TEMA 8: SEGURIDAD EN LAS COMUNICACIONES

INDICE TEMA 8

1 INTRODUCCIÓN

1.1 El gusano de Internet de 1988

2 de noviembre de 1988, el día más terrible de la historia de Internet y sin embargo también uno de sus mejores momentos. Hacia las 6:00 p.m. (hora de la costa Este de los EEUU), un licenciado de la Universidad de Cornell lanzó el primer gusano de red: el primer virus importante que llegó a Internet. Casi de inmediato el gusano invadió los ordenadores (VAX de DEC y los sistemas Sun 3 de Sun Microsystems) de todo el país, desde los laboratorios Lincoln hasta el National Supercomputer Center, pasando por las universidades de Boston y California.

En poco más de una hora el virus había cerrado muchos de los principales centros de investigación nacionales e internacionales. Afortunadamente, todos los sitios afectados (entre 4000 y 6000 máquinas) sólo representaban un 5 o un 7 por ciento del total de Internet (que en aquel entonces constaba de unas 80000 máquinas). En el 95 por ciento restante, los voluntarios se pusieron manos a la obra casi al instante. Inmediatamente nació un grupo de voluntarios autodenominado "VirusNet" y sus miembros trabajaron contra reloj para detener al gusano.

En 24 horas, se encontró un defecto en el programa del gusano que podía permitir detenerlo, se aisló y se estudió su comportamiento y se escribieron parches para cerrar los puntos vulnerables que explotaba para introducirse en los sistemas. De este modo se detuvo la amenaza. En una semana todos los ordenadores afectados estaban de nuevo en funcionamiento.

Aunque los daños producidos fueron mínimos, el gusano sirvió como "llamada de atención" a los profesionales de seguridad y tecnologías de información de todo el mundo acerca de la realidad y la seriedad de los riesgos de Internet.

Robert T. Morris Jr., el estudiante de Cornell que programó el gusano, fue condenado a tres años en libertad condicional, 400 horas de servicios a la comunidad y una multa de 1,5 millones de pesetas. Morris fue el primer "hacker" de Internet de todo el mundo. Se dice que desde el primer momento se arrepintió de haber lanzado el gusano, e incluso que se trataba de un simple "bug" en un programa que estaba realizando, y que pidió a un amigo que publicase inmediatamente el método para detenerlo en un tablón electrónico de mensajes. Desgraciadamente, el gusano acabó con la BBS antes de que nadie pudiera recoger la solución.

1.2 Cómo se ejecuta el gusano de Internet

El método utilizado por el gusano de Internet para cerrar tantos sistemas era relativamente sencillo. Después de entrar en un sistema informático, el sistema operativo creaba un único proceso para ejecutar el gusano. Después éste buscaba una conexión de red externa, enviando a través de ella una copia de sí mismo. A continuación el gusano generaba otros procesos que eran copias exactas de sí mismo.

En otras palabras, el gusano creaba un duplicado exacto de sí mismo en la memoria del ordenador. Después de esto el sistema operativo tenía dos copias del gusano en ejecución. Ambas buscaban una conexión de red externa para propagarse y se volvían a duplicar. Ya existían cuatro gusanos en el ordenador.

En poco tiempo el gusano consumía suficientes recursos como para que el sistema operativo "congelase" a los usuarios, después a los administradores y por último a sí mismo.

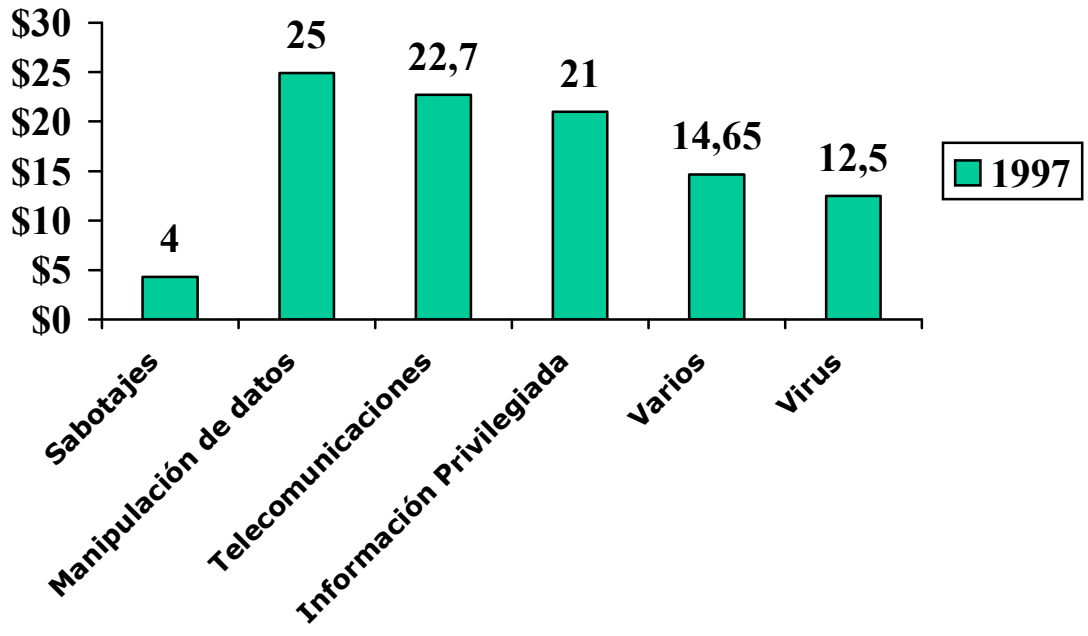
Desgraciadamente, como el gusano ya se encontraba en Internet, a menudo infectaba ordenadores apagados por el administrador en cuanto volvía a encenderlos.

1.3 Riesgos crecientes

A principios de marzo de 1997, el *Computer Security Institute* (una asociación internacional de profesionales de seguridad informática) informó que su reciente encuesta entre 249 empresas de EE.UU. revelaba que entre todas habían perdido más de 100 millones de dólares por delitos relacionados con violaciones de la seguridad informática. Si se proyecta esta cifra a todas las empresas de los Estados Unidos cuyo negocio es similar al de las empresas de la encuesta, la cifra de pérdidas resultante alcanza decenas de miles de millones de dólares. El FBI estima que las compañías de los EE.UU. pierden más de 75000 millones de dólares cada año debido a delitos informáticos.

Y los números crecen de manera exponencial cada año.

En la siguiente figura vemos un desglose de las pérdidas indicadas por las empresas consultadas.



Según un informe del departamento de defensa de los EE.UU., el 88% de sus ordenadores pueden ser atacados. Es más, el 96% de los casos en los que los hackers han entrado en sus sistemas, los profesionales de seguridad no pudieron detectarles. Está claro que los administradores de sistemas, los profesionales de seguridad, administradores de tecnología de información, Webmasters, etc. deben determinar los riesgos de su sistema y dar los pasos necesarios para reducirlos.

2 SEGURIDAD EN LAS COMUNICACIONES

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 **autentificación 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**: Autorizar 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 (snooping)* y el *análisis de tráfico (packet sniffing)*. 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 (spoofing)*, que es la suplantación de un ente autorizado para acceder a información o recursos, la *modificación (tampering o data diddling),* que incluye también la posible destrucción y creación no autorizada de datos o recursos, y la *interrupción (jamming o flooding y otros)*, que supone el impedir a entes autorizados su acceso a la información o recursos a los que tienen derecho de acceso (denegación de servicio, DoS).

Las contramedidas se suelen aplicar cuando se ha detectado un ataque, lo cual no suele ser una política adecuada. Los ataque pasivos son difíciles de detectar pero suelen existir contramedidas para prevenirlos. Por el contrario, los ataque 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.

2.1 Tipos de ataque más comunes

En los primeros años, los ataques involucraban poca sofisticación técnica. Los "insiders" (empleados disconformes o personas externas con acceso a sistemas dentro de la empresa) utilizaban sus permisos para alterar archivos o registros. Los "outsiders" (personas que atacan desde afuera de la ubicación física de la organización) se introducían en la red simplemente averiguando una contraseña válida.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas. Esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevo a la desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automatizados, etc.).

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita conocimiento técnico básico para realizarlos. El aprendiz de intruso tiene acceso ahora a numerosos programas y scripts de numerosos "hackers", BBSs y sitios web, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

Los métodos de ataque descritos a continuación están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras. Por ejemplo: después de “crackear” una contraseña, un intruso realiza un “login” como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente el atacante puede también adquirir derechos de acceso a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

Eavesdropping y Packet Sniffing (husmeo de paquetes)

Muchas redes son vulnerables al *eavesdropping*, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por *packet sniffers*, que son programas que monitorizan los paquetes que circulan por la de red. El *sniffer* puede ser colocado tanto en una estación de trabajo conectada a red, como a un router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

Este método es muy utilizado para capturar nombres de usuario y contraseñas, que generalmente viajan claros (sin cifrar) al conectarse a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

Snooping

Los ataques de esta categoría tienen el mismo objetivo que el *sniffing*, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante captura los documentos, mensajes de e-mail y otra información guardada, descargando en la mayoría de los casos esa información a su propia computadora.

El *Snooping* puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos mas sonados de este tipo de ataques fueron el robo de un archivo con más de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de informes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

Tampering o Data Diddling

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de ejecutar cualquier comando y alterar o borrar cualquier información que puede incluso terminar en la destrucción total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite apagar el sistema por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por *insiders* o *outsiders*, generalmente con el propósito de fraude o dejar fuera de servicio un competidor.

Son innumerables los casos de este tipo, como empleados bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal.

Múltiples sitios web han sido víctimas del cambio de sus páginas principales por imágenes terroristas o humorísticas, o el reemplazo de versiones de software para descargar por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos, etc.).

La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de Back Orifice y NetBus, de reciente aparición.

Spoofing

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de *sniffing* o *tampering*. Una forma común de *spoofing*, es conseguir el nombre y contraseña de un usuario legítimo para, una vez en el sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails.

El intruso usualmente utiliza un sistema para obtener información y conectarse a otro, y luego utiliza éste para entrar en otro, y en otro. Este proceso, llamado "Looping", tiene la finalidad de imposibilitar la identificación y la ubicación del atacante. El camino

tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del *looping* es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un *insider*, o por un estudiante a miles de km. de distancia, pero que ha tomado la identidad de otros.

El *looping* hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al *spoofing*. Con el IP *spoofing*, el atacante genera paquetes de Internet con una dirección de red falsa en el campo Origen, pero que es aceptada por el destinatario del paquete.

El envío de falsos e-mails es otra forma de *spoofing* permitida por las redes. Aquí el atacante envía e-mals a nombre de otra persona. Tal fue el caso de una universidad en USA que en 1998 debió reprogramar una fecha de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a los 163 estudiantes.

Muchos ataques de este tipo comienzan con **ingeniería social** (que se verá posteriormente), y la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica.

Jamming o Flooding

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra también *spoofing*). El sistema responde al mensaje, pero como no recibe respuesta, acumula *buffers* con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos nodos de Internet han sido dados de baja por el "ping de la muerte", una versión-trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta activo en la red, el ping de la muerte causa el reinicio o el apagado instantáneo del equipo.

Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servidores destino.

Bombas Lógicas

Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificará la información o provocará el cuelgue del sistema.

Ingeniería Social

Básicamente convencer a la gente de que haga lo que en realidad no debería. Por

ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la contraseña con alguna excusa convincente. Nunca se deben de subestimar este tipo de ataques.

Difusión de Virus

Si bien es un ataque de tipo *tampering*, difiere de éste porque puede ser introducido en el sistema por un dispositivo externo (disquetes) o través de la red (e-mails u otros protocolos) sin intervención directa del atacante. Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse a través de una LAN o WAN rápidamente, si es que no esta instalada una protección antivirus en los servidores, estaciones de trabajo, y los servidores de e-mail.

Cientos de virus son descubiertos mes a mes, y técnicas más complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada. Por eso es indispensable contar con una herramienta antivirus actualizada y que pueda responder rápidamente ante cada nueva amenaza.

El ataque de virus es el más común para la mayoría de las empresas, que en un gran porcentaje responden afirmativamente cuando se les pregunta si han sido víctimas de algún virus en los últimos 5 años.

Explotación de errores de diseño, implementación u operación

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" han sido descubiertas en aplicaciones de software, sistemas operativos, protocolos de red, navegadores de Internet, correo electrónico y toda clase de servicios en LANs o WANs.

Hay multitud de ataques basados en explotar las vulnerabilidades del protocolo TCP/IP, entre ellos la Predicción de Números de Secuencia TCP (“ISN prediction / IP spoofing”), base del famoso ataque de Kevin Mitnick al San Diego Supercomputer Center de 1994, en el cual se suplantaba una conexión de una máquina privilegiada interna desde una máquina externa para ganar un acceso de confianza, o el secuestro de sesiones ("Session hijacking").

Sistemas operativos abiertos como Unix tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados, como Windows. Constantemente encontramos en Internet avisos de nuevos descubrimientos de problemas de seguridad (y herramientas de *hacking* que los explotan), por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades y pueden diagnosticar un servidor, actualizando su base de datos de tests periódicamente, además de normas y procedimientos de seguridad en los procesos de diseño e implementación de proyectos de informática.

Obtención de Contraseñas

Este método (usualmente denominado *cracking*), comprende la obtención "por fuerza bruta" u otros métodos más inteligentes, de aquellas contraseñas que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchas contraseñas de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca

la cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles contraseñas hasta encontrar la correcta.

Es muy frecuente *crackear* una contraseña explotando agujeros en los algoritmos de cifrado utilizados, o en la administración de las contraseñas por parte la empresa.

Por ser el uso de contraseñas la herramienta de seguridad más cercana a los usuarios, es aquí donde hay que poner énfasis en la parte "humana" con políticas claras (¿cómo se define una contraseña?, ¿a quién se esta autorizado a revelarla?) y una administración eficiente (¿cada cuanto deben de cambiarse?)

No muchas organizaciones están exentas de mostrar contraseñas escritas y pegadas en la base del monitor de sus usuarios, u obtenerlas simplemente preguntando al responsable de cualquier PC cual es su contraseña.

Otras formas de "colgar" un equipo

Otro método para colgar un equipo es el denominado "*Land attack*", en el que se genera un paquete con direcciones IP y puertos de origen y destino idénticos. Existen diferentes variantes para este ataque. Una de ellas usa idénticas direcciones IP de origen y destino, pero no números de puertos.

Un ataque característico de los equipos con Windows es el *Supernuke* (llamado también a veces *Winnuke*), que hace que los equipos que escuchan por el puerto UDP 139 se cuelguen. NetBIOS es un protocolo integral para todas las versiones en red de Windows. Para transportar NetBIOS por IP, Microsoft ideó el Windows Networking (Wins), un esquema que enlaza el tráfico NetBIOS a puertos TCP y UDP 137, 138 y 139. Al enviar a estos puertos fragmentos UDP, se pueden arruinar equipos Windows que no estén arreglados o disminuir la velocidad del equipo durante un largo tiempo.

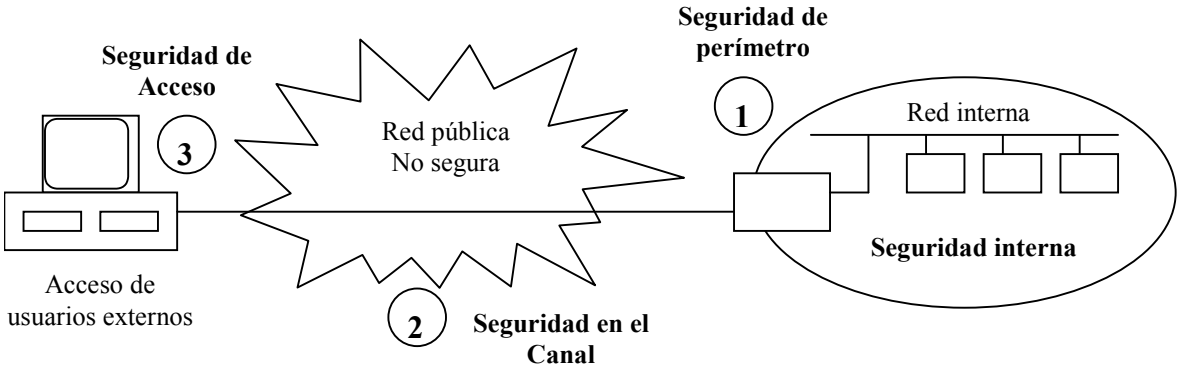
Teardrop data de fines de 1997. Al igual que el Supernuke, los ataques Teardrop 1 y Teardrop 2 afectan a fragmentos de paquetes. Algunas implementaciones de colas IP no vuelven a agrupar correctamente los fragmentos que se superponen, haciendo que el sistema se cuelgue. Windows NT 4.0 de Microsoft es especialmente vulnerable a este ataque, aun cuando se ha aplicado el Service Pack 3. La empresa hizo un parche del Teardrop 1 en mayo de 1997, pero se mostró vulnerable al Teardrop 2, que supuso colocar una bandera de "urgente" en la cabecera de un fragmento TCP. Hasta el lanzamiento de un *hot fix* en enero de 1998.

2.2 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**. El problema de seguridad puede aparecer dentro de la propia empresa, en su red interna, provocado bien por empleados 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**.

2.3 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 existen. 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 Auditorias de Seguridad. Estas pueden ser llevadas a cabo por personal de la propia empresa o por consultorías externas. Una Auditoria 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 contraseñas 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 contraseña 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 contraseñas 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 el, 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 contraseña de la cuenta del usuario administrador del sistema en caso de necesidad. (Guardar bajo llave la contraseña del sistema, dividirla en partes y repartirla entre varias personas de manera que juntándose puedan administrar el sistema, etc.)

3 SEGURIDAD DE PERÍMETRO. CORTAFUEGOS

3.1 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 autorizado desde y hacia el exterior. Otra razón importante es que pueden proporcionar un bastión en el que centrar los esfuerzos de administración y auditoría. 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.

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. Cualquier empleado utilizando un módem para hacer una conexión a Internet mediante el protocolo PPP y comprometer la seguridad de toda la red.

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 (toda es una *zona de riesgo*). 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* o *telnet* 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 al propio cortafuegos o a un reducido grupo 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.

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 contarfuegos 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 o contra ataques debidos a los datos que se transfieren salvo que se combine con algún tipo de software antivirus. 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.

3.2 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. 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.

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 (situación muy poco recomendable). 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 ejecutando los usuarios. 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.

3.3 Capa de trabajo del cortafuegos.

También podemos clasificar los cortafuegos por la capa de la pila de protocolos en la que trabajen.

3.3.1 Cortafuegos a nivel de Red

Por lo general se trata de un encaminador (router) o una computadora especial que examina las características de los paquetes IP para decidir cuáles deben pasar y cuáles no. Por ejemplo se podría configurar el encaminador para que bloquease todos los mensajes que provengan del sitio de un determinado competidor, así como todos los mensajes destinados al servidor de ese competidor. Los profesionales de las redes a menudo denominan a este proceso como lista negra.

Normalmente se suele configurar un encaminador para que tenga en cuenta la siguiente información para cada paquete antes de decidir si debe enviarlo:

- Dirección IP de origen y destino (cabecera IP, nivel 3)
- Puerto origen y destino (campo de datos IP, cabecera nivel 4)
- Protocolo de los datos (TCP,UDP o ICMP) (cabecera IP, nivel 3)
- Si el paquete es inicio de una petición de conexión (campo de datos IP, cabecera nivel 4)

Si se instala y se configura correctamente un cortafuegos a nivel de red, éste será muy rápido y casi totalmente transparente para los usuarios.

Para servidores Linux un software que permite realizar funciones de filtrado para implementar un cortafuegos a nivel de red es el IP Chains o IP Tables.

3.3.2 Cortafuegos a nivel de circuito

Se trata de una versión avanzada de los cortafuegos vistos en el punto anterior que trabajan en la capa de transporte. La seguridad en este caso está basada en el establecimiento, seguimiento y liberación de las conexiones que se realizan entre las máquinas internas y externas. Observan la conveniencia o no de la existencia de esas conexiones en función del tipo de aplicación que realiza la conexión y la procedencia de la petición. Además, realizan seguimiento en los números de secuencia de la conexión buscando aquellos paquetes que no corresponden con conexiones establecidas. Durante este seguimiento, se establece un circuito virtual entre el cliente y el servidor a través del cortafuegos, que hace transparente la existencia de dicho cortafuegos.

3.3.3 Cortafuegos a nivel de aplicación

Suele ser un ordenador que ejecuta software de servidor Proxy. La palabra "proxy" significa "actuar por poderes" o "en nombre de otro". Los servidores proxy hacen precisamente esto, se comunican con otros servidores del exterior de la red en nombre de los usuarios.

En otras palabras un servidor proxy controla el tráfico entre dos redes estableciendo la comunicación entre el usuario y él mismo y entre él mismo y el ordenador destino. De este modo la red local queda oculta para el resto de Internet. Un usuario que acceda a Internet a través de un servidor proxy aparecerá para los otros ordenadores como si en realidad fuera el servidor proxy (se muestra la dirección IP de éste). Esto combinado con un servicio NAT, puede hacer completamente invisibles las direcciones IP de los ordenadores de la red interna hacia el exterior.

Como trabaja a nivel de aplicación, este tipo de cortafuegos es más seguro y potente, pero también menos transparente y rápido que un encaminador. Existen servidores proxy disponibles para diferentes servicios como HTTP, FTP, Gopher, SMTP y Telnet. Es necesario configurar un servidor proxy diferente (aunque pueden residir en la misma máquina) para cada servicio que se desee proporcionar. Dos de los servidores proxy más populares para las redes basadas en UNIX y Linux son TIS Internet Firewall Toolkit y SOCKS. Para servidores Windows NT tanto el Internet Information Server (IIS) de Microsoft, como el Commerce Server de Netscape incluyen servidores proxy.

Al implementar un servidor proxy a nivel de aplicación, los usuarios de la red deberán utilizar programas clientes que puedan trabajar con un proxy. Los diseñadores han

creado muchos protocolos TCP/IP, como HTTP, FTP y otros, pensando en la posibilidad de utilizar un proxy. En la mayoría de los navegadores web, los usuarios pueden establecer fácilmente sus preferencias de configuración para seleccionar el servidor proxy a utilizar.

Desgraciadamente no todos los protocolos están pensados para utilizar un proxy, y en esos casos puede ser necesario seleccionar las aplicaciones para Internet según su compatibilidad un protocolo proxy habitual, por ejemplo SOCKS.

Como contrapartida a todos los posibles inconvenientes, el software de proxy se pueden combinar con la utilización de antivirus para detectar, dentro de los contenidos que se intercambian las aplicaciones a través del proxy, las huellas de virus en los mensajes de correo, documentos, applets embebidos en páginas HTML (Java, ActiveX, …), ejecutables, etc. y eliminarlos o advertir del riesgo al usuario.

3.4 Topologías de cortafuegos

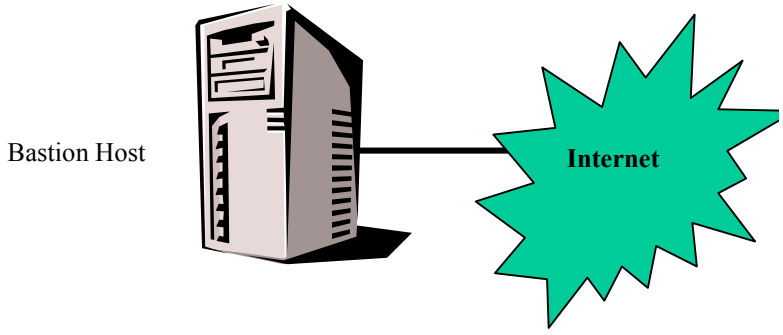
Aunque el propósito de todos los cortafuegos es el mismo, existen diferencias en sus topologías y prestaciones. Los siguientes son algunos ejemplos de las múltiples posibilidades existentes:

- Bastión Host
- Encaminador con filtrado (Screening Router)
- Host con doble conexión (Dual-Homed Host)
- Cortafuegos mediante filtrado de host (Screened Host)
- Cortafuegos mediante filtrado de subred (Screened Subnet)

3.4.1 Bastion Host

Son sistemas identificados por el administrador de la red como puntos clave en la seguridad de la red. Son auditados regularmente y pueden tener software modificado para filtrar y bloquear determinados intentos de conexión, trazar las comunicaciones y reparar fallos de seguridad del sistema.

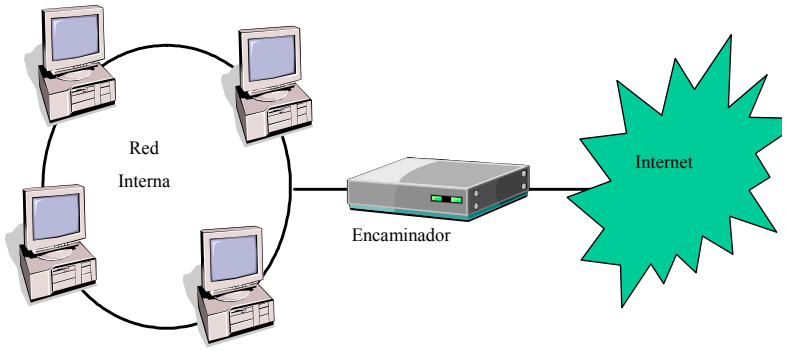
Un ejemplo simple es el caso de la instalación de un software de cortafuegos personal en el equipo del usuario. Mediante este tipo de software el usuario puede controlar, bloquear y filtrar el tráfico de datos que entra y sale por cada uno de los puertos de comunicación de su ordenador personal, tanto si utiliza aplicaciones cliente, como si ofrece servicios a equipos remotos.



3.4.2 Encaminador con filtrado (Screening Router)

Son un componente básico de la mayor parte de los cortafuegos. Pueden ser un router comercial o basado en un ordenador convencional, con capacidad para filtrar paquetes. Tienen la capacidad para bloquear el tráfico entre redes o nodos específicos basándose en direcciones y puertos TCP/IP (trabajan a nivel de red). Algunos cortafuegos sólo consisten en un "screening router" entre la red privada e Internet.

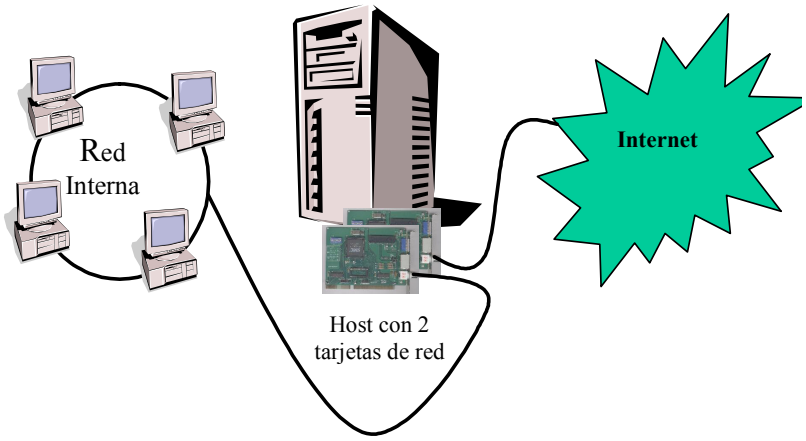
En general permite la comunicación entre múltiples nodos de la red protegida y de Internet. La zona de riesgo es igual al número de nodos de la red protegida y el número y tipo de servicios para los que se permite el tráfico. Es difícil controlar los daños que pueden producirse dado que el administrador 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, aunque algunos poseen capacidades de registro de eventos para paliar esto. 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.

3.4.3 Host con doble conexión (Dual-Homed Host)

Algunos cortafuegos son implementados sin necesidad de un screening router. Para ello se conecta un servidor mediante dos tarjetas independientes a la red que se quiere proteger y a Internet, desactivando las funciones de reenvío TCP/IP. Este dispositivo puede ser un bastion host y funcionar como servidor (Web, FTF, …) tanto para la red interna como para la red externa. Los hosts de la red privada pueden comunicarse con el bastión host, 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. El permiso para el uso de cada aplicación se suele habilitar instalando el software de proxy adecuado para cada una de ellas.

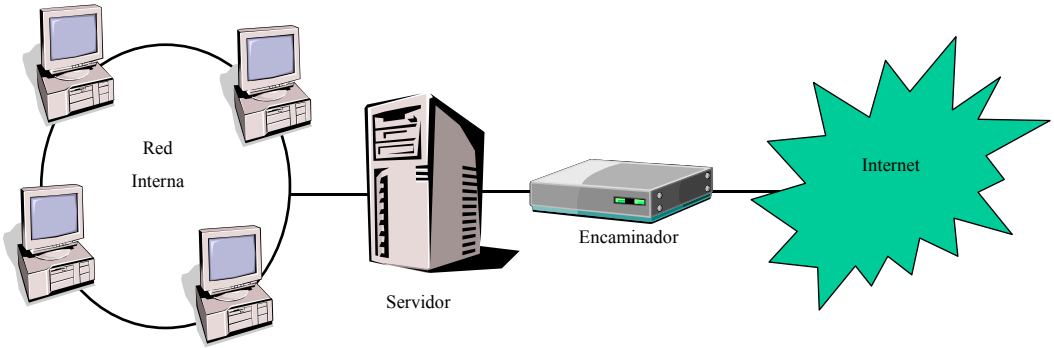
En el segundo caso, el acceso de los usuarios a Internet es más sencillo, pero la seguridad puede verse comprometida. Si un hacker gana acceso a una cuenta de usuario, tendrá acceso a toda la red protegida. La cuenta de un usuario puede verse comprometida por elegir una contraseña sencilla de adivinar, 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.

3.4.4 Cortafuegos mediante filtrado de Host (Screened Host)

Es la configuración de cortafuegos más común. Está implementada usando un bastion host y un screening rotuer. 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.

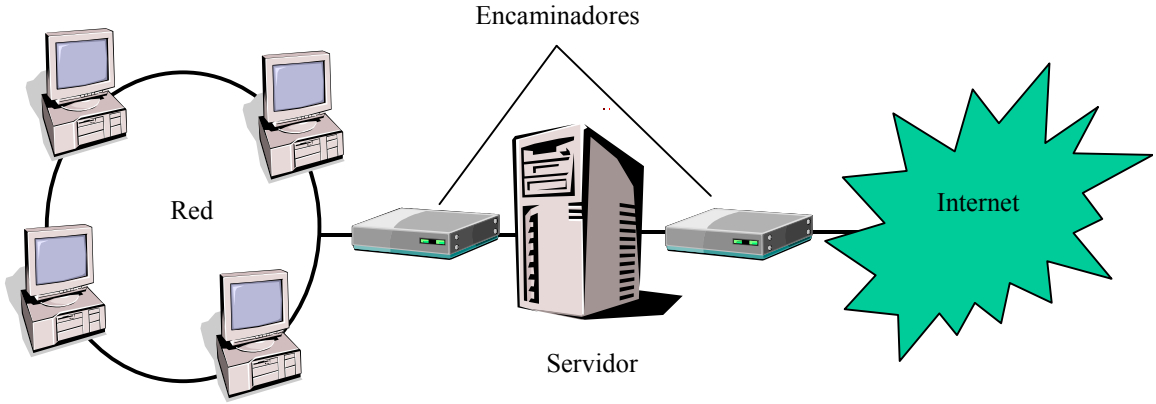


Como el bastion host está en la red privada, la conectividad para los usuarios es muy buena, eliminando los problemas que suelen aparecer al tener definidas rutas extrañas. Si la red privada es una red local virtual extensa, el esquema funciona sin necesidad de cambios en las direcciones de la red local 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 host de doble conexión.

3.4.5 Cortafuegos mediante filtrado de subred (Screened Subnet)

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.

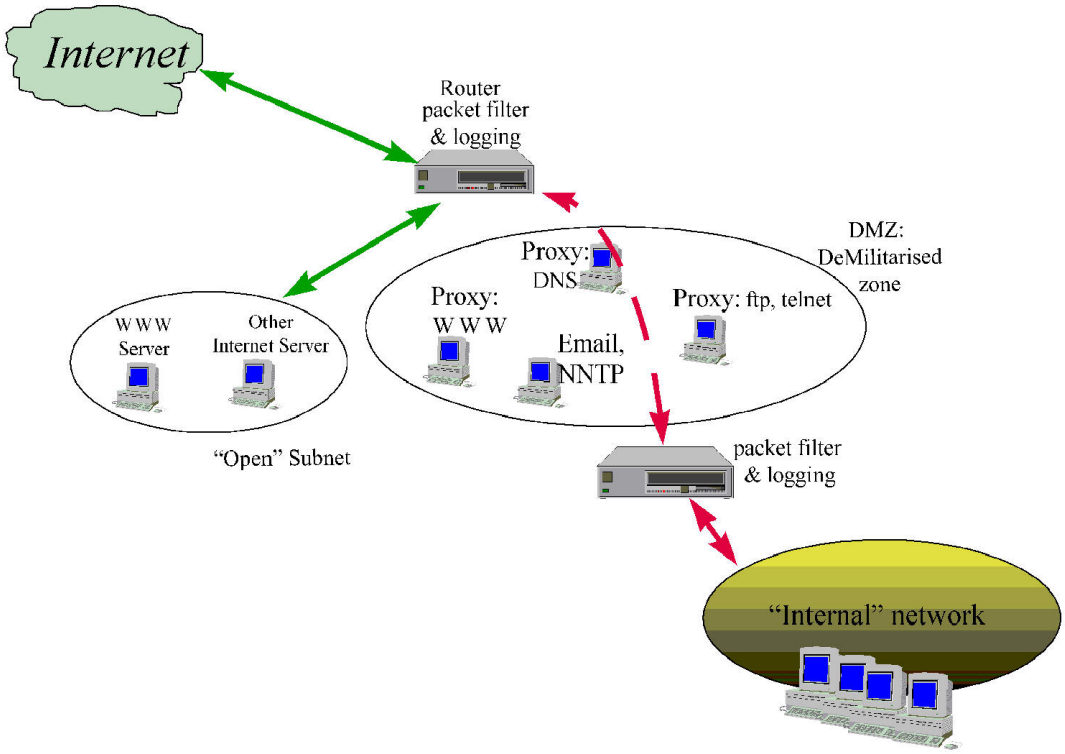


En la subred suele haber un bastion host como único punto de acceso a la misma. En este caso, la zona de riesgo es pequeña y está formada por el propio bastion host, los screening routers que filtran el tráfico y proporcionan las conexiones entre Internet, la sudred y la red privada. La facilidad de 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, la hacker debe reconfigurar el tráfico en tres redes, sin desconectarlas, sin dejarse encerrado a si 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.

La subred que incluye el cortafuegos y los encaminadores se denomina Zona Neutra o Zona Desmilitarizada *(Demilitarized Zone - DMZ)*. En esta zona desmilitarizada pueden encontrarse más servidores, bien orientados a dar servicios a usuarios que acceden desde la red externa (red abierta), o bien para facilitar los servicios de proxy y el acceso a internet a los usuarios de la red interna. Estos servicios pueden residir en una misma máquina, el propio bastión host, o en varias.



3.5 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.

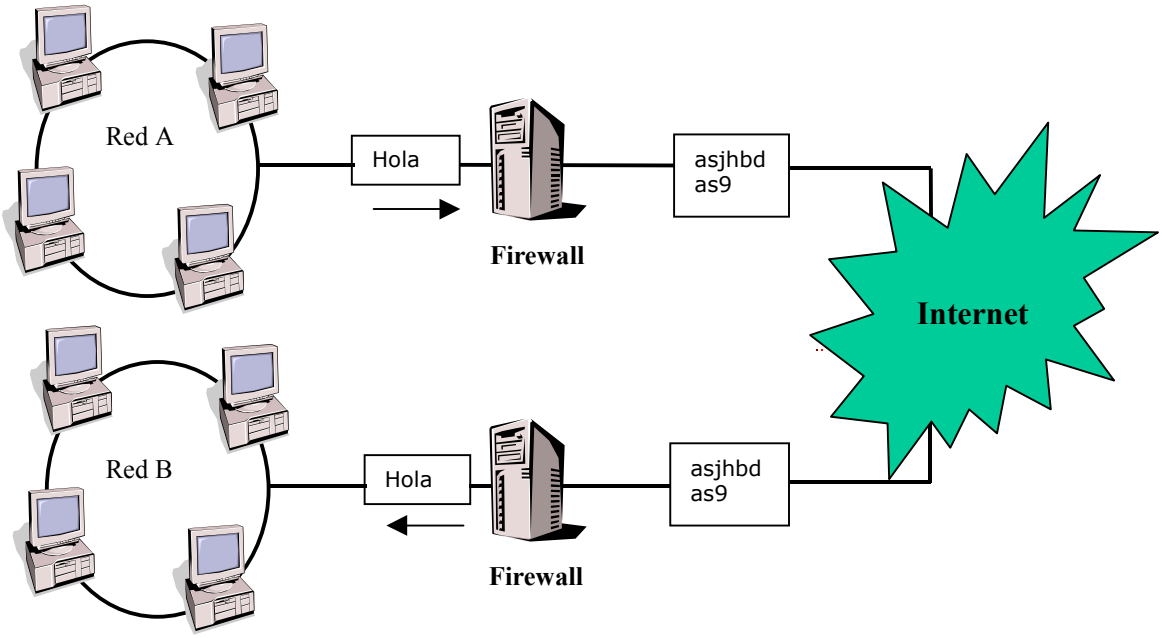
Otro aspecto fundamental es que un cortafuegos no puede ser considerado como una vacuna. No debe instalarse un determinado tipo de cortafuegos porque para alguien sea *suficientemente seguro*. Dicho concepto debe ser resultado de un análisis del coste de implantación, administración, nivel de protección 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.

3.6 Codificación en Cortafuegos. Las VPN.

Es posible utilizar los cortafuegos para conectar entre sí dos LAN de manera segura y transparente, es decir: los usuarios verán ambas redes como la misma LAN o como si

estuvieran unidas entre sí directamente (a través de puentes o conmutadores), y además los datos que se intercambien ambas redes viajarán cifrados por Internet, asegurando su privacidad.

Esta configuración se conoce como Red Privada Virtual o VPN.



3.7 *Túneles en Cortafuegos*

Con el rápido crecimiento del mercado de intranets, muchas empresas han descubierto la necesidad de crear túneles en sus cortafuegos que permitan a los usuarios autorizados acceder a los recursos que de otro modo serían inaccesibles. En otras palabras, pueden bloquear el sitio FTP al exterior, a los usuarios de Internet y permitir que los usuarios de su intranet se conecten a él desde sus casas.

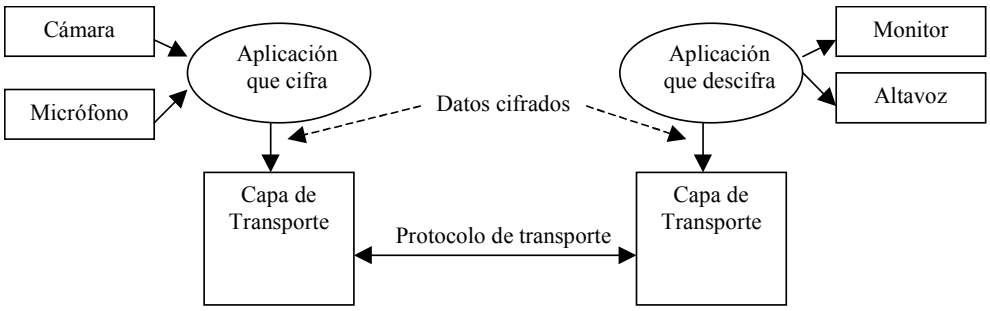
Este proceso se conoce como *tunneling* y el cortafuegos debe incluir un mecanismo que permita, de manera segura, al cliente abrir un túnel a través de él.

Por ejemplo y debido al amplio uso de la capa de socket seguro SSL en los servidores seguros y a que en las intranets muchas conexiones se producen mediante servidores seguros, SSL debe ampliar el protocolo de proxy Web para que el cliente SSL pueda abrir el túnel. Sin embargo esta técnica tiene también sus inconvenientes.

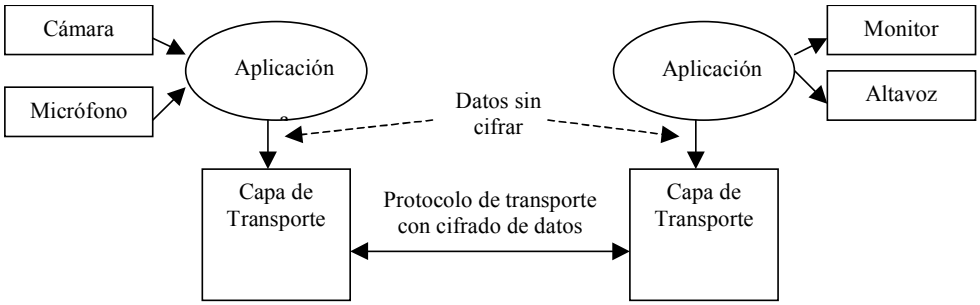
4 SEGURIDAD EN EL CANAL

Aunque los usuarios de las computadoras que son extremo de una comunicación puedan estar tranquilos en cuanto a la seguridad de estas computadoras, 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.

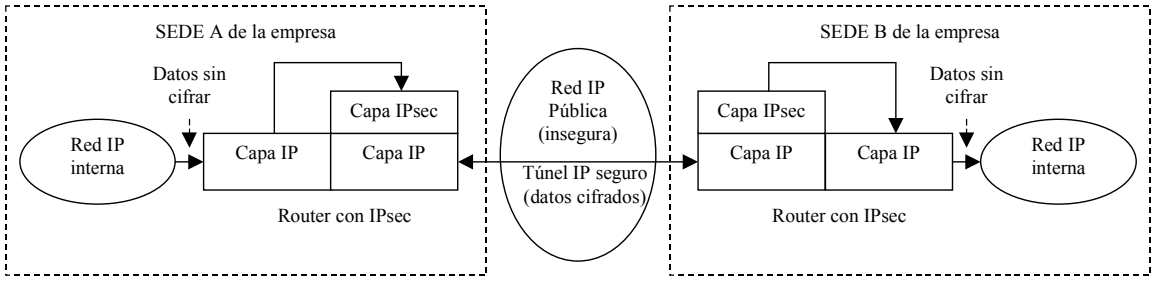
El cifrado de los datos puede aplicarse a distintos niveles:



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

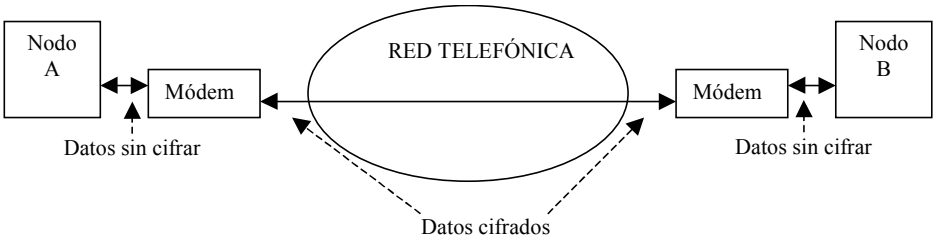


- **Transporte**: La capa de transporte puede utilizar un protocolo que cifre el campo de datos de cada segmento que envía (TPDU) donde van los datos del usuario. Para ello ambas entidades de transporte, a uno y otro extremo han de ser capaces de negociar ese protocolo con cifrado de datos (por ejemplo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



- **Red**: Se pueden utilizar protocolos de red que utilicen cifrado de datos, de manera que el campo de datos de las unidades que transmite el protocolo van cifrados. 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 el cifrado 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 cifrado dentro del campo de datos de los datagramas IP convencionales que atraviesan la red pública.



- **Enlace**: En este caso el cifrado/descifrado lo 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 cifrar la información que transmiten cuando dialogan con otro módem con las mismas capacidades.

4.1 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.

4.1.1 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.

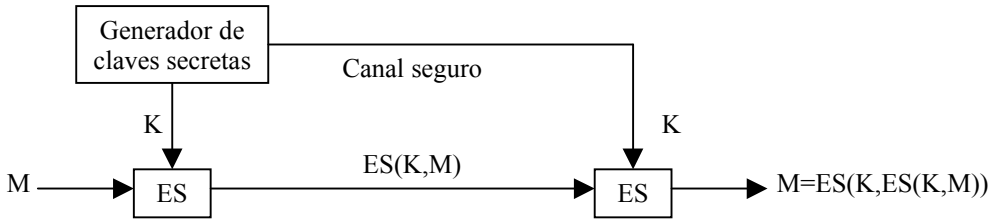
4.1.2 Cifrado por transposición

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.

4.2 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 a 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.



4.2.1 Data Encryption Standard (DES)

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 2^{56}, 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 [STALLINGS 97], 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 (ver actualmente el algoritmo AES).

4.2.2 International Data Encryption Algorithm (IDEA)

IDEA es un algoritmo de cifrado por bloques patentado por la firma suiza Ascom. Sin embargo su uso no comercial está autorizado siempre que se solicite permiso.

Se trata de un algoritmo basado en el estándar DES, siendo tan rápido como éste (e incluso más si se implementa en hardware) y bastante más seguro. Ha superado todos los intentos de la comunidad científica de romper su cifrado hasta el momento.

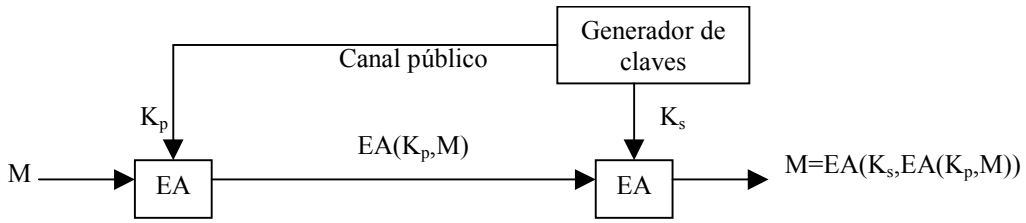
IDEA utiliza 52 subclaves de 16 bits y cifra en 8 pasos. Cada bloque se divide en cuatro cuartetos de 16 bits y se utilizan 3 operaciones distintas para combinar dos valores

de 16 bit produciendo un resultado de también 16 bit: XOR, suma (modulo 256) y una multiplicación con características especiales.

IDEA evita el uso de tablas de búsqueda o cajas de sustitución y se emplea, entre otras aplicaciones, en el popular programa de cifrado PGP.

4.3 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 una 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 $MOD(D\cdot E,X)=1$, 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: $C=MOD(M^E,N)=MOD(19^5,119)=66$.

h) Para descifrar: $M=MOD(C^D,N)=MOD(66^{77},119)=19$.

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 un 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 [STALLINGS 97]. 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.

5 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.

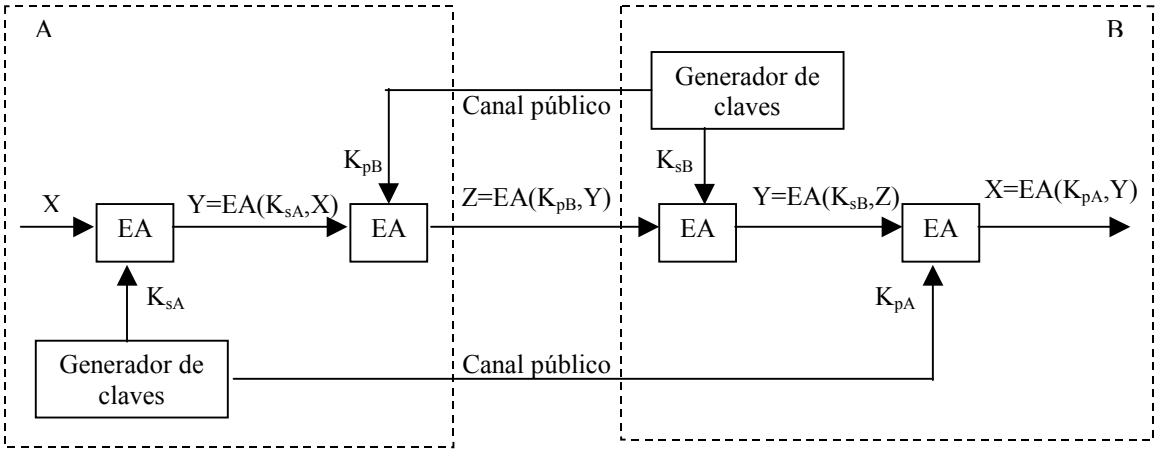
5.1 Autentificación mediante firma digital

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 $M=EA(K_p,EA(K_s,M))$.

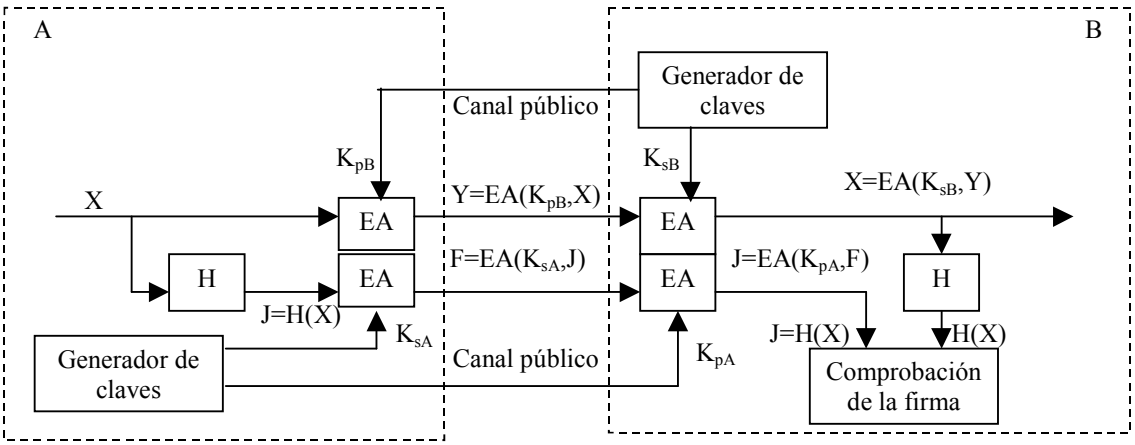
El usuario A, emisor del mensaje X, lo firmará cifrándolo con su clave secreta K_{sA}. Si se transmitiese así el mensaje $Y=EA(K_{sA},X)$, cualquier usuario que conozca la clave publica de A, K_{pA}, podría descifrarlo. Por ello A hace un segundo cifrado utilizando la

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.

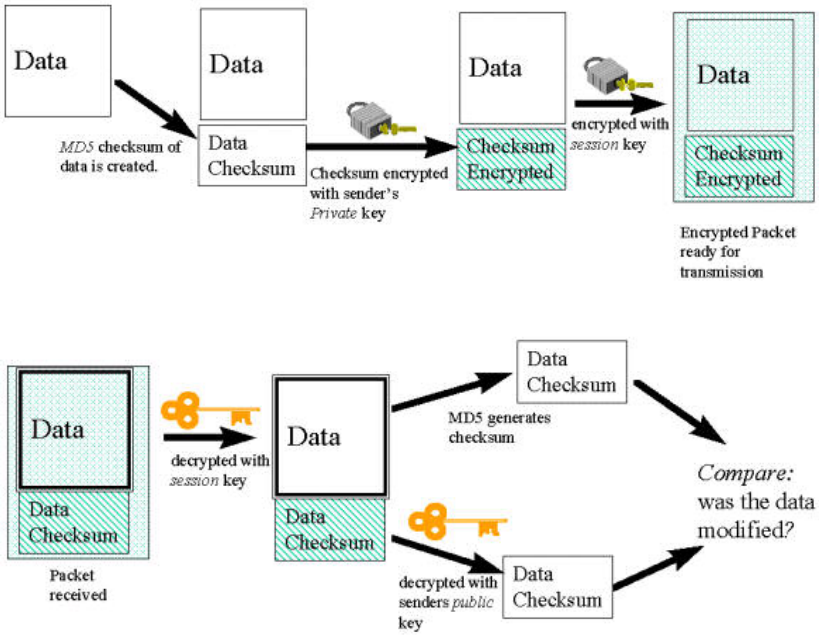


Un algoritmo muy conocido para generar una firma digital para un conjunto de datos dado es el MD5.

MD5 fue desarrollado por el Profesor Ronald L. Rivest en el MIT y la descripción de su funcionamiento puede encontrarse en la RFC 1231. El algoritmo genera una firma de 128 bits y se conjetura que es computacionalmente imposible generar dos mensajes cuya firma MD5 coincida, así como reproducir el mensaje original a partir de ella.

El algoritmo está orientado a producir firmas para mensajes largos antes de su cifrado y es mucho más fiable que el checksum o cualquier otro método tradicional.

En las siguientes figuras se muestra un ejemplo de funcionamiento de la firma digital de un mensaje utilizando el algoritmo MD5.



5.2 *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

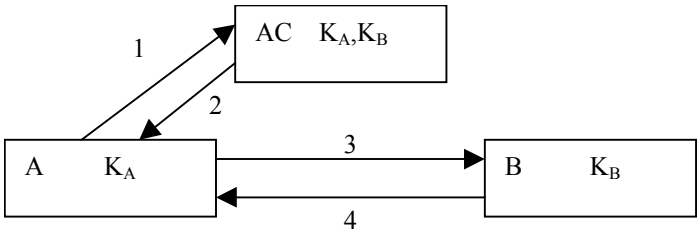
actualizadas cuantas veces se quiera de forma segura a través de la misma red. De la misma manera se tendrá seguridad sobre la autenticidad del interlocutor.

5.2.1 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 ha 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}.



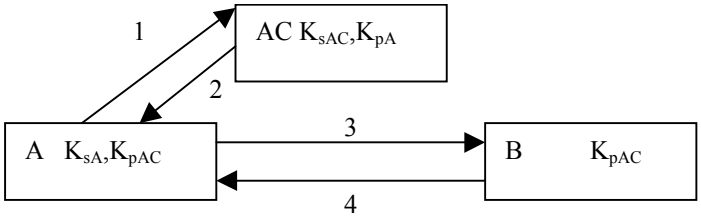
5.2.2 Emisión de certificados en el cifrado asimétrico

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 autentificarse 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 $M=[ID_A,K_{pA},T]$ (donde ID_A 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 B sin cifrar 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 autentificada por una firma que sólo ha podido generar la AC.

Hay que advertir que el mismo procedimiento es válido para que B autentifique 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.



6 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.

6.1 Compartamentalización

Los repetidores y conmutadores que disponen de la posibilidad de filtrar el tráfico de red que circula por sus puertos permiten la compartamentalización 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 anti-escuchas o determinar que equipo es el legítimo usuario de un puerto frente a posibles intrusos.

También colaboran a la compartamentalización 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.

6.2 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 contraseñas de usuarios de la red. La compartamentalización 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.

6.3 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, SAMBA (carpetas compartidas). 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 revenir 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. 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 auditoría, ya que presentan un fácil punto de penetración.

7 BIBLIOGRAFÍA

Bibliografía consultada para la realización de este capítulo:

[STALLINGS 97]
Stallings, W. (1997).
Comunicaciones y redes de computadores, 5ª ed.
Prentice Hall Iberia.

[TANENBAUM 96]
Tanenbaum, A.S. (1996).
Computer Networks. (Third Edition).
Prentice-Hall.

[HALSALL 95]
Halsall, F. (1995).
Data Communications, Computer Networks and Open Systems.
Addison-Wesley.

[FREER 88]
Freer, J. (1988).
Introducción a la tecnología y diseño de Sistemas de Comunicaciones y Redes de Ordenadores.
Anaya Multimedia.

[ALONSO 95]
Alonso, J. M. (1995).
Protocolos de comunicaciones para sistemas abiertos.
Addison-Wesley Iberoamericana.

[RFC-2196]
B. Fraser Editor (1997)
Site Security Handbook

[BELLOVIN 89]
S. Bellovin (1989)
Security Problems in the TCP/IP Protocol Suite
Computer Communication Review, vol 19, 2, pp. 32-48

[KLANDER 98]
Klander, L. (1998).
A Prueba de Hackers
Anaya Multimedia

[BRENT 92]
D. Brent Chpman (1992)
Network (In)Security Through IP Packet Filtering

Proc. Of the 3rd USENIX UNIX Security Symposium

[RANUM 93]
M. Ranum
Thinking About Firewalls

- Lista de distribución de la seguridad en Unix (restringida):
  solicitud a security-request@cpd.com
- El Foro de los Riesgos (ACM): http://www.acm.org
- Lista Virus-L: comp.virus o por subscripción
- Lista BugTraq:
  bugtraq-request@crimelab.com
  texto: subscribe bugtraq Nombre Apellido
- Lista CERT (Equipo de Respuesta de Emergencia Informática): http://www.cert.org
- Lista TCP/IP comp.protocols.tcp-ip o por subscripción
- Lista SUN-NETS: estaciones SUN, NFS, NIS y DNS
  sun-netsr-equest@umiacs.umd.edu
- Grupos alt.security y comp.security