuarios a Internet es más sencillo, pero la seguridad puede verse comprometida. Si un hacker gana acceso a una cuenta de usuario, tendrá acceso a toda la red protegida. La cuenta de un usuario puede verse comprometida por elegir una clave sencilla de adivinar, o por algún descuido. El principal inconveniente es que un hacker mínimamente preparado puede borrar sus huellas fácilmente, lo que hace muy difícil descubrir el ataque. Si el único usuario es el administrador, la detección del intruso es mucho más fácil, ya que el simple hecho de que alguien entrado en el sistema es un indicativo de que sucede algo raro.

Esta estructura de cortafuegos ofrece la ventaja sobre un screening router, de que es más fácil actualizar el software del sistema para obtener registros del sistema en distintos tipos de soporte, lo que facilita el análisis de la situación en caso de que la seguridad se haya visto comprometida. El aspecto más débil de esta estructura es su modo de fallo. Si el cortafuegos es destruido, es posible que un hacker preparado reactive el reenvío TCP/IP teniendo libre acceso a toda la red protegida. Para detectar esta situación conviene tener al día las revisiones del software con el fin de eliminar los “bugs” de

seguridad. Además no conviene hacer público el tipo y versión del sistema operativo instalado en la máquina para no facilitar el trabajo de los posibles atacantes.

2.3.4.- Screened Host Gateway.

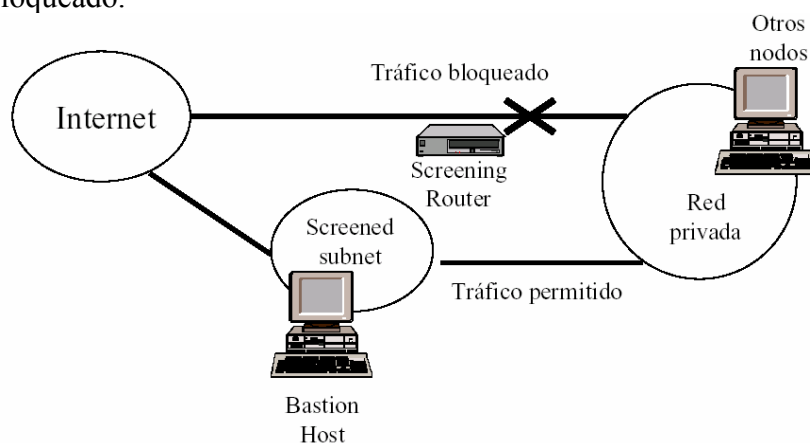
Es la configuración de cortafuegos más común. Está implementada usando un bastion host y un screening router. Habitualmente el bastion host está en la red privada, y el screening router está configurado de modo que el bastion host es el único nodo de dicha red que es accesible desde Internet para un pequeño número de servicios.



Como el bastion host está en la red privada, la conectividad para los usuarios es muy buena, eliminando los problemas que suelen aparecer al tener definidas rutas extrañas. Si la red privada es una red local virtual extensa, el esquema funciona sin necesidad de cambios en las direcciones de la red local siempre que ésta esté usando direcciones IP válidas. La zona de riesgo se circunscribe al bastion host y el screening router. La seguridad de éste último depende del software que ejecute. Para el bastion host, las consideraciones sobre seguridad y protección son similares a las hechas para un sistema del tipo dual homed gateway.

2.3.5.- Screened Subnets.

En algunas configuraciones de cortafuegos se crea una subred aislada, situada entre la red privada e Internet. La forma habitual de usar esta red consisten emplear screening routers configurados de forma que los nodos dicha subred son alcanzables desde Internet y desde la red privada. Sin embargo, el tráfico desde Internet hacia la red privada es bloqueado.



En la subred suele haber un bastion host como único punto de acceso a la misma. La zona de riesgo es pequeña y está formada por el propio bastion host, los screening routers que filtran el tráfico y proporcionan las conexiones entre Internet, la subred y la red privada. La facilidad de uso y las prestaciones de la subred varían, pero en general sus servicios se basan en un bastion host que ofrece los servicios a través de gateways para las aplicaciones, haciendo hincapié en que lo que no está explícitamente permitido, está prohibido.

Si este tipo de cortafuegos es atacado en un intento de destruirlo, el hacker debe reconfigurar el tráfico en tres redes, sin desconectarlas, sin dejarse encerrado a sí mismo y sin que los cambios sean detectados por máquinas y usuarios. Aunque esto puede ser posible, todavía puede dificultarse más si los routers sólo son accesibles para su reconfiguración desde máquinas situadas en la red privada.

Otra ventaja de este tipo de cortafuegos es que pueden ser instalados de forma que oculten la estructura de la red privada. La subred expuesta es muy dependiente del conjunto de software que se ejecute en el bastion host. La funcionalidad es similar a la obtenida en los casos anteriores, sin embargo la complejidad de configuración y encaminamiento es mucho mayor.

2.3.6.- Gateways Híbridos.

Cualquier estructura diferente de las anteriores. Por ejemplo sistemas que conectados a Internet pero que sólo son accesibles a través de enlaces serie conectados a servidores de terminales ethernet en la red privada. Este tipo de configuraciones pueden beneficiarse del uso de múltiples protocolos, el encapsulamiento de unos protocolos sobre otros. Sin embargo, ocultar la estructura del cortafuegos no es un medio de aumentar la seguridad en sí mismo, sino una forma de dificultar el ataque. Conviene tener en cuenta que un hacker no se va a desanimar por la existencia de este tipo de dificultades.

2.4.- Aplicabilidad.

No se puede hablar de que tipo de cortafuegos es el mejor, ya que dicha afirmación depende de muchos factores que hacen que cada caso pueda tener una respuesta diferente. Entre dichos factores figuran el coste, la política de la empresa, la tecnología de red y el personal que se tiene disponible. Todos estos factores pueden pesar más que consideraciones puramente técnicas.

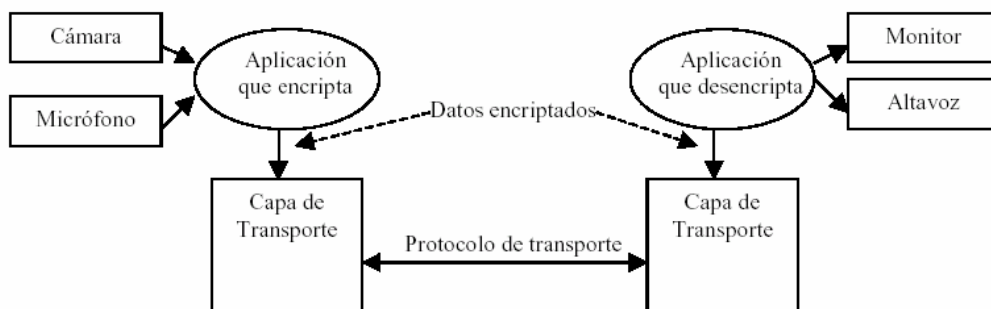
Conviene tener en cuenta que un cortafuegos es un dispositivo de red de importancia creciente, al menos desde el punto de vista de administración y seguridad. Debe considerarse como un punto desde el que poder controlar con más facilidad los riesgos a los que puede estar sometida una red de computadores. El concepto de **zona de riesgo** es fundamental. Lo ideal sería que cada nodo de la red protegida tuviese un alto nivel de seguridad de modo que el cortafuegos fuese redundante. Sin embargo, siendo realistas esta alternativa es poco viable.

Otro aspecto fundamental es que un cortafuegos no puede ser considerado como una vacuna. No debe instalarse un determinado tipo de cortafuegos porque para alguien sea *suficientemente seguro*. Dicho concepto debe ser resultado de un análisis del coste de implantación, administración, nivel de protección obtenido y valor de los datos que se protegen. Es importante no tener prisas a la hora de tomar este tipo de decisiones, ya que el uso del cortafuegos no se reduce a su diseño e implementación, ya que para garantizar su éxito en la defensa de la red privada es necesario **una cuidada labor de administración y vigilancia del mismo**.

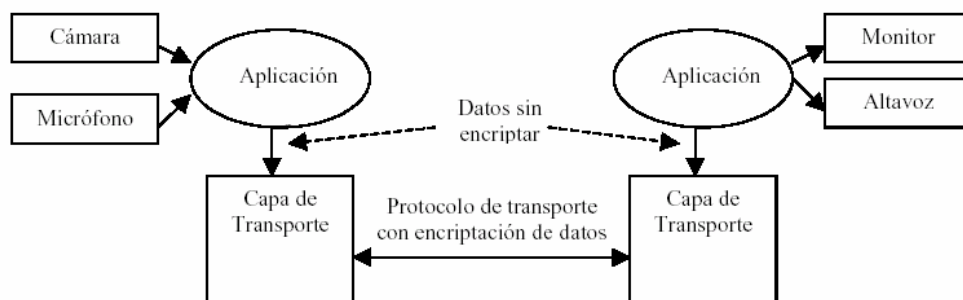
3.- Seguridad en el canal.

Aunque los usuarios de los computadores que son extremo de una comunicación puedan estar tranquilos en cuanto a la seguridad de estos computadores, la red de comunicaciones siempre es un punto de desconfianza. La prevención ante los ataques a la red suele pasar siempre por el uso de alguna u otra manera de técnicas de **criptografía** tanto para proteger el secreto de los datos como para permitir la identificación de quienes los envían o reciben. La criptografía es el estudio de técnicas de cifrado seguras, mientras que el **criptoanálisis** es el estudio de las técnicas orientadas a romper los cifrados. El conjunto de ambas ciencias se conoce como **criptología**. A la aplicación de las técnicas de criptografía en las comunicaciones se dedicarán los siguientes apartados.

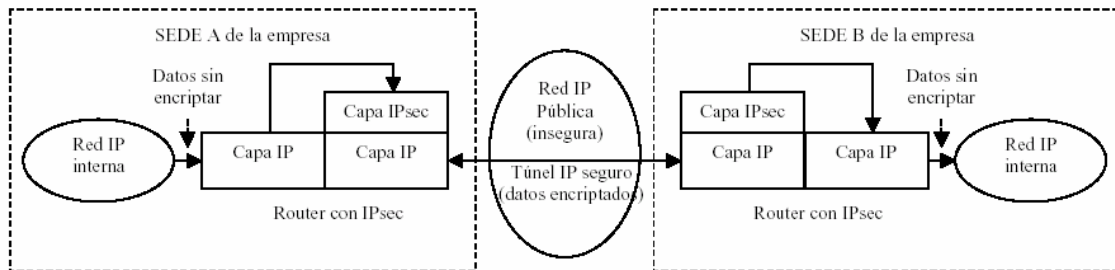
Puede aplicarse la encriptación a distintos niveles:



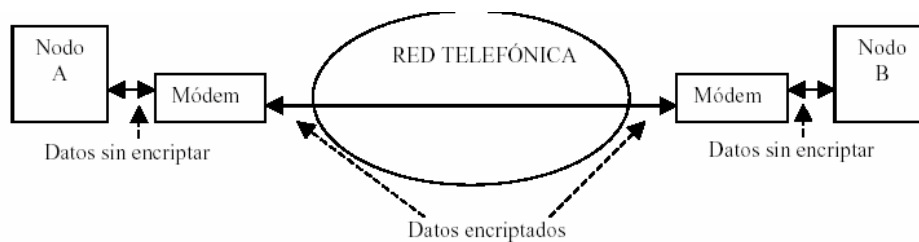
- **APLICACIÓN:** La aplicación que envía los datos del usuario, por ejemplo una de videoconferencia, encripta los datos antes de entregárselos a la capa de transporte y son desencriptados por la aplicación que recibe los datos antes de entregárselos al usuario receptor.



- **TRANSPORTE:** La capa de transporte puede utilizar un protocolo que encripte el campo de datos de cada segmento que envía (TPDU) donde van los datos del usuario. Para ello ambas entidades de transporte, a uno y otro extremo han de ser capaces de negociar ese protocolo con encriptación.



- **RED:** Se pueden utilizar protocolos de red que utilicen encriptación, de manera que el campo de datos de las unidades que transmite el protocolo van encriptados. Pero esto exige que todos los nodos de la red, incluidos los que hacen el encaminamiento, soporten ese protocolo. Por ejemplo, en una red IP todos los nodos de la red deberían actualizar el protocolo actual, IPv4, a la nueva versión IPv6 que admite encriptación del campo de datos del datagrama. Otra alternativa consiste en establecer “túneles” en una red IP insegura entre “routers” que unen distintas subredes de una empresa entre sí, empleando un protocolo como IPsec (IP seguro) que viaja encriptado dentro del campo de datos de los datagramas IP convencionales que atraviesan la red pública.



- **ENLACE:** En este caso la encriptación/desencriptación la realiza el ETCD (DTE) empleado por el usuario como interfaz con la línea física de comunicación que le une con el o los interlocutores. Un ejemplo son los módem capaces de encriptar la información que transmiten cuando dialogan con otro módem con las mismas capacidades.

3.1.- Métodos básicos de criptografía.

Los métodos básicos de cifrado son el **cifrado por sustitución** y el **cifrado por transposición**. Prácticamente todas las técnicas de cifrado se basan en uno de estos métodos o en combinaciones de ambos. Todos los métodos requieren el uso de algún tipo de clave.

3.1.1.- Cifrado por sustitución.

El cifrado por sustitución consiste en sustituir cada carácter, octeto o bloque de datos por otro de acuerdo con un algoritmo determinado, generalmente, basado en algún tipo de clave. Los ejemplos más sencillos son:

a) **Aplicación de Máscaras XOR:** Se hace la operación XOR del dato a transmitir con la clave, y se recupera es dato original volviendo a hacer la operación XOR con la misma clave.

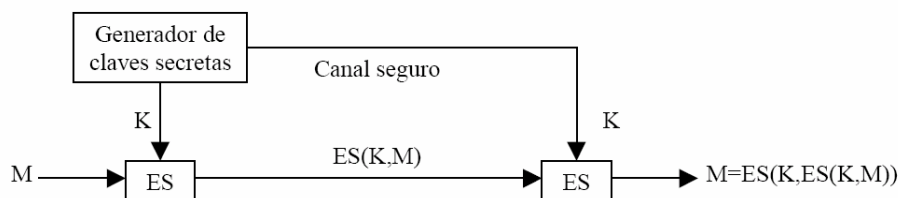
b) **Utilización de tablas de traducción:** Estas tablas asignan a cada dato un dato diferente que es el que se transmite. El receptor con la misma tabla podrá conocer el dato real que representa el dato recibido.

3.1.2.- Cifrado por transposición.

Consiste en tomar bloques de datos y cambiar el orden de estos dentro del bloque. Haciendo la transposición inversa se consigue recuperar el bloque original.

3.2.- Criptografía simétrica.

Si se utiliza la misma clave para el cifrado y el descifrado de los datos se habla de criptografía simétrica. Los métodos que usan claves simétricas se conocen también como **métodos de clave secreta** ya que sólo aquellos entes que intervienen en la comunicación deben conocer la clave. Si se denomina M a la información a transmitir aún sin cifrar, K la clave utilizada y $ES()$ a la función de cifrado simétrico, en la criptografía simétrica el mensaje que se transmite es $ES(K,M)$, resultado de cifrar M con la clave K . El mensaje original se recupera aplicando el mismo algoritmo de cifrado con la misma clave, es decir, $M=ES(K,ES(K,M))$. El gran problema en la criptografía simétrica está en el uso de claves secretas. Estas deben ser generadas por elementos seguros (en muchos casos uno de los extremos de la comunicación) y transmitidas por canales también seguros, lo que implica generalmente una vía diferente de la red de comunicaciones.



Un ejemplo de criptografía simétrica es el *Data Encryption Standard*, DES, desarrollado por el US National Bureau of Standards e IBM. Utiliza claves de 64 bits aunque en realidad solo 56 son útiles. El algoritmo combina métodos de transposición y sustitución para codificar normalmente bloques de 64 bits, aunque se puede aplicar de dos modos diferentes:

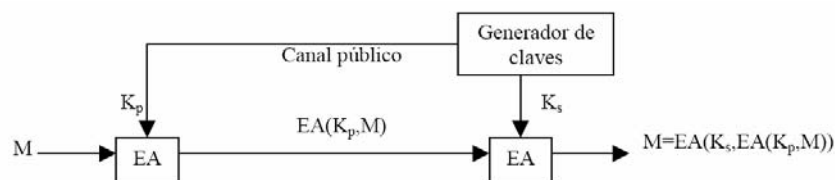
- a) **En modo bloque:** De un bloque de información de 64 bits se genera otro bloque de 64 bits cifrado, siendo el resultado equivalente a una sustitución.
- b) **En modo stream:** El algoritmo se puede aplicar a un flujo de octetos sin esperar a tener un bloque completo de 64 bits y resulta más difícil de romper por que la codificación de un octeto depende de la anterior.

La potencia del algoritmo DES está en el enorme espacio de claves 256, es decir, aproximadamente $7,6 \cdot 10^{16}$ claves y en el diseño de las 8 tablas o cajas de sustitución que se emplean en el algoritmo y que nunca se han hecho públicas. Aunque existen sospechas sobre puntos débiles en el diseño de estas cajas no se conoce actualmente ningún método práctico de ataque al DES. En cuanto al posible ataque mediante pruebas con distintas claves, en el momento del desarrollo del algoritmo DES en 1977, suponiendo que una máquina pudiese hacer un cifrado DES por microsegundo y que fuese necesario como media revisar la mitad del espacio de claves para romper el cifrado, el tiempo total estimado sería de más de 1000 años.

Aunque el algoritmo ha sido seguro hasta la actualidad, ahora se estima que se podría diseñar una máquina paralela con un coste de alrededor de un millón de dólares que conseguiría romper el cifrado en unas cuantas horas. Por ello se buscan alternativas y una de las posibles es el DES Triple que como su nombre indica está basado en el algoritmo DES clásico.

3.3.- Criptografía asimétrica.

Si la clave es distinta para el cifrado y el descifrado, se habla de criptografía asimétrica. Los métodos que usan claves asimétricas generalmente mantienen secreta la clave empleada para el descifrado y hacen pública entre el resto de usuarios la clave con la que deben cifrar los mensajes para que sólo él los pueda descifrar, por lo que se conocen también como **métodos de clave pública**. Si se denomina M a la información a transmitir aún sin cifrar, K_S a la clave secreta para el descifrado, K_P a la clave pública para el cifrado y $EA()$ a la función de cifrado asimétrico, el mensaje que se transmite es $EA(K_P, M)$, resultado de cifrar M con la clave K_P . El mensaje original se recupera aplicando el mismo algoritmo de cifrado pero con la clave secreta, es decir, $M = EA(K_S, EA(K_P, M))$.



Para que un método de clave pública sea funcional se han de cumplir dos requisitos:

- a) Debe ser muy difícil averiguar K_S a partir de K_P .
- b) Debe ser muy difícil obtener la información que contiene el mensaje cifrado si no se dispone de K_S .

El algoritmo RSA publicado en 1978 por tres investigadores del MIT cumple estos dos requisitos y es desde entonces la única técnica mundialmente aceptada de clave pública.

Es un método de cifrado en el que el bloque de información original y el bloque cifrado son un número entero entre 0 y $N-1$ para un N dado. Los pasos a seguir para la utilización del algoritmo RSA son los siguientes:

- a) Se escogen dos números primos grandes (generalmente mayores que 10^{100} , aunque este ejemplo se expone con valores pequeños): $P=7$, $Q=17$.
- b) Se calcula $X=(P-1) \cdot (Q-1)=96$ y $N=P \cdot Q=119$.
- c) Se elige un número primo respecto a X , por ejemplo $E=5$.
- d) La clave pública será $K_p=(E,N)=(5,119)$.
- e) Se calcula D de tal manera que $\text{MOD}(D \cdot E, X)=1$, por ejemplo $D \cdot 5/96=4+1/96 \Rightarrow D=77$.
- f) La clave secreta será $K_s=(D,N)=(77,119)$.
- g) Para cifrar el mensaje $M=19$: $C=\text{MOD}(M^E, N)=\text{MOD}(19^5, 119)=66$.
- h) Para descifrar: $M=\text{MOD}(C^D, N)=\text{MOD}(66^{77}, 119)=19$.

Se eligen P y Q muy grandes para que sea difícil de factorizar el producto $N=P \cdot Q$, ya que P y Q son primos y debe de haber el gran número de posibles pares (P, Q) . Los tres desarrolladores retaron a la comunidad científica a descifrar un mensaje cifrado con una clave pública con modulo N de 129 dígitos decimales. En 1994, 1600 computadores cooperando en Internet y tras ocho meses de trabajo descubrieron el código.

Esto no invalida el uso de RSA, sino que indica que la clave ha de ser más grande. Actualmente se considera suficiente un tamaño de clave de 1024 bits, aproximadamente 300 dígitos decimales. Sin embargo, esto implica que el algoritmo de cifrado es lento, se estiman 0,1 segundos para 512 bits en su implementación en hardware. Por ello se emplea para determinadas aplicaciones como, por ejemplo, el intercambio de claves para el uso de un algoritmo simétrico.

4.- Seguridad de Acceso.

La seguridad de acceso contempla básicamente la **identificación** del usuario o entidad que desea acceder, la **autorización** del acceso y la **auditoria** de las tareas realizadas en el sistema por la entidad que ha accedido. La identificación de usuarios o entidades que acceden se realiza generalmente mediante palabras clave, sistemas de firma digital de los mensajes u otros medios. Esta identificación incluye a las máquinas involucradas en la comunicación en casos como el comercio electrónico.

Una problemática aún no resuelta por completo es el acceso de usuarios a través de redes extrañas a la empresa. Imagínese el caso de un empleado de una empresa A que visita a otra B y pide permiso a para conectar su computadora portátil a la red de B para acceder a sus datos que residen en A:

- a) Para la red B el empleado de A es un elemento completamente extraño y potencialmente peligroso por lo que su acceso a través de su red ha de ser vigilado y limitado.
- b) Para el empleado de A la red B es extraña y potencialmente insegura, por lo que su acceso a través de ella es peligroso y se han de poner todos los medios necesarios para proteger la información que se intercambie durante la conexión.
- c) Para la red A el empleado será conocido (y posiblemente el ordenador que utiliza), pero la red desde la que accede es potencialmente insegura. Por ello, se han de extremar las medidas para identificar correctamente y sin posibilidad de engaño al usuario y su equipo, y otorgarle un acceso temporal para evitar su posterior reutilización por parte de alguien extraño a la empresa.

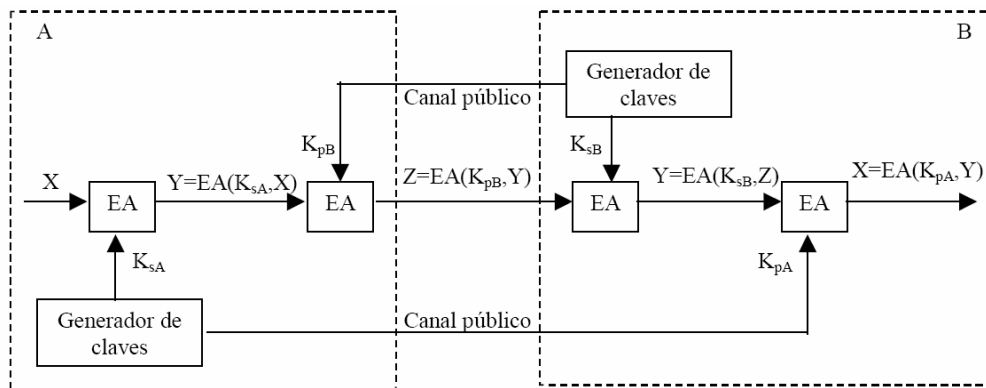
Algunas de las técnicas que se describen a continuación son utilizadas para resolver algunos de los problemas que plantean estas situaciones.

4.1.- Autenticación mediante firma digital.

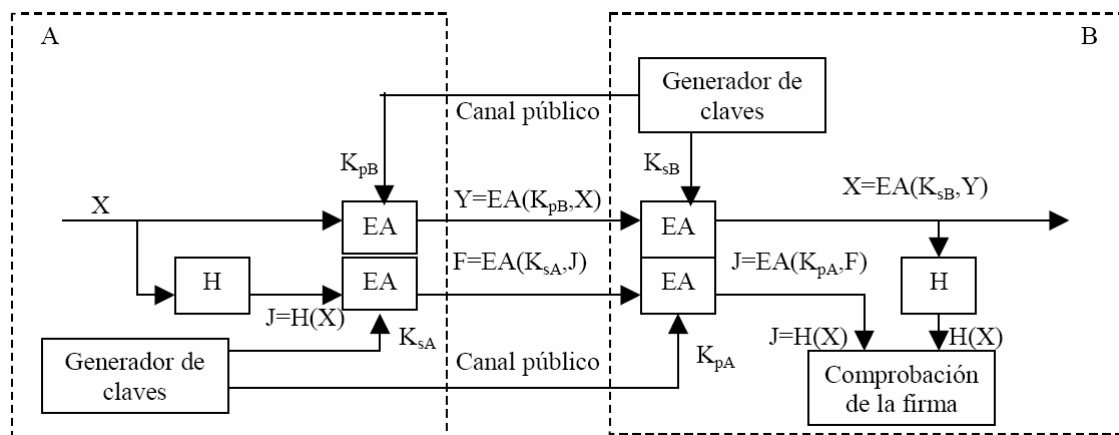
Una de las aplicaciones del cifrado asimétrico es comprobar la autenticidad de los mensajes, es decir, la confirmación para el receptor de que el mensaje recibido ha sido emitido realmente por quien dice ser su emisor. Para ello el algoritmo de cifrado asimétrico ha de cumplir además de $M=EA(K_S,EA(K_P,M))$, que $M=EA(K_P,EA(K_S,M))$.

El usuario A, emisor del mensaje X, lo firmará cifrándolo con su clave secreta K_{SA} . Si se transmitiese así el mensaje $Y=EA(K_{SA},X)$, cualquier usuario que conozca la clave pública de A, K_{PA} , podría descifrarlo. Por ello A hace un segundo cifrado utilizando la clave pública de B, K_{PB} , de tal manera que ahora sólo B podrá descifrar el mensaje $Z=EA(K_{PB},Y)$. Cuando B recibe el mensaje y le aplica su clave secreta el resultado que obtiene es un mensaje aún cifrado $Y=EA(K_{SB},Z)$. Si B consigue descifrar ese mensaje Y con la clave pública de A, $X=EA(K_{PA},Y)$ significará que A es realmente quien ha enviado el mensaje ya que sólo él tiene la clave secreta para cifrar el mensaje de esa manera.

Obsérvese además que la firma digital es sólo necesaria en el caso de la criptografía asimétrica. Si se empleara criptografía simétrica con claves secretas la autenticidad del mensaje está implícita puesto que sólo el otro interlocutor conoce la clave secreta si la distribución de la misma se ha hecho de manera segura.



El aplicar dos veces consecutivas un cifrado asimétrico a un mensaje completo puede ser muy costoso en tiempo de computación por lo que generalmente no se firma todo el mensaje sino un código reducido que lo represente. Este código se suele obtener mediante la aplicación al mensaje completo de una función *hash*, $H()$, sencilla, irreversible y conocida públicamente, que aplicada a X nos da una cadena con unos pocos octetos $J = H(X)$. El mensaje completo sólo se cifra con la clave pública de B, $Y = EA(K_{pB}, X)$, y junto con el se envía la firma consistente en aplicar la clave secreta de A al resultado de la función hash $F = EA(K_{sA}, J)$. Una vez que recibe el mensaje cifrado y la firma, B obtiene $X = EA(K_{sB}, Y)$ y $J = EA(K_{pA}, F)$. Si B comprueba que al aplicar la función hash a X obtiene el mismo resultado J que le ha llegado en la firma, estará seguro de que el mensaje procede realmente de A.



4.2.- Autoridades certificadoras.

Para que los métodos de clave secreta funcionen es vital que las claves se distribuyan de forma segura. En el caso de los de clave pública, el problema es más sutil. ¿Cómo se sabe que la clave pública que distribuye una estación N que se incorpora a una comunidad es realmente distribuida por la estación N y no por alguien que la suplanta?.

Un sistema de comunicaciones seguro debe disponer de una *autoridad certificadora* (denominada AC a partir de ahora) para la comunidad, encargada de gestionar las claves secretas y/o públicas y de asegurar su pertenencia exclusiva a un usuario de una forma automática y dinámica, agilizando así el intercambio de claves de una forma segura.

Dos situaciones pueden comprometer la seguridad del sistema:

- a) La AC tiene que ser un sistema seguro ya que cualquier fallo en su seguridad comprometería la seguridad de todo el sistema que se fía de su integridad.
- b) Cada entidad que se incorpora a la comunidad segura ha de establecer un enlace seguro con la AC mediante algún sistema de “entrevista personal” que asegure la identidad de ambas partes y en la que se realice el intercambio de las claves secretas o públicas que se utilizarán en el enlace seguro.

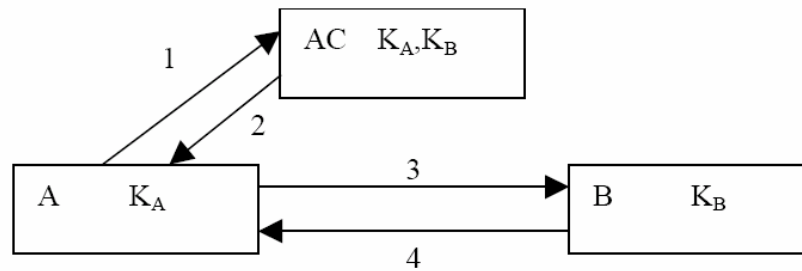
Si se salvan con éxito estas dos situaciones, los usuarios de la comunidad podrán a intercambiar información a través de la red cifrada mediante claves secretas o públicas actualizadas cuantas veces se quiera de forma segura a través de la misma red. De la misma manera se tendrá seguridad sobre la autenticidad del interlocutor.

4.2.1.- Distribución de claves en el cifrado simétrico.

En el cifrado simétrico, la autoridad certificadora, generará las claves secretas a usar por cada usuario o para cada sesión (dos usuarios podrían utilizar varias claves secretas para distintas sesiones simultáneas o no).

Cuando dos miembros quieren ponerse en contacto, el que toma la iniciativa solicita a la AC una clave a usar sólo para esa sesión. Los pasos a seguir son los siguientes:

1. A hace la petición de comunicar con B a la AC, usando K_A , clave secreta que comparten solo A y la AC.
2. La AC genera la clave para la sesión K_{ses} (puede que incluya más parámetros como tiempo de validez, etc.) y construye un mensaje con dos partes: la clave para la sesión y esa misma clave cifrada con la clave K_B que comparte con B, es decir, $M=[K_{ses}, ES(K_B, K_{ses})]$, y se lo envía a A cifrado con K_A : $ES(K_A, M)$.
3. A descifra M con K_A , y obtiene K_{ses} y algo indescifrable $ES(K_B, K_{ses})$ que le envía a B sin cifrar para establecer la comunicación.
4. B obtiene K_{ses} descifrando la petición de A con K_B con lo que sabe que la petición de A está legitimada por la AC que es la única que a podido cifrar la clave de sesión usando K_B . A partir de ahí B acepta la sesión con A utilizando para el intercambio de información K_{ses} .

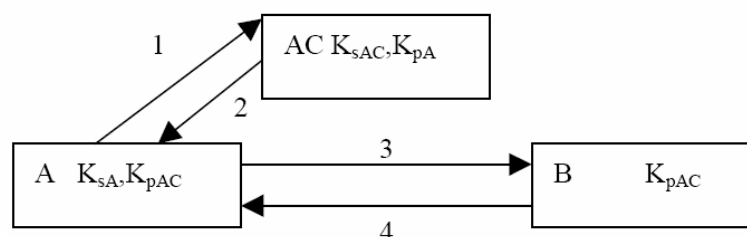


4.2.2.- Emisión de certificados en el cifrado asimétrico.

En el cifrado asimétrico la AC distribuye parejas de clave pública y secreta únicas para cada usuario (o sesión). Además generará *certificados de autenticidad*, con un tiempo de validez limitado, que permitirán a un extremo autenticarse ante el otro para una determinada sesión o intercambio de información. Un ejemplo del posible proceso a seguir sería el siguiente:

1. Si A quiere comunicar con B, A hace la petición de un certificado a la AC, usando K_{sA} , clave secreta cuya pareja K_{pA} conoce la AC.
2. La AC genera un certificado compuesto al menos por el mensaje $M=[IDA, K_{pA}, T]$ (donde IDA es un identificador público de A, por ejemplo su e-mail, y T el tiempo de validez del certificado) y una firma de la AC calculada como $F=EA(K_{sAC}, H(M))$ (donde K_{sAC} es la clave secreta de la AC cuya pareja K_{pAC} , conocen todos los miembros de la comunidad y H es una función hash) y se lo envía a A cifrado con K_{pA} : $EA(K_{pA}, [M, F])$.
3. A descifra el certificado $[M, F]$ con K_{sA} , y se lo envía a sin cifrar B para establecer la comunicación.
4. B calcula por un lado $H(M)$ y por otro descifra con K_{pAC} la firma F de la AC $EA(K_{pAC}, F)$. Finalmente si comprueba que $H(M)=EA(K_{pAC}, F)$ estará seguro de que A es quien dice ser y que puede utilizar la clave K_{pA} para cifrar la información y aceptar la conexión puesto que está autenticada por una firma que sólo ha podido generar la AC.

Hay que advertir que el mismo procedimiento es válido para que B autentique su clave pública K_{pB} ante A, e incluso también es válido si se desea que las parejas (K_{sA}, K_{pA}) y (K_{sB}, K_{pB}) utilizadas en la sesión entre A y B sean distintas de las que comparten con la AC.



5.- Seguridad interna.

Los ataques a la seguridad pueden realizarse desde el interior de la red de la empresa, bien por parte de usuarios de esa red, por intrusos que acceden físicamente a alguno de los sistemas de la red o por intrusos que desde el exterior de la red han ganado el acceso a alguno de los sistemas internos de la red. En estos dos últimos casos el intruso generalmente suplanta a uno de los usuarios legítimos de la red o acceden a través de algún agujero de seguridad en el sistema. Para prevenir el que estos ataques prosperen se pueden implantar técnicas como las siguientes.

5.1.- Compartimentalización.

Los repetidores y conmutadores que disponen de la posibilidad de filtrar el tráfico de red que circula por sus puertos permiten la compartimentalización de la red local. Estos equipos consiguen que el tráfico de tramas de unas zonas de la red o incluso de cada puerto, no pueda ser visto por sistemas conectados en otras zonas u otros puertos. Las formas básicas de protección implementadas en estos equipos son:

- **Seguridad anti-escuchas:** A través de cada puerto sólo se podrán recibir las tramas en cuyo encabezamiento aparezca la dirección física de las computadoras conectadas a través de ese puerto o de las tramas enviadas a direcciones “broadcast”.
- **Seguridad anti-intrusos:** A través de cada puerto sólo podrán enviar tramas aquellas computadoras cuya dirección física haya sido admitida como legítima para utilizar ese puerto.

Este tipo de dispositivos pueden llevar a cabo un aprendizaje inteligente que facilita la configuración de los mismos, de manera que a través del tráfico que escuchan, determinan que dispositivos tienen conectados en cada puerto para realizar filtrado antiescuchas o determinar qué equipo es el legítimo usuario de un puerto frente a posibles intrusos.

También colaboran a la compartimentalización de la red los encaminadores a nivel de protocolos de red (*routers*, encaminamiento en la capa de red). Al encaminar protocolos de red como IP, IPX, etc., permiten a la vez filtrarlos total o parcialmente, en función por ejemplo de las direcciones lógicas de los datagramas. Podrían introducirse incluso cortafuegos en el interior de la red para llevar el filtrado hasta niveles superiores, pero esta solución ya es menos habitual.

5.2.- Monitorización.

La monitorización de una red suele ser uno de los procesos previos al ataque a la seguridad de los sistemas conectados a la misma. La red puede ser monitorizada por sniffers (programas que capturan tramas de la red para su posterior análisis) instalados en algún sistema de la red mediante el sistema de los programas *troyanos* o por el uso ilegítimo de alguna cuenta de usuario más o menos privilegiada. La información obtenida sirve para explotar otros agujeros de seguridad u obtener claves de usuarios de

la red. La compartimentalización de la red descrita en el apartado anterior, dificulta grandemente la labor de monitorización de los *sniffers*.

Sin embargo la misma técnica de monitorización puede servir para detectar y perseguir a los intrusos. La detección de determinados volúmenes o contenidos de tráfico sospechoso mediante un programa *analizador de protocolos* (que básicamente es un *sniffer* de elevadas prestaciones) permite la detección de ataques. El mismo programa puede ayudar a determinar la procedencia y responsabilidad del ataque.

5.3.- Seguridad en servidores.

Además de las actividades y actitudes de auditoria, formación, concienciación y responsabilidad descritas en el apartado referido a las políticas de seguridad, se describen a continuación medidas a tener en cuenta cuando se instalan servicios de red en una máquina.

En primer lugar, conviene tener claro que existen muchos tipos servicios y que cada uno de ellos tiene sus propios requisitos de seguridad. Como norma común el administrador de la máquina que ofrezca algún servicio de red, debe preocuparse de conocer la problemática particular que cada servicio ofertado presenta y, además, mantener actualizado el software de soporte para dicho servicio con el fin de ir tapando los agujeros de seguridad que se descubran.

Puede considerarse la siguiente división de los servicios:

- En función de su visibilidad:
 - Servicios que **sólo deben ser accedidos desde máquinas** de nuestra propia red, por ejemplo NFS. En estos casos, puede ser suficiente con proteger el servidor interno de cualquier acceso desde máquinas fuera de nuestra red.
 - Servicios **ofrecidos a otras redes**, por ejemplo un servidor web. En estos casos la protección es más compleja, y es el conjunto servicio/protocolo/servidor, el que debe incluir aquellas medidas de seguridad necesarias para prevenir el acceso no autorizado o la modificación de información
- En función del tipo de usuario:
 - Servicios **accesibles sólo por usuarios de nuestra red**. Por ejemplo, podemos desear que sólo usuarios de nuestra organización puedan utilizar nuestros servicios ftp o telnet.
 - Servicios **accesibles por cualquier usuario**. Por ejemplo, un ftp anónimo.

En general, es aconsejable dedicar máquinas diferentes para ofrecer servicios a cada grupo de usuarios, separando aquellos ofrecidos al exterior de los de uso interno. Esta práctica permite definir estrategias de administración diferentes sobre cada grupo de servicios, facilitando la tarea del administrador. Debe evitarse al máximo la instalación

en una misma máquina de servicios ofrecidos sólo a nuestros usuarios y los ofrecidos libremente. Cada uno de estos servidores será accesible a través de uno o varios cortafuegos que aseguran la partición de la red en función del nivel de seguridad que se requiera.

Hay que tener especial cuidado con aquellos servicios que permitan conexiones anónimas o a cuentas de invitado. Se debe poner especial hincapié en aislar dichos servidores del resto de la red protegida. Además, la tendencia actual es que cada sitio puede ser considerado responsable del contenido de la información que es públicamente accesible. Además, en estos casos hay que reforzar al máximo las medidas de auditoria, ya que presentan un fácil punto de penetración.