



**¿CÓMO FUNCIONA LA SEGURIDAD EN INTERNET?**

**MIQUEL SORIANO**

## Índice

<b>ÍNDICE</b> .....	<b>2</b>
<b>1. INTRODUCCIÓN</b> .....	<b>5</b>
1.1 INTRODUCCIÓN .....	5
1.2 SOLUCIONES AL PROBLEMA .....	7
<b>2. ¿CÓMO PROTEGER EL ORDENADOR?</b> .....	<b>8</b>
2.1 INTRODUCCIÓN .....	8
2.2 ANTIVIRUS .....	9
2.3 PROGRAMAS ESPÍA O SPYWARE .....	9
2.4 FIREWALL PERSONAL .....	10
2.4.1 Instalación.....	10
2.5 REGLAS BÁSICAS .....	11
<b>3. AMENAZAS, SERVICIOS Y MECANISMOS DE SEGURIDAD EN REDES DE COMUNICACIÓN</b> .....	<b>12</b>
3.1 INTRODUCCIÓN .....	12
3.2 ATAQUES.....	12
3.3 ATAQUES PASIVOS.....	15
3.4 ATAQUES ACTIVOS.....	15
3.5 ATAQUES DE INGENIERÍA SOCIAL.....	16
3.5.1 Phishing .....	16
3.5.2 Virus.....	18
3.6 ATACANTES .....	20
3.7 MECANISMOS DE SEGURIDAD.....	21
3.8 SERVICIOS DE SEGURIDAD.....	22
<b>4. MECANISMOS CRIPTOGRÁFICOS</b> .....	<b>24</b>
4.1 INTRODUCCIÓN .....	24
4.2 OBJETIVOS DE LA CRIPTOGRAFÍA .....	24
4.3 MÉTODOS CRIPTOGRÁFICOS.....	25
4.3.1 Criptografía moderna.....	26
4.3.1.1 Métodos simétricos o de clave privada.....	26
4.3.1.2 Métodos asimétricos o de clave pública.....	26
4.3.2 Funciones Hash.....	28
4.3.3 Firma digital .....	28
4.3.3.1 Digital Signature Algorithm DSA.....	29
4.4 GESTIÓN DE CLAVES .....	30
4.4.1 Distribución de claves simétricas mediante técnicas asimétricas.....	30
4.4.2 Distribución de claves asimétricas.....	31
4.5 CERTIFICADOS.....	31
4.5.1 Generación y distribución de certificados.....	33
4.5.2 Validación de certificados.....	33

4.5.3	Revocación .....	34
<b>5.</b>	<b>CORTAFUEGOS E IDS. SEGURIDAD PERIMETRAL .....</b>	<b>35</b>
5.1	SISTEMAS FIREWALL (CORTAFUEGOS).....	35
5.2	DETECCIÓN DE INTRUSIONES .....	37
5.2.1	Clasificación de los Sistemas de Detección de Intrusos .....	39
5.2.1.1	Fuentes de información .....	39
5.2.1.2	Estrategia de Análisis .....	40
5.2.1.3	Respuesta .....	41
5.3	INTEGRACIÓN.....	41
<b>6.</b>	<b>SEGURIDAD EN SERVICIOS WEB .....</b>	<b>43</b>
6.1	INTRODUCCIÓN .....	43
6.2	CONCEPTOS BÁSICOS DE TLS .....	43
6.2.1	¿QUÉ ES EL PROTOCOLO TLS? .....	43
6.2.2	Algoritmos criptográficos soportados por TLS.....	44
6.2.3	El sub-protocolo de negociación o “handshake” .....	45
6.2.3.1	Proceso de autenticación del servidor .....	47
6.2.3.2	Técnica de ataque “man-in-the-middle” .....	48
6.2.3.3	Autenticación del cliente .....	48
6.2.4	Protocolo de registro: transferencia de datos.....	50
<b>7.</b>	<b>COMERCIO ELECTRÓNICO SEGURO .....</b>	<b>52</b>
7.1	VENTAJAS E INCONVENIENTES DEL COMERCIO ELECTRÓNICO .....	52
7.2	MODELOS DE COMERCIO .....	53
7.3	NECESIDADES, REQUISITOS Y RIESGOS .....	54
7.4	MÉTODOS DE PAGO Y SEGURIDAD: LOS PARTICIPANTES .....	54
7.4.1	Arquitectura lineal .....	55
7.4.2	Arquitectura triangular .....	56
7.4.3	Modelo 3 dominios.....	56
<b>8.</b>	<b>HERRAMIENTAS DEL HACKER .....</b>	<b>59</b>
<b>9.</b>	<b>ANEXO A. ALGORITMO CRIPTOGRÁFICO RSA .....</b>	<b>61</b>
9.1	INTRODUCCIÓN .....	61
9.2	GENERACIÓN DE CLAVES .....	61
9.3	CIFRADO DE MENSAJES .....	62
9.4	DESCIFRADO DE MENSAJES .....	62
<b>10.</b>	<b>ANEXO B. TIPOS DE FIREWALLS .....</b>	<b>64</b>
10.1	TIPOS DE FIREWALLS.....	64
10.2	FIREWALL DE FILTRADO DE PAQUETES.....	64
10.3	SERVIDORES PROXY .....	64
10.4	FIREWALLS DE INSPECCIÓN DE PAQUETES .....	65
10.5	FIREWALLS HÍBRIDOS .....	66
<b>11.</b>	<b>ANEXO C. SEGURIDAD A NIVEL DE RED. IPSEC (INTERNET PROTOCOL SECURITY) .....</b>	<b>67</b>

¿Cómo funciona la seguridad en Internet?

11.1	INTRODUCCIÓN .....	67
11.2	MODOS IPSEC.....	68
11.3	CABECERA DE AUTENTICACIÓN (AH: AUTHENTICATION HEADER).....	69
11.4	CONFIDENCIALIDAD (ESP: ENCAPSULATING SECURITY PAYLOAD).....	72
11.5	AUTENTICACIÓN MÁS CONFIDENCIALIDAD .....	75

# 1. Introducción.

## 1.1 Introducción

Desde hace ya unos años el uso de Internet se está extendiendo más que considerablemente por toda la población mundial, incluyendo la española. Internet es una herramienta muy práctica para encontrar información rápidamente, comunicarse mediante el correo electrónico con empresas o amigos, realizar compras sin moverse de casa, etc., y todo ello con un coste muy reducido.

El problema que ha traído consigo la rápida eclosión de Internet en la población es la consideración de que Internet es una red segura. Internet no es una red segura ya que no fue diseñada para serlo, si no que más bien fue creciendo y evolucionando tecnológicamente sin preocupaciones sobre la seguridad de la misma. Lo importante era conseguir que las comunicaciones funcionasen, la seguridad se intentaba implementar después, si es que se pensaba alguna vez en ella.

Cualquier usuario o entidad que desee conectarse a Internet debe disponer de una serie de mecanismos de seguridad sino quiere poner en riesgo su información privada. Hasta la aparición de Internet, la seguridad en las comunicaciones era una problemática reconocida, pero limitada a ámbitos militares o gubernamentales. El dominio de las comunicaciones seguras ha sido un factor fundamental en el desenlace de la mayoría de los conflictos militares del siglo XX, incluyendo la segunda guerra mundial. En este contexto, la seguridad de las comunicaciones es la forma de ocultar información crítica, y evitar cualquier posible manipulación. La situación actual es muy diferente, la seguridad es un aspecto crucial en las comunicaciones, y afecta a todos los usuarios. Este cambio se debe especialmente a los siguientes aspectos:

- El desarrollo de redes y sistemas de interconexión, que provoca que el número de personas que puedan acceder a cualquier sistema sea enorme.
- El uso de ordenadores y redes informáticas en el tratamiento y transmisión de información crítica, por ejemplo, transferencias bancarias, intercambio de datos en negocios, etc...
- La mayor facilidad para realizar un ataque, dado la disponibilidad de una tecnología más sofisticada.

Desde hace ya unos cuantos años han salido a la luz casos de delitos informáticos como utilización de números de tarjetas de crédito "robadas" en Internet, modificación de páginas web etc. Todo parece obra de los denominados hackers o crackers, individuos que se dedican a cometer actos ilegales en Internet, como la irrupción no autorizada en sistemas comerciales, el acceso al correo electrónico de individuales de manera no autorizada, etc. El problema no radica únicamente en los hackers, si no que también abarca un margen mucho más amplio. Debido a la naturaleza técnica de Internet, cualquier administrador de red de una compañía portadora de datos por donde pase nuestro correo electrónico o información como número de tarjeta VISA puede observar y modificar la misma sin problema, sin que ninguno de los dos extremos de la comunicación sepa jamás que ha ocurrido este hecho. Este hecho es sin duda grave ya que toda información sobre una persona debería ser privada a no ser que el propio individuo quiera facilitar esta información. Actualmente, enviar un correo electrónico por Internet es como enviar una carta sin sobre. Todo el mundo puede leerla. Es claro pues que se necesitan mecanismos de protección de la privacidad de las comunicaciones y de los sistemas conectados a Internet

Es difícil obtener estadísticas fiables del número de ataques con éxito. El problema de la inseguridad en redes es real. Las motivaciones actuales para atacar a una red son mucho mayores que hace años: fraudes, robo de recursos de telecomunicaciones, espionaje industrial, intrusión ilegal para conseguir beneficios económicos o políticos, etc. Además de estos ataques, las redes deben estar protegidas contra posibles accidentes, por ejemplo envío de información a direcciones erróneas, o fallos accidentales en la protección de información crítica. Aunque es una evidencia, es preciso señalar que el coste de la instalación de los sistemas de seguridad debe ser menor que el que supondría una serie de ataques continuados. Aunque hay muchos tipos de ataques a una red, sólo algunos son útiles al atacante, bien por falta de oportunidad, o bien por el coste que supone realizar ese ataque.

Al mismo tiempo, existen usuarios que ignoran los riesgos que supone no tomar precauciones. La evolución constante de la tecnología y el desarrollo de nuevas herramientas y técnicas de ataque, está constantemente cambiando y los intrusos están constantemente desarrollando nuevas herramientas y técnicas de forma que las soluciones de seguridad adoptadas correctamente en una fecha no se mantienen efectivas indefinidamente.

Otro factor que contribuye a la vulnerabilidad de la Internet es el rápido crecimiento y uso de la red, acompañado por un rápido desarrollo de servicios de red involucrando aplicaciones complejas. Con frecuencia, esos servicios no son diseñados, configurados, o mantenidos de forma segura. En la urgencia por obtener nuevos productos para el mercado, los desarrolladores no se aseguran adecuadamente que no estén repitiendo errores previos o introduciendo nuevas vulnerabilidades.

La siguiente tabla muestra un ejemplo de requisitos de seguridad que debe tener en cuenta una empresa, en función de su ámbito de actuación

<b>Entorno aplicación</b>	<b>Requisitos</b>
Todas las redes	Impedir accesos no autorizados ("Crackers")
Banca.	Protección manipulación de datos Identificación detallada de transacciones de clientes. Proteger PINs. Asegurar la privacidad de los clientes
Comercio electrónico	Asegurar el origen y la integridad de las transacciones. Proteger la privacidad colectiva. Establecer relaciones auténticas entre firmas electrónicas y transacciones.
Gobierno.	Proteger la información no clasificada pero crítica de posibles manipulaciones o revelaciones no autorizadas. Proporcionar firmas electrónicas a los documentos gubernamentales.

Empresas públicas de telecomunicaciones.	Restringir el acceso a funciones de administración a personas autorizadas. Protección contra servicios de interrupción. Protección de la privacidad de los clientes.
Redes privadas/colectivas.	Protección de la privacidad individual y del colectivas. Asegurar la autenticidad del mensaje.

*Tabla 1.1. Requisitos de seguridad en función del ámbito de actuación*

A lo largo de este documento se describirán los conceptos básicos de las tecnologías involucradas en la seguridad en redes y su uso en comercio electrónico.

## **1.2 Soluciones al problema**

Desde el punto de vista técnico podríamos dividir el problema en dos partes: la intrusión no autorizada en ordenadores y redes conectadas a Internet, y la confidencialidad y autenticación de los datos que transmitidos a través de Internet.

La intrusión no autorizada a redes privadas conectadas a Internet se soluciona con la instalación de las máquinas denominadas firewalls (cortafuegos), cuya misión es delimitar el tráfico de información que puede ir y venir de la red privada hacia Internet. De esta manera se imposibilita el hecho de que un hacker pueda entrar en un sistema privado por que simplemente no tiene conexión a el.

Para el segundo problema, la confidencialidad y autenticación de los datos que se transmiten por Internet se utilizan técnicas de criptografía. Estas técnicas también se pueden utilizar para autenticar que la persona y/o máquina que requiere un servicio o manda un correo electrónico es realmente ella y no cualquier otra, imposibilitando así la suplantación de identidad.

Así como no existe ningún estándar de cómo implementar un firewall, los protocolos y algoritmos utilizados para el cifrado de los datos son estándares abiertos y libres. Es decir, cualquier individuo u organización puede disponer de las características de estos algoritmos para poder implementarlos y de esta manera se asegura la compatibilidad entre diferentes soluciones programadas.

## 2. ¿Cómo proteger el ordenador?

### 2.1 Introducción

Navegar por Internet tiene muchas ventajas, pero los riesgos de una falta de protección en el ordenador pueden ser considerables. Las medidas de seguridad a aplicar dependen del tipo e importancia de información que debe ser protegida. A continuación se detallan algunas:

- Realizar copias de seguridad.
- No guardar nada confidencial en directorios compartidos de programas P2P como eMule, eDonkey, etc...
- Instalar un antivirus.
- Apagar el ordenador siempre que no se esté utilizando.
- Extremar el cuidado en sistemas con IP fijas (ADSL).
- Instalar el software de firewall personal, preferentemente con sistema de detección de intrusos. (Para usuarios expertos)
- No instalar software de fuentes no conocidas.
- No compartir discos o impresoras en Internet, especialmente directorios compartidos con programas P2P.

Para proteger toda la información y los programas que han ido introduciéndose en el ordenador debemos realizar copias de seguridad y mantenerlas siempre actualizadas. Estas copias permiten recuperar los datos en caso de pérdidas provocadas por fallos de hardware o en caso de indisponibilidad de acceso a los mismos. Existen diferentes modos de realizar las copias de seguridad, pero para un uso no profesional basta con realizar una copia cada varios días en soporte externo (CD-ROM o DVD, memoria USB, ZIP, etc.).

Es importante no guardar la copia de seguridad en el mismo lugar donde tenemos el ordenador, ya que en caso de accidente o robo podríamos perder ambas cosas. Es muy recomendable tener siempre a mano un disco de arranque y, por si fuera necesario, el sistema operativo para instalar. Con éste es posible, en algunas ocasiones, corregir un error o, al menos, salvar la información nueva que no se haya registrado en la última copia de seguridad.

Uno de los elementos que protegen nuestro ordenador de posibles intrusiones es la contraseña. Es muy aconsejable usarla y procurar que no la sepa nadie que no deba tener acceso a ella. Para que resulte realmente efectiva deben tenerse en cuenta algunas recomendaciones:

- No escribir contraseñas en papel ni en documentos del ordenador.
- Cambiar de contraseña periódicamente.
- Elegir contraseñas difícilmente deducibles, evitando que coincidan, por ejemplo, con la fecha de nacimiento o el número de teléfono
- No utilizar las mismas claves para sitios web peligrosos o desconocidos que para entidades con un alto nivel de seguridad.

Cada vez que se efectúa una actualización crítica del sistema es necesario crear un nuevo disco de arranque. Por si no fuera posible corregir el error y fuera necesario reinstalar el sistema, también se aconseja tener siempre disponible el CD de instalación. También deberían mantenerse actualizados el sistema operativo y los programas, con las correcciones recomendadas. Habitualmente, los fabricantes van actualizando sus programas a medida que, a través del uso masivo de los mismos, se detectan errores. También suelen ampliar las

medidas de seguridad y es importante, tanto para la correcta estabilidad del sistema como para su seguridad ante posibles ataques, ir introduciendo todas las correcciones recomendadas.

## 2.2 Antivirus

Los virus son programas que se instalan en el ordenador sin que el propietario sea consciente, con fines maliciosos (por ejemplo, destruir archivos o el disco, propagarse a otros ordenadores o provocar un mal funcionamiento del ordenador). Las formas en las que se propagan son muy variadas y evolucionan con el tiempo. Para evitar posibles infecciones de virus es conveniente:

- Disponer de un software antivirus actualizado (debe actualizarse periódicamente, no basta con que sea más o menos nuevo). Para actualizarlo, deben consultarse las instrucciones del fabricante del programa.
- Verificar los documentos recibidos del exterior (vía correo electrónico, pen drive, descargas...) con el antivirus.
- Ejecutar sólo aquellos programas de los que tengamos garantía de su origen.

Un antivirus puede fallar por dos razones distintas: puede no detectar un virus al ser diferente de los que conoce; pero también puede detectar como virus un programa inofensivo que por casualidad tenga dentro de su código secuencias similares a las de un virus. Este segundo caso se conoce como "falso positivo".

El correo electrónico es una de las vías más importantes de transmisión de virus, ya que no siempre tenemos garantías suficientes de su remitente. Esto conlleva algunos riesgos como el posible acceso al contenido del correo por parte de terceros, la suplantación de identidad del remitente o el envío de virus. Para utilizarlo corriendo los riesgos mínimos es recomendable:

- No ejecutar directamente los ficheros anexos, es mucho más seguro extraerlos previamente a un directorio del ordenador.
- En caso de recibir correos no solicitados es recomendable confirmar el envío con el remitente o borrar el mensaje directamente. Nunca debe abrirse aunque provenga de un remitente conocido.
- No participar en correos encadenados. Existe un gran número de correos que contienen falsas noticias acerca de virus. Las casas comerciales y centros de alerta legítimos tienen como norma redirigir a servidores web donde dan información de forma fiable y detallan las acciones a tomar. No deben reenviarse correos indiscriminadamente.
- Cifrar la información crítica. (para usuarios expertos)

## 2.3 Programas espía o spyware

Los programas espía o spyware son aplicaciones maliciosas o engañosas que se instalan inadvertidamente junto con otros programas descargados por el usuario. Este tipo de programas puede ejecutar varias acciones diferentes: algunos se dedican a recopilar información del sistema en el que se encuentran instalados para luego enviarla a través de Internet. Otros se dedican a mostrar continuamente publicidad no deseada o a modificar las páginas visualizadas para incluir enlaces no existentes en el original. Todas estas acciones se enmascaran tras confusas autorizaciones, por lo que rara vez el usuario es consciente de ello.

Otro de los efectos de los spyware más intrusivos es que pueden cambiar nuestra página de inicio por otra, a elección del programa espía, que tanto puede ser una página en blanco como una de contenido dudoso. Si se intenta restaurar la página de inicio desde las opciones del explorador se verá que eso no es posible. Los cambios que el espía ha realizado en el registro del sistema no lo permiten.

- Para evitar los inconvenientes producidos por este tipo de programas espía se recomienda el uso de programas antiespía. Estos programas funcionan de forma similar a los programas antivirus, pero analizan el sistema en busca de programas espía y los eliminan. No son incompatibles con los programas antivirus, sino complementarios. Teniendo ambos instalados en nuestro ordenador estaremos mejor protegidos contra posibles intrusiones en nuestro sistema.

## **2.4 Firewall personal**

A medida que aumenta el uso de los ordenadores personales, el tiempo que están conectados a Internet y la importancia de la información con la que trabajamos, es necesario aumentar también su nivel de seguridad. Del mismo modo que un delincuente informático puede intentar acceder al ordenador de una gran empresa, puede también intentar acceder a un ordenador personal mal protegido con el objetivo de sustraer ficheros personales o instalar virus desde la red.

La herramienta adecuada para salvaguardar la seguridad del sistema es un firewall personal. El firewall personal es un programa que funciona en el ordenador de forma permanente. El programa monitoriza las conexiones que entran y salen del ordenador y es capaz de distinguir las que son legítimas de las realizadas por atacantes. En este segundo caso, las bloquea y lo notifica al usuario del ordenador.

### **2.4.1 Instalación**

Para instalar un firewall personal, en primer lugar es necesario asegurarse de que no existe ningún otro ya instalado. La instalación de dos firewalls personales no aumenta la seguridad, sino que genera fallos y conflictos entre ambos.

Además de las preguntas habituales de instalación, el firewall personal normalmente le solicitará que seleccione un nivel de seguridad. Se recomienda utilizar el nivel de seguridad normal a menos que sea un usuario experto.

Durante los primeros días de funcionamiento, el firewall personal suele enviar un gran número de mensajes. Estos avisos serán fundamentalmente de dos tipos:

- Peticiones de conexión de programas: al usar un programa, normalmente se establecen conexiones a Internet. El firewall personal detectará esta conexión y advertirá al usuario de ello.
- Ataques detectados: el sistema advertirá de que su sistema está siendo atacado. La frecuencia de los ataques puede llegar a ser de 3 o 4 por hora. No hay que alarmarse, casi siempre son ataques que se dirigen a redes enteras y que no afectan a ninguna máquina. Son intentos de ataque sin éxito de los cuales le informa el firewall personal.

En cualquiera de estos casos, el firewall personal puede avisar de nuevo o sólo registrar el ataque, según la opción que usted elija. Es decir, en caso de un nuevo acceso le avisará de nuevo o, por el contrario, repetirá nuestra última orden. Se recomienda utilizar todos los programas con conexión en la red disponibles los primeros días hasta que no haya mensajes de aviso y el firewall personal los tenga todos registrados. En cuanto a los ataques, ocurrirá lo mismo. Los primeros días se mostrará un número muy alto de ataques que irán disminuyendo progresivamente. Una vez el firewall personal esté en funcionamiento debe seguirse manteniendo y actualizando. Un firewall personal sólo es seguro si reconoce y detecta los últimos ataques conocidos. Igual que ocurre con los antivirus y, en general, todo el software, es conveniente actualizarlo con la última versión disponible.

## **2.5 Reglas básicas**

Tal como se indica en la página web de la Caixa, a continuación se citan 10 reglas básicas para mejorar la seguridad de su ordenador

1. No deben abrirse mensajes electrónicos de origen desconocido.
2. No deben facilitarse datos personales o códigos PIN de acceso.
3. No deben abrirse archivos de remitentes desconocidos.
4. No deben anotarse las claves de acceso (PIN) en ningún documento.
5. No deben utilizarse PIN triviales o de fácil deducción.
6. No debe confiarse nunca en regalos y promociones de fácil obtención, ni responder a mensajes que soliciten información de forma urgente.
7. Es preciso tener un sistema antivirus, utilizarlo y, periódicamente, actualizarlo. También es conveniente instalar un sistema antiespía para evitar los programas espía y de publicidad no deseada
8. Es preciso tener actualizado el navegador, así como instalar los parches del sistema operativo.
9. Es importante tener en consideración unas normas de protección del PC
10. Es preciso mantenerse informado sobre la seguridad general en el uso de Internet.

### 3. Amenazas, servicios y mecanismos de seguridad en redes de comunicación.

#### 3.1 Introducción

Para tasar de forma efectiva las necesidades de seguridad de una organización y para evaluar y elegir los productos y las políticas de seguridad, el administrador necesita alguna forma sistemática para definir los requisitos de seguridad y caracterizar las formas de satisfacer estos requisitos. Para ello se consideran los 3 aspectos fundamentales de la información: ataques, mecanismos y servicios.

En este apartado se tratan los ataques y mecanismos, los servicios se analizan en apartados posteriores. Como introducción se definirán de forma genérica los diversos aspectos que se tratan:

- Amenaza: una persona, cosa, evento o idea que supone algún peligro para un activo, ya sea un equipo o información (en términos de confidencialidad, integridad, disponibilidad o uso legítimo)
  - deliberada (acción de un hacker, por ejemplo)
  - accidental (Información confidencial enviada a una dirección equivocada)
- Ataque: es la ejecución de una amenaza, es decir, cualquier acción que compromete la seguridad de la información que posee una persona u organización.
  - pasivo (ej: monitorización)
  - activo (ej: modificación de los datos de una transacción financiera)
- Defensas: medidas de protección ante las amenazas.
- Vulnerabilidades: Puntos débiles en las defensas o inexistencia de éstas.
- Riesgo: medida del coste de una vulnerabilidad (teniendo en cuenta la probabilidad de un ataque satisfactorio). El riesgo es cuantificable; es el producto del valor activo por probabilidad éxito del ataque.
- Mecanismo de seguridad es aquel mecanismo diseñado para detectar, prevenir o reparar un ataque de seguridad.
- Riesgo residual: Riesgo tras implantar medidas o mecanismos de seguridad

#### 3.2 Ataques.

A la hora de proporcionar seguridad en la información, es muy importante prevenir y detectar los posibles fraudes o estafas. La naturaleza del ataque realizado sobre una determinada organización, varía ampliamente de unas circunstancias a otras. Afortunadamente se puede enfocar el problema desde otro ángulo, buscando los tipos genéricos de ataques para los que se puede realizar contraataques. En general la información viaja de un origen o fuente a un destino, tal como se muestra en la figura 3.1.

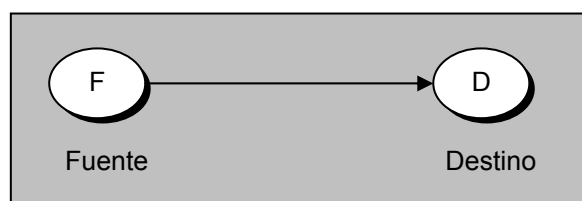


Figura 3.1. Flujo normal de información.

Los tipos de ataques de seguridad sobre un sistema de ordenadores o sobre una red, se caracterizan viendo la función que desempeña el sistema mientras proporciona la información.

Los ataques se pueden agrupar en 4 categorías generales que son las siguientes:

- **Interrupción:** Una parte del sistema se destruye o se convierte en no disponible o inutilizable. Es un ataque a la disponibilidad. Ejemplos de este ataque son la destrucción de una parte del hardware como el disco duro, el corte de una línea de comunicación, ...

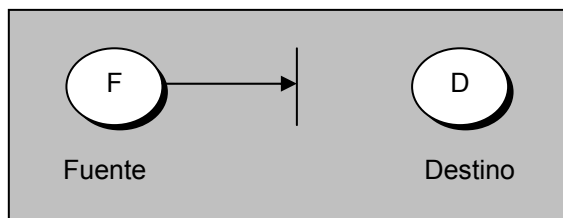


Figura 3.2. Interrupción.

- **Interceptado:** Alguien no autorizado consigue acceder al sistema. Es un ataque a la confidencialidad. Ese alguien puede ser una persona, un programa o un ordenador. Ejemplos de este ataque son la copia ilícita de ficheros o programas y la intervención de las conexiones para capturar datos en la red

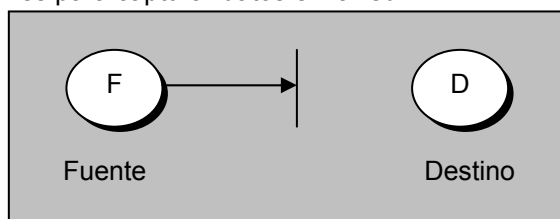


Figura 3.3. Interceptado.

- **Modificación:** Una entidad no autorizada además de conseguir acceso, también modifica algo del sistema. Ejemplos de este ataque son cambiar valores en un fichero de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de los mensajes que se transmiten en la red.

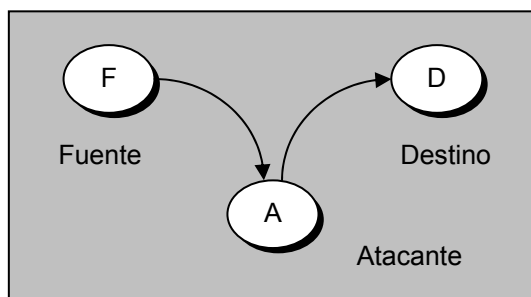


Figura 3.4. Modificación.

- **Fabricación:** Una entidad no autorizada inserta falsificaciones en el sistema. Es un ataque a la autenticidad. Ejemplos de este ataque son la inserción de mensajes ilegítimos en la red

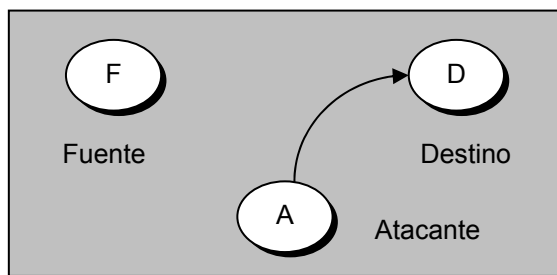


Figura 3.5. Fabricación

Típicamente las comunicaciones en redes siguen el modelo cliente-servidor. Este modelo o arquitectura consiste básicamente en que un programa -el Cliente informático- realiza peticiones a otro programa -el servidor- que le da respuesta. Por ejemplo, cuando un usuario se conecta a una página web, el usuario dispone de un software navegador (cliente), que establece la comunicación con el proveedor de contenidos (servidor) que ha sido solicitado. Debe tenerse en cuenta que el servidor no se ejecuta necesariamente sobre una sola máquina ni es necesariamente un sólo programa. La siguiente figura muestra los típicos ataques que se pueden realizar.

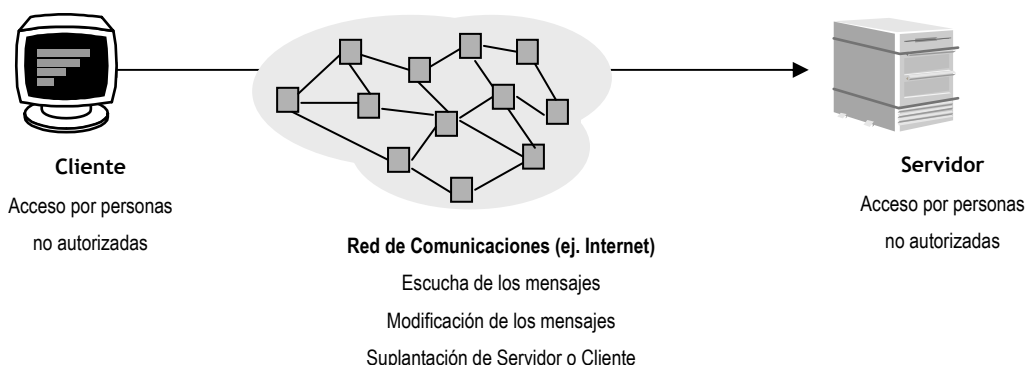


Figura 3.6. Posibles ataques en una comunicación cliente-servidor.

En el contexto de las comunicaciones a través de una red, se puede hacer la siguiente clasificación de los ataques:

- **Revelación:** Proporcionar a una persona o proceso que no posee la clave criptográfica adecuada, el contenido de un mensaje.
- **Análisis del tráfico:** Descubrimiento del patrón del tráfico entre varias partes. En algunas aplicaciones se puede determinar la frecuencia y duración de las conexiones así como el número y duración de los mensajes.
- **Enmascaramiento:** Inserción de mensajes en la red desde un origen fraudulento. Esto incluye la creación de mensajes por parte de un atacante que se supone que proceden de una entidad autorizada. También incluye la respuesta fraudulenta, por parte de alguien que no es el receptor del mensaje, diciendo que éste ha sido o no recibido.
- **Modificación del contenido:** Cambio del contenido de un mensaje incluyendo inserción, borrado, transposición o modificación.

- Modificación de la secuencia: Cualquier modificación de la secuencia de un mensaje entre 2 entidades, incluyendo inserción, borrado y reordenación.
- Modificación del tiempo: Retardar o reenviar mensajes. En una aplicación, tanto una sesión completa como una secuencia de mensajes de una sesión previa válida, pueden ser reenviados. También un mensaje individual perteneciente a una secuencia puede ser reenviado o retardado.
- Repudio: Negación de la recepción de un mensaje por parte de un destinatario, o de la transmisión por parte de una fuente.

Otra forma posible de clasificar los ataques y que se amplía en los siguientes apartados es en ataques activos y pasivos.

Los servicios de seguridad proporcionan formas de contraatacar a la mayoría de estos ataques.

### 3.3 Ataques pasivos.

En este tipo de ataques el objetivo es obtener la información que está siendo transmitida. Los motivos de un ataque de este tipo pueden ser la interceptación de datos, o el análisis del tráfico que permita conocer la naturaleza de la comunicación entre los usuarios.

Los ataques pasivos pueden ser de dos tipos: revelación de los contenidos del mensaje y análisis del tráfico.

La revelación de los contenidos del mensaje se comprende fácilmente. Una conversación telefónica, un mensaje del correo electrónico, un fichero transferido, puede contener información crítica o confidencial.

El segundo ataque pasivo, análisis del tráfico, es más complejo. Se supone que se tiene una forma de enmascarar el contenido de los mensajes u otra información del tráfico para que los atacantes, incluso si capturan el mensaje, no puedan extraer la información. La técnica más común para enmascarar los contenidos es el cifrado. Aunque se tengan los mensajes cifrados, un atacante puede observar el patrón de los mismos. El atacante podría determinar la localización y la identidad de los comunicantes y observar la frecuencia y longitud de los mensajes que se están intercambiando. Esta información podría ser útil para adivinar la naturaleza de la comunicación que está teniendo lugar.

Los ataques pasivos son muy difíciles de detectar, puesto que no comprenden alteración de los datos. Sin embargo, es factible impedir el éxito de estos ataques. Así pues, la investigación se centra más que en la prevención de los mismos, en impedir que tengan éxito.

### 3.4 Ataques activos.

Los ataques activos son aquellos en los que hay modificación de la cadena de datos o creación de una cadena falsa. Se dividen en 4 subcategorías: suplantación de identidad o enmascaramiento, reenvío, modificación de mensajes y denegación del servicio.

- El enmascaramiento o suplantación de identidad tiene lugar cuando una entidad pretende suplantar a otra. Un ataque de enmascaramiento normalmente incluye una de las otras formas de ataque activo. Por ejemplo se pueden capturar secuencias de autenticación y reenviarlas después de que haya tenido lugar una secuencia de autenticación válida. De esta forma se capacita a una entidad autorizada que tiene

pocos privilegios, a obtener privilegios extra haciéndose pasar por otra entidad que sí los tiene.

- El reenvío comprende la captura pasiva de una unidad de datos y su posterior retransmisión para producir un efecto no autorizado.
- La modificación de mensajes simplemente quiere decir que una parte de un mensaje legítimo es alterada, o que los mensajes son borrados o reordenados para producir un efecto no autorizado. Por ejemplo un mensaje tal como “Se permite al usuario x leer el fichero confidencial cuentas” se puede modificar quedando “Se permite al usuario y leer el fichero confidencial cuentas”.
- La denegación del servicio impide o inhibe el uso normal o el manejo de las comunicaciones. Este ataque puede tener un objetivo específico; por ejemplo, una entidad puede destruir todos los mensajes dirigidos a un destinatario particular. Otra forma de negación del servicio es la rotura completa de la red, bien por discapacitación, bien por sobrecargarla con mensajes.

Los ataques activos presentan características opuestas a los activos. Mientras que los ataques pasivos son difíciles de detectar, pero tienen medidas para impedir su éxito, los activos son muy difíciles de impedir, puesto que esto requeriría protección física de todos los caminos de comunicaciones durante todo el tiempo. Por tanto el objetivo es la detección y la recuperación después de una interrupción o retardo causada por estos ataques. Puesto que la detección tiene un efecto disuasorio, esto puede también contribuir a impedirlos.

### **3.5 Ataques de ingeniería social**

No basta con tener la mejor tecnología de seguridad -firewall, antivirus, antiespías, etc- instalado en nuestro ordenador para estar completamente seguros en Internet. Muchas veces son nuestras propias conductas las que nos ponen en peligro

El fraude en Internet se basa en una técnica denominada Ingeniería social. Las técnicas de ataque de ingeniería social se basan en el engaño; el internauta es inducido a actuar de una determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado.

#### **3.5.1 Phishing**

Los ataques denominados phishing usan correos electrónicos engañosos, aparentemente emitidos por fuentes fiables (por ejemplo, entidades bancarias) con la intención de obtener datos confidenciales del usuario. Su objetivo, cuando se dirigen a clientes de entidades financieras, es intentar que éstos divulguen sus datos, como el número de la tarjeta de crédito o las claves de acceso (PIN). Para conseguir dicho objetivo, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. El método es sencillo: se diseña una web fraudulenta, con apariencia prácticamente idéntica a la web original, intentando hacer creer al usuario que está conectado a su banco u otra página web de una entidad de su confianza. Al conectarse a la web fraudulenta se les piden los datos financieros o personales. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.

El correo fraudulento suele conducir al lector hacia sitios web que replican el aspecto de la empresa que está siendo utilizada para robar la información. En realidad, tanto los contenidos como la dirección web (URL) son falsos y se limitan a imitar los contenidos reales. Incluso la información legal y otros enlaces no vitales pueden redirigir al usuario confiado a la página web real. En algunos casos, incluso se utiliza el nombre de un empleado real de una empresa como remitente del correo falso. De esta manera, si el receptor intenta confirmar la

veracidad del correo llamando a la compañía, desde ésta le podrán confirmar que la persona que dice hablar en nombre de la empresa trabaja en la misma.

En cualquier caso, para evitar posibles fraudes de phishing es conveniente saber que la inmensa mayoría de entidades financieras nunca pide por correo electrónico ninguna información financiera a sus usuarios, como contraseñas, números de tarjeta o claves personales (PIN).

Otros consejos útiles para evitar que un usuario ilegítimo pueda conseguir nuestras claves son los siguientes:

1. Evitar en lo máximo posible realizar transacciones financieras en lugares públicos donde el acceso a Internet está disponible para muchas personas (p. ej. locutorios, cibercafés,...). Estos ordenadores podrían tener algún sistema para "capturar" datos personales, como claves de acceso.
2. Tener su navegador actualizado para tener los protocolos de seguridad en regla.
3. Observar si la dirección comienza con https: en lugar de solo http: Es recomendable comprobar que la navegación es segura y el sitio web bancario transmite su información cifrada mediante el protocolo de seguridad SSL (Secure Sockets Layer) que garantiza la comunicación entre el servidor y el cliente evitando que otros capturen o vean los datos intercambiados y garantizando la autenticidad del servidor al que nos conectamos y evitando que éste sea suplantado por un tercero. Una prueba rápida para comprobar la veracidad de la web de nuestro banco y no ser engañados por algunas web creadas para robar datos, es dar un "doble click" sobre el candado amarillo que aparece en la parte inferior/derecha de nuestro navegador, una vez realizado nos saldrá el certificado de autenticidad que asegura la identidad de nuestro Banco. En el capítulo 4 se detalla el concepto de certificado de autenticidad y en el capítulo 6 se detalla el funcionamiento del protocolo TLS.

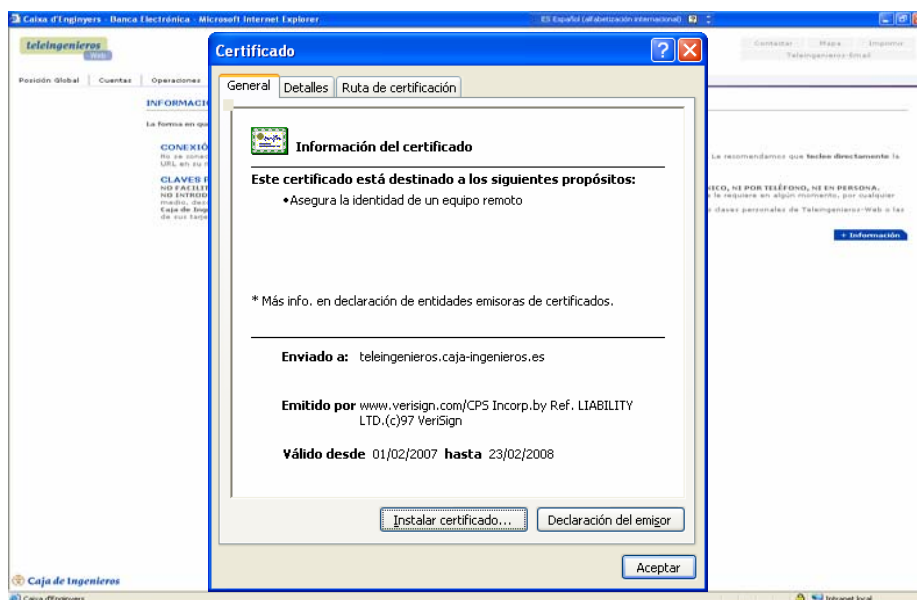
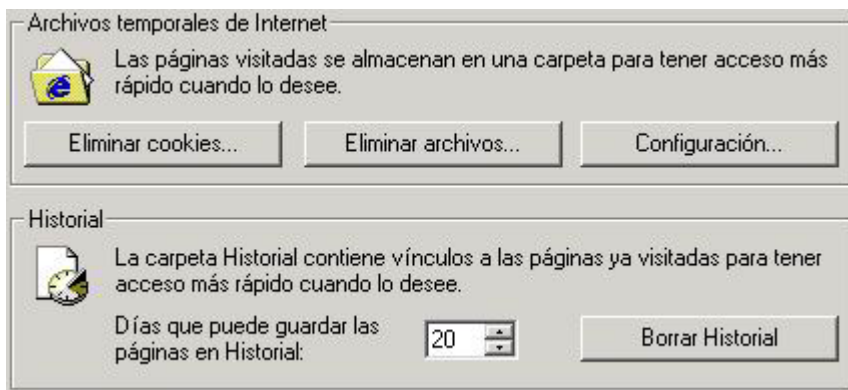


Figura 3.7. Visualización de una página web segura y su certificado digital.

4. Las claves de acceso deben almacenarse en secreto. Nunca deben ser reveladas a nadie ni anotadas en lugares visibles o de fácil acceso, como la pantalla, teclados, ni hacer un documento que ponga "claves-bancarias.txt".

5. Las claves usadas no deben ser palabras de un diccionario (deben parecer aleatorias) y deben ser modificadas periódicamente.
6. Cierre la sesión cuando termine de operar con su oficina virtual.
7. Borre la caché de su navegador al finalizar la sesión.



8. Tal como se ha comentado en el capítulo anterior, es muy recomendable el uso de software antivirus y antiespía en el equipo y manténgalo actualizado.

### 3.5.2 Virus.

Quizá el tipo más sofisticado de amenazas de los sistemas informáticos son programas que explotan las vulnerabilidades del sistema. En este contexto se incluyen programas de aplicación y de utilidades, editores y compiladores.

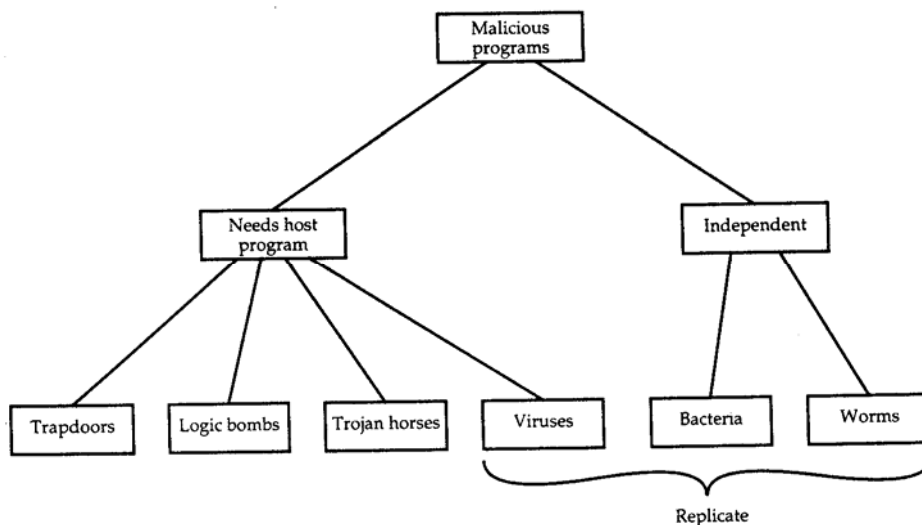


Figura 3.9. Clasificación de las amenazas software.

Este apartado empieza con una visión general del espectro de las amenazas del software. Estas amenazas se pueden dividir en 2 categorías, las que necesitan un programa anfitrión (host program) y las independientes. Esta clasificación se muestra en la figura 3.9.

Las primeras son fragmentos de programas que no pueden existir de forma independiente de un programa de aplicación, utilidad o sistema. Las otras son programas autocontenidos que pueden ser listados y ejecutados por el sistema operativo. A continuación se hará un breve análisis de cada uno de ellos.

### ***Puertas traseras.***

Las puertas traseras son mecanismos implantados en los programas por sus creadores, que les permiten a éstos realizar acciones determinadas sin tener que pasar por algunas secciones del programa, como procesos de autenticación etc. Se suelen utilizar preferentemente en tareas de depuración en las que muchas veces es necesario ejecutar repetidamente partes de un programa pero no se desea perder tiempo en realizar todos los pasos del programa que se desea depurar.

Muchas veces su presencia se debe al despiste de los desarrolladores que olvidan eliminarlas de sus programas. De la misma forma, los intrusos una vez que han conseguido el acceso a un programa, suelen crearlas para poder volver a entrar en él.

### ***Bombas lógicas.***

Uno de los tipos de amenazas de programas más antiguos son las bombas lógicas. Son códigos incrustados en algún programa legítimo que se ejecutan cuando se dan ciertas condiciones. Ejemplos de condiciones que pueden actuar como detonadores de la bomba lógica son la presencia o ausencia de ciertos ficheros, un día determinado de la semana o una fecha, o también un usuario particular que haga correr la aplicación. Una vez activada, la bomba puede borrar o alterar datos o ficheros completos, o causar cualquier tipo de daño en la máquina.

### ***Caballos de Troya.***

Un caballo de Troya es un programa que imita la ejecución de otros programas, pero realiza otras funciones completamente distintas a las esperadas.

Normalmente causan daños irreversibles, como introducir en medio de un programa secuencias de código que provocan la pérdida de todos los ficheros por parte del usuario que ejecuta el programa.

Existe otro caballo de Troya a priori menos destructivo pero que también puede tener graves consecuencias. Son los caballos de Troya utilizados para comprometer la seguridad del sistema. Normalmente se ocultan bajo el nombre de un fichero del sistema como puede ser el caso de los programas login.

Un caso típico de caballo de Troya consiste en reescribir el programa login de forma que cada vez que un usuario acceda al sistema su contraseña quede registrada en algún fichero.

### ***Virus.***

Un virus es un fragmento de código que se inserta en un programa ejecutable, de modo que cuando el programa es ejecutado, se ejecuta también el virus. La función que un virus pretende realizar es propagarse a sí mismo por todo el sistema. Para ello, va infectando a otros programas en los que inserta el fragmento de código vírico. La técnica es muy simple, cuando el fichero infectado es ejecutado, el fragmento de código vírico también se ejecuta, volviéndose a copiar a sí mismo al final del propio fichero, con lo que cuando termina de ejecutarse dicho fragmento de código vírico, vuelve a tener a continuación el mismo fragmento, de modo que la ejecución del programa nunca termina.

### ***Bacterias.***

Las bacterias son programas que no dañan de forma explícita los ficheros. Su único propósito es copiarse a sí mismos de forma que ocupan todos los recursos del sistema e incluso pueden llegar a bloquearlo. Las bacterias se reproducen de forma exponencial,

restando capacidad al disco duro, la memoria o el procesador, impidiendo a los usuarios el acceso a estos recursos.

### **Gusanos.**

Los gusanos son programas que se reproducen copiándose de un ordenador a otro a través de la red. A diferencia de los virus son independientes y no necesitan otro programa donde alojarse. Normalmente no producen ningún daño en el sistema, excepto malgastar los recursos, llegando incluso a sobrecargar la red.

La solución ideal para todas estas amenazas es la prevención, pero en general, esta meta es imposible de alcanzar. Los esfuerzos se centran en hacer que el mínimo número de ataques de virus tengan éxito. La tecnología desarrollada a este efecto avanza paso a paso.

## **3.6 Atacantes**

Una de las principales amenazas para la seguridad son los intrusos, a los que normalmente se denomina *crackers*. En un importante estudio sobre intrusión realizado, Anderson identificó 3 clases de intrusos:

- **“Masquerader”**: Un individuo que no está autorizado para usar un determinado ordenador, y a pesar de eso, penetra en el sistema de control de acceso para aprovecharse de la cuenta de otro usuario legítimo.
- **“Misfeasor”**: Un usuario legítimo que accede a unos datos, programas o recursos a los que no está autorizado, o que tiene autorizado el acceso, pero hace mal uso de los mismos a su favor.
- **Usuario clandestino**: Un usuario que se apodera del control que supervisa el sistema y lo utiliza para evitar el control de acceso.

El “masquerader” es normalmente un usuario externo, el “misfeasor” un usuario de la propia red, y el usuario clandestino puede ser ambos.

El tipo de ataques que puede realizar un intruso comprende un rango amplio, desde los que se pueden llamar benignos, a los serios. Dentro de los primeros se encuentran aquellos que simplemente quieren echar un vistazo en la red. Como ataques serios se pueden citar la lectura de datos restringidos, la realización de modificaciones no autorizadas de los datos, o la rotura del sistema.

Los intrusos benignos podrían ser tolerables, aunque consumen recursos y hacen más lenta la utilización del sistema por parte de los usuarios legítimos. Sin embargo no hay forma de saber a priori, si un intruso será benigno o maligno. Como consecuencia de esto, incluso en los sistemas que no contienen recursos particularmente sensibles, hay un motivo para controlar este problema.

Los ataques serios por parte de los intrusos son un problema real y creciente. Algunas de las razones de este crecimiento son:

- ***Globalización***: Las presiones de la competición internacional han producido un gran número de casos recientes de espionaje industrial. Muchos clubs de hackers están vendiendo sus servicios a las empresas para este propósito.
- ***Cambio de la arquitectura cliente/servidor***: Las empresas tradicionalmente han mantenido la mayoría de sus datos o en ordenadores centrales, donde se guardan con un software de seguridad sofisticado, o en sistemas autónomos como PCs, los cuales no son accesibles de forma remota. Al aumentar la popularidad de la

arquitectura cliente/servidor, se quitaron ambas barreras. Muchos servidores funcionan sobre UNIX, el cual es conocido por su falta de características de seguridad como ordenador central, por lo que es el favorito de los hackers.

- *Rápido aprendizaje de los hackers:* A los hackers les encanta compartir información. A causa de su natural aversión a la seguridad, los hackers son más capaces que sus adversarios de hacer frente a los más recientes trucos del mercado. Además cuando el personal de seguridad intercambia información sobre puntos vulnerables, los atacantes pueden a menudo espiar y explotar estas vulnerabilidades antes de que puedan restablecerse todos los agujeros de seguridad creados en el sistema.

El colectivo "hacker" no es un colectivo homogéneo: White Hat hackers, Grey Hat hackers (Ethical hackers), Script Kiddies, Hacktivist, Black Hat Hackers . En el nivel alto se encuentran usuarios con un amplio conocimiento de la tecnología, y en el nivel bajo aquellos que aunque utilizan los programas no saben como funcionan. El trabajo en equipo combina las 2 armas de los intrusos: conocimiento sofisticado de como hacer la intrusión y disponibilidad para pasar mucho tiempo probando la debilidad.

### **3.7 Mecanismos de seguridad.**

Los mecanismos de seguridad son aquellos que permiten ofrecer los servicios de seguridad de los que se hablará más adelante. No hay un único mecanismo que proporcione todos los servicios de seguridad. Hay que subrayar que de todos los mecanismos de seguridad en uso, hay un tipo de ellos que destaca sobre todos los demás, que son las técnicas o mecanismos criptográficos.

El cifrado es el más antiguo de entre los mecanismos de protección. La criptografía (del griego kryptos, «ocultar», y graphos, «escribir», literalmente «escritura oculta») es la ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera que sólo sean legibles por las personas a quienes van dirigidos. La criptografía es el estudio de sistemas matemáticos que involucra a dos problemas de seguridad: privacidad y autenticación. El cifrado y descifrado como transformaciones de la información, son la forma más común de proporcionar seguridad.

Los mecanismos más importantes son los siguientes:

- Intercambio de autenticación. Corrobora que una entidad, ya sea origen o destino de la información, es la deseada.
- Cifrado. Garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados.
- Integridad de datos. Este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir. Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.
- Firma digital. Este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía al receptor junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad.

- Control de acceso. Esfuerzo para que sólo accedan a los recursos del sistema o a la red, aquellos usuarios autorizados.
- Tráfico de relleno. Consiste en enviar tráfico espúreo junto con los datos válidos para que el enemigo no sepa si se está enviando información, ni qué cantidad de datos útiles se está transfiriendo.
- Control de encaminamiento. Permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

Por otro lado, la mayoría de los sistemas de ordenadores proveen mecanismos de control de accesos en su primera línea de defensa. Este mecanismo únicamente limita el acceso a un objeto en el sistema, pero no modela ni restringe qué es lo que un individuo puede hacer con el objeto en el caso de que tenga acceso a su manipulación

Los controles de acceso y modelos de protección no son útiles ante amenazas internas. Si una contraseña es débil y se compromete, las medidas de control de acceso no pueden prevenir la pérdida o corrupción de la información a la que el usuario estaba autorizado a acceder. En general, los métodos estáticos de aseguramiento de propiedades de seguridad en un sistema o son insuficientes, o pueden resultar demasiado restrictivos para los propios usuarios.

Por otro lado también podemos encontrar mecanismos de identificación y autenticación. Estos mecanismos posibilitan la identificación adecuada de los sujetos y objetos del sistema. La identificación es la declaración de quién es el usuario (conocido a nivel global), mientras que autenticación es la prueba o confirmación de esa identificación

Por último, hay otra serie de mecanismos con el objetivo de velar por la disponibilidad de un sistema. Algunos de ellos actúan a modo de filtros, dejando pasar aquella información que esté autorizada, en el caso de routers (con listas de acceso o ACL) y cortafuegos o firewalls. Y por último los que de alguna manera detectan amenazas, como antivirus y sistemas de detección de intrusos. Éstos últimos forman la última línea de defensa en el esquema general de protección de un sistema informático, y no sólo son útiles para detectar incidentes de seguridad, sino también intentos de romper la seguridad.

Los sistemas de protección física son un mecanismo práctico para salvaguardar los equipos terminales de posibles ataques. Sin embargo, la dispersión geográfica de los sistemas de transmisión en redes, hace que una protección de este tipo suponga un alto coste económico, haciéndolos totalmente desaconsejables en estos casos. Los sistemas criptográficos, por otro lado, son muy útiles para la seguridad en redes de datos, ya que permiten paliar muchas de las posibles vulnerabilidades que estas presentan.

### **3.8 Servicios de seguridad**

Se entiende por servicio de seguridad aquél que mejora la seguridad de los sistemas de procesado y de comunicación de la información de un grupo determinado de personas o de una organización. Un servicio de seguridad hace frente a ataques contra la seguridad empleando uno o varios mecanismos.

En el estándar de arquitectura de seguridad de la ISO se definen cinco servicios:

- 1- Confidencialidad:** Protege contra el acceso no autorizado a parte o a la totalidad de la información.
- 2- Autenticación:** Proporciona la certeza de la identidad de una entidad. Puede ser simple o mutua. Cuando es simple, únicamente uno de los comunicantes tiene que demostrar su identidad. Cuando es mutua, ambos comunicantes se identifican el uno al otro.
- 3- Integridad:** Protege contra la modificación, el borrado o la sustitución de la información durante la transmisión. Igual que ocurre con el servicio de confidencialidad, se puede aplicar a una cadena de mensajes, a un único mensaje, o a campos específicos del mensaje.
- 4- No repudio:** Protege contra la negación de una entidad que participa en una comunicación, de haber enviado un mensaje (repudio de origen) o de haberlo recibido (repudio de entrega). Dicho servicio también es conocido como irrenunciabilidad.
- 5- Control de acceso:** Protege contra el uso o la manipulación no autorizada de recursos. Se controla el acceso a los sistemas informáticos y a los enlaces de datos evitando las infiltraciones y el uso no autorizado de recursos.

En la Tabla 2.1 se muestra una serie de analogías entre los servicios de seguridad y la vida cotidiana.

Servicio de seguridad	Ejemplo de la vida cotidiana
Autenticación	Carné con identificación fotográfica Huellas dactilares
Control de acceso	Llaves y cerrojos
Confidencialidad	Tinta invisible Carta lacrada
Integridad	Tinta indeleble
No repudio	Firma notariada Correo certificado

Tabla 3.1. Analogías entre servicios de seguridad y vida cotidiana.

## 4. Mecanismos criptográficos

### 4.1 Introducción

A lo largo de la historia el ser humano ha desarrollado unos sistemas de seguridad que le permiten comprobar en una comunicación la identidad del interlocutor (ej. tarjetas de identificación, firma), asegurarse de que sólo obtendrá la información el destinatario seleccionado (ej. correo certificado), que además ésta no podrá ser modificada (ej. notariado) e incluso que ninguna de las dos partes podrá negar el hecho (ej. Notariado, firma) ni cuándo se produjo (ej. fechado de documentos). En la mayor parte de los casos el sistema de seguridad se basa en la identificación física de la persona, información que se contrasta con el documento de identidad.

Actualmente cada vez mayor número de actividades se está trasladando al mundo electrónico a través de Internet. Se hace, por lo tanto, necesario trasladar también los sistemas de seguridad a este contexto en el que el principal problema reside en que no existe contacto directo entre las partes implicadas. Necesitamos un documento digital que ofrezca las mismas funcionalidades que los documentos físicos con el plus de ofrecer garantías aún sin presencia física.

Las técnicas criptográficas constituyen uno de los mecanismos más utilizados para proveer dichos servicios. Por ello, serán presentadas con detalle posteriormente, aunque a continuación se darán unas breves pinceladas sobre estos conceptos.

#### **Criptografía:**

La ciencia de la criptografía estudia las comunicaciones electrónicas, principalmente digitales, que se realizan en un medio hostil, vulnerable y en el que existe una desconfianza entre las entidades comunicantes.

- 1- **Hostil:** pueden existir atacantes que quieran evitar que la comunicación tenga lugar.
- 2- **Vulnerable:** los atacantes pueden desear modificar la información transmitida u obtenerla de forma ilícita.
- 3- **Desconfianza:** un participante puede intentar perjudicar al otro.

Los sistemas analizados por la criptografía enmascaran la información con el objetivo de garantizar una serie de requisitos, como la confidencialidad, integridad, autenticación, etc.

#### **Criptanálisis:**

El criptanálisis trata de romper los sistemas que la criptografía implementa para así poder obtener, por ejemplo, la información enmascaramiento por tales técnicas.

### 4.2 Objetivos de la criptografía

Las tecnologías de la seguridad de la información tienen tres objetivos fundamentales:

- **Confidencialidad o privacidad.** La confidencialidad de los datos es la protección de la información personal y sensible contra la revelación y los ataques tanto intencionados como no intencionados por parte de una posible tercera parte.
- **Autenticación.** La autenticación proporciona la seguridad de que los datos recibidos fueron en realidad enviados por quien asegura haberlo hecho. Se pueden diferenciar dos tipos de autenticación:
  - de entidad simple, ya sea del emisor o del recipiente de la información; y

- mutua o bidireccional en la que ambos intercomunicantes se autentican uno al otro.
- **Verificabilidad.** La criptografía no sólo permite garantizar la confidencialidad y autenticidad, sino también poder corroborar incluso ante terceros que los datos recibidos fueron los originalmente emitidos y fueron emitidos por quien firmó el documento.

Además de estos objetivos básicos, y de los servicios definidos por la ISO (apartado anterior), la seguridad de un sistema debe garantizar los siguientes:

- **Disponibilidad.** Se ha de asegurar que no le sea negado a un usuario legítimo el acceso al sistema y se han de proporcionar recursos alternativos para poder utilizarlos en caso de caída de éste.
- **Idempotencia.** Cuando una operación se puede realizar un número indeterminado de veces sin que cause ningún daño al sistema, se dice que es *idempotente*.

Las tecnologías empleadas para garantizar estos servicios se pueden dividir en dos categorías:

- las relacionadas con las comunicaciones: protección de la información mientras es intercambiada; y
- las relacionadas con el sistema físico: protección de la información dentro de los ordenadores local y remoto (características de los sistemas operativos, gestión de las bases de datos, etc.).

### 4.3 Métodos criptográficos

Las técnicas criptográficas, tales como el cifrado de datos o la firma digital, son empleadas en todos los sistemas que necesiten garantizar los servicios comentados en el apartado anterior. El mecanismo más básico empleado es el denominado **criptosistema** o **algoritmo criptográfico**, el cual define dos transformaciones:

- el **cifrado**: es la conversión el **texto en claro** (*plaintext*) en el **texto cifrado** o **criptograma** (*ciphertext*) mediante el empleo de una determinada **clave**; y
- el **descifrado**: es el proceso inverso.

La aplicación más inmediata de un algoritmo criptográfico (aunque no la única) es asegurar el servicio de confidencialidad: en lugar de transmitir el texto en claro se envía el cifrado, de forma que un atacante no podrá descifrar el contenido de la información transmitida a no ser que conozca la clave de descifrado.

La seguridad de un sistema de cifrado radica casi totalmente en la privacidad de las claves secretas. Por ello, los ataques que puede realizar un criptoanalista enemigo están orientados a descubrir dichas claves y pueden ser de varios tipos (se supone que el atacante tiene acceso al texto cifrado):

- Ataque con sólo texto cifrado (*ciphertext-only attack*).
- Ataque con texto en claro conocido (*known-plaintext attack*). El enemigo, además de poseer los criptogramas, también dispone de los textos en claro asociados.
- Ataque con texto en claro escogido (*chosen-plaintext attack*). El enemigo puede conseguir el criptograma asociado a cualquier texto en claro.
- Ataque con texto cifrado escogido (*chosen-ciphertext attack*). El enemigo puede obtener el texto en claro de cualquier criptograma.
- Ataque con texto escogido (*chosen-text attack*). Combina los dos ataques anteriormente mencionados.

### 4.3.1 Criptografía moderna

La principal diferencia de los sistemas criptográficos modernos respecto a los clásicos está en que su seguridad no se basa en el secreto de todas las partes del procedimiento, sino en la robustez de sus operadores (algoritmos empleados) y sus protocolos (forma de usar los operadores), siendo el único secreto la clave (los operadores y protocolos son públicos).

Los algoritmos de cifrado se pueden dividir en dos categorías: simétricos o de clave privada y asimétricos o de clave pública. A continuación se explicará cada uno de ellos.

#### 4.3.1.1 Métodos simétricos o de clave privada

La criptografía simétrica (e.g., DES o AES) usa la misma clave para cifrar y para descifrar un mensaje (figura 4.1) y su seguridad se basa totalmente en el secreto de dicha clave (el algoritmo es públicamente conocido). Generalmente se utilizan dos funciones: una para realizar el cifrado y otra para el descifrado. Su principal desventaja es que hace falta que el emisor y el receptor compartan la clave.

En un buen sistema simétrico, a no ser que se conozcan todos los bits de la clave, no se podrá extraer ninguna información del texto cifrado.

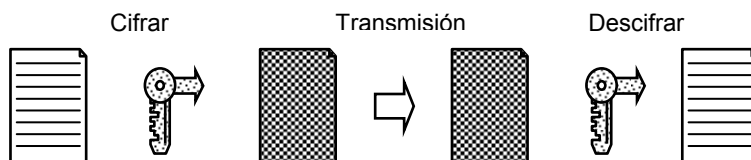


Figura 4.1. Criptografía de clave privada.

Dado que las claves usadas para cifrar y para descifrar son idénticas, no se pueden disociar los procesos de confidencialidad y autenticación, es decir, si se ofrece un servicio utilizando criptografía simétrica, también se está ofreciendo el otro. Entre los algoritmos más comúnmente utilizados para ofrecer estos servicios se pueden destacar el DES (Data Encryption Standard), el AES (Advanced Encryption Standard) y el IDEA.

El beneficio más importante de la criptografía de clave simétrica es su velocidad lo cual hace que éste tipo de algoritmos sean los más apropiados para el cifrado de grandes cantidades de datos. El problema que presenta la criptografía de clave simétrica es la necesidad de distribuir la clave que se emplea para el cifrado por lo que si alguien consigue hacerse tanto con el mensaje como con la clave utilizada, podrá descifrar el mensaje. Por esta razón se plantea el uso de un sistema criptográfico basado en claves asimétricas, como veremos a continuación.

#### 4.3.1.2 Métodos asimétricos o de clave pública

En este caso, cada usuario del sistema criptográfico ha de poseer una pareja de claves:

Clave privada: será custodiada por su propietario y no se dará a conocer a ningún otro.

Clave pública: será conocida por todos los usuarios.

Esta pareja de claves es complementaria: lo que cifra una SÓLO lo puede descifrar la otra y viceversa. Estas claves se obtienen mediante métodos matemáticos complicados de forma que por razones de tiempo de cómputo, es imposible conocer una clave a partir de la otra. Las dos claves de cada usuario (pública y privada) están relacionadas matemáticamente de tal forma que los datos cifrados por una de las dos sólo pueden ser descifrados por la otra.

Este tipo de algoritmos se pueden utilizar de dos formas, dependiendo de si la clave pública se emplea como clave de cifrado o de descifrado. En el primer caso (figura 4.2), cuando un usuario, A, quiere enviar información a otro usuario, B, utiliza la clave pública de B,  $K_{pu_B}$ , para cifrar los datos. El usuario B utilizará su clave privada (que sólo él conoce),  $K_{pr_B}$ , para obtener el texto en claro a partir de la información (cifrada) recibida. Si otro usuario, C, quiere enviar información al usuario B, también empleará la clave pública  $K_{pu_B}$ . Este modo se suele emplear para proporcionar el servicio de confidencialidad, pues sólo el usuario B es capaz de descifrar los mensajes que los usuarios A y C le han enviado.

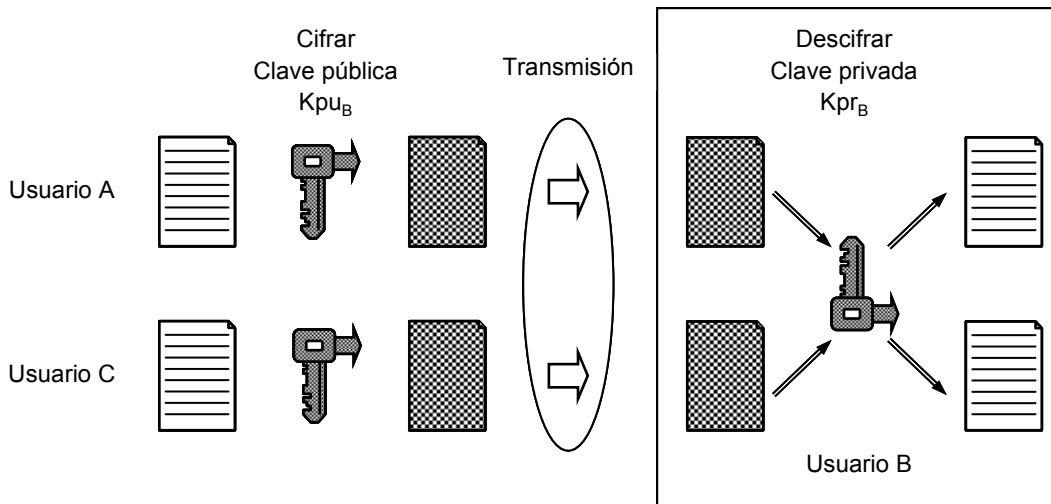


Figura 4.2. Criptografía de clave pública: confidencialidad.

En el otro modo de operación (figura 4.3), es el usuario B quien cifra la información utilizando su clave privada,  $K_{pr_B}$ , de forma que cualquiera que conozca  $K_{pu_B}$  podrá descifrar la información transmitida. Este método se puede emplear para proporcionar el servicio de autenticación, ya que la obtención del texto en claro a partir del texto cifrado es una garantía de que el emisor del mensaje es el propietario de  $K_{pu_B}$  (lógicamente, para saber que el mensaje obtenido de la descifrado del texto cifrado es el texto en claro original, éste se ha de obtener por otros medios para realizar una comparación – esto se verá más adelante). También es la base para la construcción de los mecanismos de firma digital.

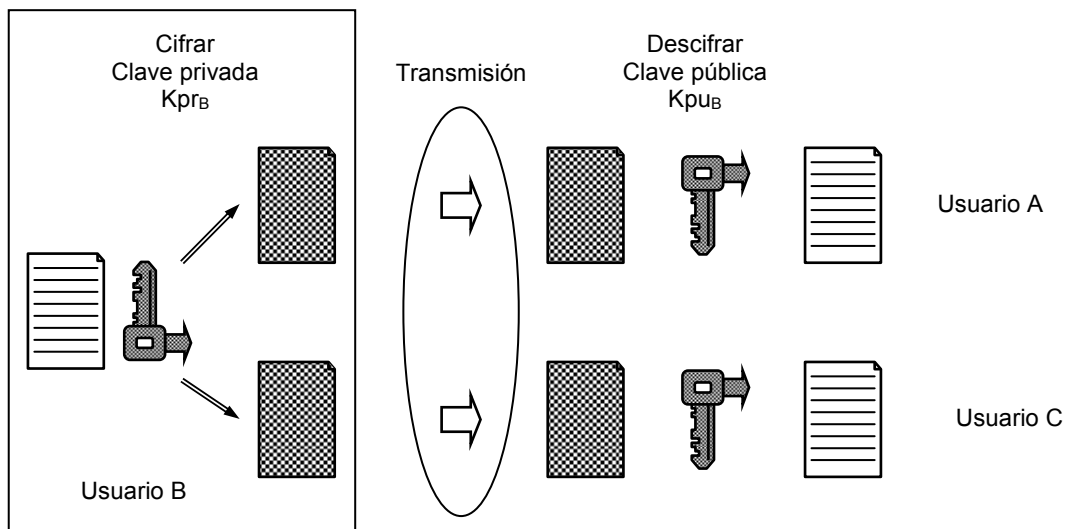


Figura 4.3. Criptografía de clave pública: autenticación.

El beneficio obtenido consiste en la supresión de la necesidad del envío de la clave, siendo por lo tanto un sistema más seguro. El inconveniente es la lentitud de la operación. Para solventar dicho inconveniente, el procedimiento que suele seguirse para realizar el cifrado de un mensaje es utilizar un algoritmo de clave pública junto a uno de clave simétrica. Los algoritmos de clave pública se suelen emplear para facilitar la gestión de claves simétricas utilizadas en cada sesión (session key o one-time-key) que son simétricas. Entre los algoritmos de clave pública, el más habitualmente utilizado es el RSA.

En el anexo 1 se detalla el funcionamiento del algoritmo RSA

### 4.3.2 Funciones Hash

Un **valor hash** de un mensaje es un valor “único” generado a partir de él. Esto se realiza pasando el mensaje a través de una función criptográfica con las siguientes propiedades:

- Su algoritmo es conocido públicamente.
- Son de un solo sentido; o sea, a partir del valor hash no se puede obtener los datos originales.
- El valor hash es obtenido de tal forma que es muy poco probable obtener el mismo valor a partir de otros datos.

La robustez de una función hash se basa en la de las características mencionadas anteriormente. Por ejemplo, si un atacante conoce un mensaje y su valor hash y puede encontrar otros datos que produzcan el mismo valor hash, será capaz de realizar una sustitución sin que esta pueda ser detectada.

Entre los algoritmos de hash más empleados cabe destacar el SHA-1 (*Secure Hash Algorithm*) que produce una salida de 160 bits, y el MD5 de RSA Data Security Inc. que produce 128 bits de salida (considerado algo más débil que el primero).

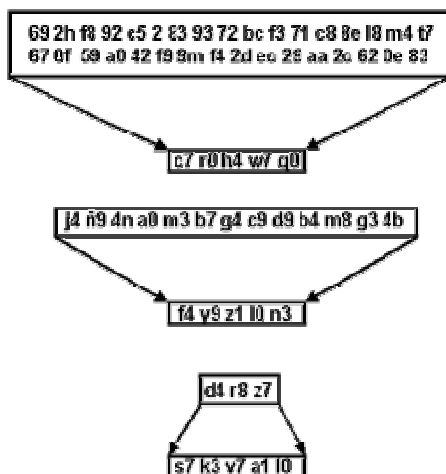


Figura 4.4. Ejemplo de operación de una función de hash

### 4.3.3 Firma digital

La **firma digital** es un mecanismo utilizado en los sistemas de información para asegurar la integridad del mensaje y la autenticación del emisor.

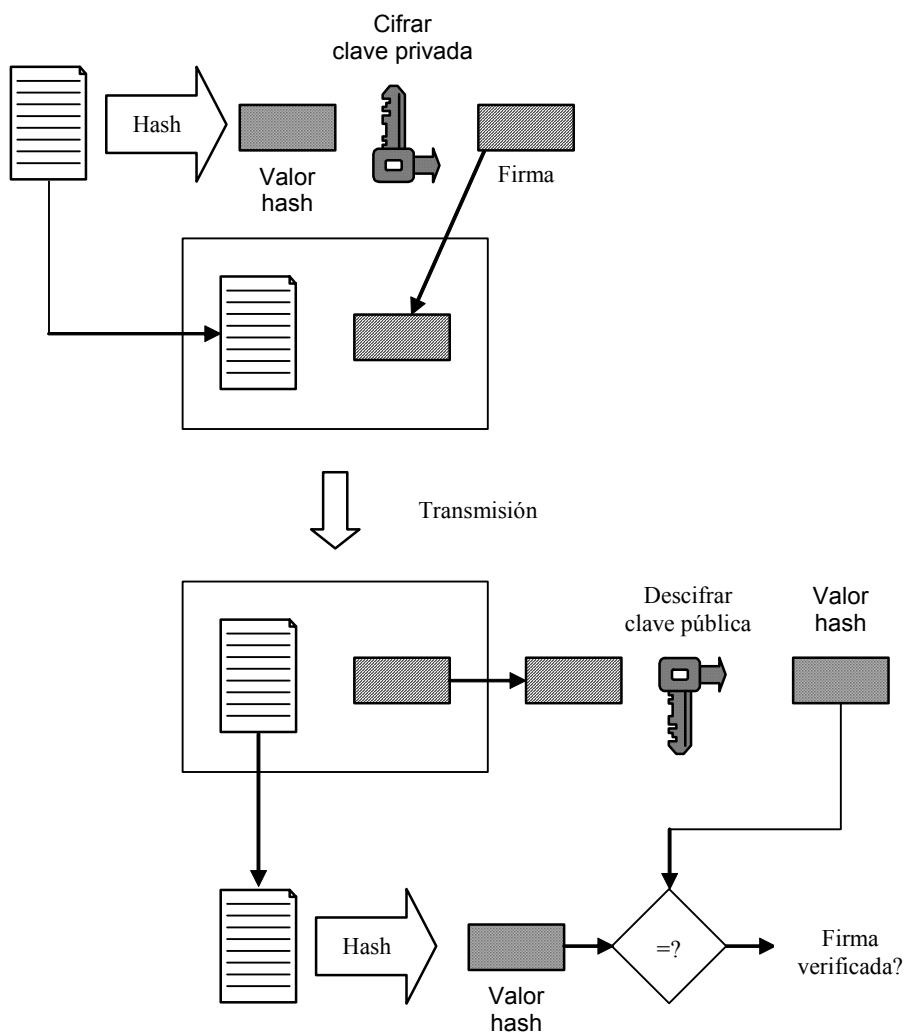


Figura 4.5. Esquema de firma digital

Este método (figura 4.5) consiste en la obtención de un valor hash del mensaje y su posterior cifrado con la clave privada del emisor. En recepción se descifra el hash con la clave pública del emisor y se compara con otro valor hash obtenido en recepción de forma independiente a partir del mensaje recibido.

La firma digital permite soportar el servicio de no repudio, ya que la verificación de la firma garantiza que ésta sólo puede haber sido generada por el poseedor de la clave privada; o sea, su usuario legítimo (a no ser que la clave privada haya sido comprometida). Esta propiedad es fundamental a la hora de realizar transacciones económicas, ya que, por ejemplo, cuando una entidad realiza un pedido de unos determinados bienes o servicios, el proveedor de éstos ha de tener un medio para poder denunciar al solicitante ante las autoridades competentes en caso de éste niegue haber realizado el mencionado pedido.

#### 4.3.3.1 Digital Signature Algorithm DSA

Un algoritmo ampliamente empleado es el *Digital Signature Algorithm* (DSA) definido en el *Digital Signature Standard* (DSS), propuesto por el U.S. National Institute of Standards and Technology (NIST). Este método se basa en la función exponencial discreta en un campo de elementos finito, la cual tiene la característica de ser difícilmente reversible, ya que realizar el logaritmo discreto es una operación de una gran complejidad.

Desde el punto de vista del usuario, la creación de una firma digital se realiza de la misma manera independiente de si se emplea RSA o DSA, aunque éste último conlleva una mayor carga computacional. Sin embargo, al contrario de lo que ocurre con RSA, DSA no proporciona la capacidad para proporcionar el servicio de confidencialidad.

#### 4.4 Gestión de claves

Todas las técnicas criptográficas dependen en última instancia de una o varias claves, independientemente del tipo de servicio que proporcionen, por lo que la gestión de éstas es una tarea de vital importancia. Esta labor incluye básicamente:

- La generación de las claves de forma que cumplan los requisitos necesarios para su correcta utilización.
- Su distribución a todas las entidades que las puedan necesitar.
- La protección necesaria para evitar su revelación o sustitución.
- El suministro de mecanismos para informar a las entidades que las conocen en caso de que la seguridad de dichas claves haya sido comprometida.

El tipo de método empleado para llevar a cabo la gestión de las claves es diferente según el tipo de criptografía utilizada (simétrica o asimétrica).

Todas las claves tienen un tiempo determinado de vida, el **criptoperiodo**, para evitar que las técnicas de criptoanálisis tengan el suficiente tiempo e información para “romper” el algoritmo criptográfico asociado. El ciclo de vida de una clave incluye las siguientes fases:

- **Generación.** Este proceso es dependiente del algoritmo en el que se va utilizar la clave en cuestión, aunque generalmente se emplea una fuente generadora de números pseudo-aleatorios como base para la creación de la clave. El método ideal de generación sería aquél que escogiera una clave con la misma probabilidad que cualquier otra posible, ya que cualquier indicio determinista en el proceso podría facilitar el criptoanálisis.
- **Registro.** Las claves se han de enlazar a la entidad que las usará.
- **Distribución.** Aunque pueden utilizarse criptografía de clave simétrica para la distribución, habitualmente se utiliza criptografía de clave pública, utilizando el proceso que se indica en el apartado siguiente.
- **Recuperación.** Esto puede ser necesario en el caso de que una clave se pierda.
- **Reemplazo o actualización.** Esto será necesario cuando el criptoperiodo haya finalizado o en otras circunstancias especiales.
- **Revocación.** Esto se llevará a cabo cuando la seguridad de una clave haya sido comprometida.
- **Destrucción.** Esto hace referencia a borrar cualquier rastro de la clave.

##### 4.4.1 Distribución de claves simétricas mediante técnicas asimétricas

Como ya se ha explicado anteriormente, el servicio de confidencialidad se puede proporcionar utilizando tanto técnicas simétricas como asimétricas, pero estas últimas suponen una mayor carga computacional que las hace poco prácticas para la cifrado de grandes bloques de datos. Por ello, los métodos que se emplean comúnmente son una combinación de ambas categorías criptográficas.

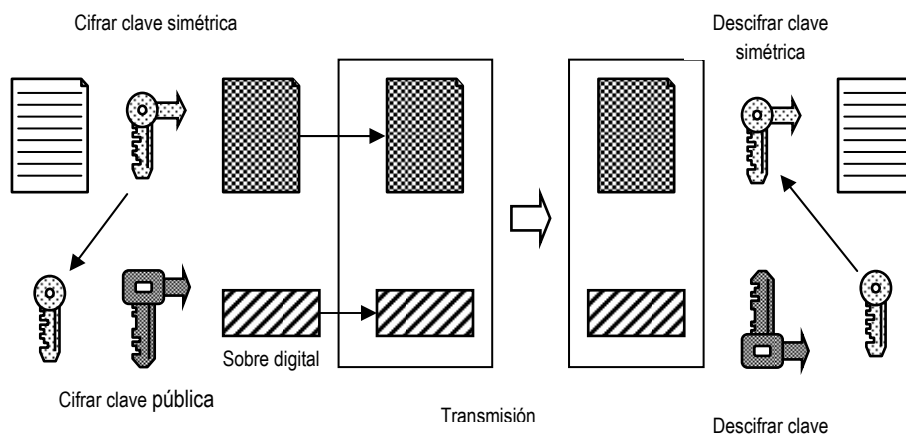


Figura 4.6. Distribución asimétrica de claves simétricas.

Generalmente, el proceso de distribución se realiza en los siguientes pasos (figura 3.6):

- 1- Se cifra el texto en claro con una clave simétrica para obtener así el texto cifrado.
- 2- La clave simétrica se cifra con la clave pública del recipiente. Al resultado de esta operación se lo denomina **sobre digital**.
- 3- Se envía el texto cifrado y la clave simétrica cifrada.
- 4- En recepción, se descifra la clave simétrica con la clave privada del recipiente.
- 5- Se descifra el texto cifrado con la clave simétrica obtenida en el paso 4, obteniendo así el texto claro original.

#### 4.4.2 Distribución de claves asimétricas

La gestión de claves asimétricas es totalmente diferente de la descrita anteriormente, en la que hace falta que cada participante almacene una clave para cada una de las otras entidades con las que mantiene comunicaciones.

En los métodos asimétricos, cada entidad sólo ha de poseer un par de claves (una privada y una pública) independientemente del número de sistemas con los que se comunique. El único requisito que se ha de cumplir es la garantía de la integridad de la clave, para así evitar que un posible atacante sustituya una clave pública y suplante a su usuario legítimo; este tipo de ataque se denomina *man-in-the-middle*. Para evitar este problema se recurre a lo que se denominan los **certificados de clave pública**, que son emitidos por unas entidades de confianza llamadas **Autoridades Certificadoras** (ACs, *Certification Authorities*) y que garantizan que una determinada clave pública pertenece a su verdadero poseedor.

#### 4.5 Certificados

El grado de seguridad que una red telemática puede proporcionar es mayor cuando ésta se controla mediante mecanismos centralizados que cuando se hace de forma distribuida, pues una gestión global facilita la aplicación de técnicas con el objetivo de evitar ataques contra la privacidad, la integridad y la autenticación de la información.

Sin embargo, aplicar un control centralizado a Internet no es viable, pues va en contra de su naturaleza. La solución actualmente empleada para securizar las comunicaciones realizadas a través de Internet se basan en métodos criptográficos asimétricos gestionados por **Terceras Partes Confiables** (TTP, *Trusted Third Parties*), de modo similar a como actuaría un notario.



Figura 4.7. Certificación digital.

Estas entidades, entre las que se encuentran las ya mencionadas ACs, permiten garantizar los servicios de confidencialidad e integridad de los datos y el no repudio de origen y destino.

Una arquitectura de gestión de certificados para Internet ha de proporcionar un conjunto de mecanismos para que la autenticación de emisores y recipientes sea simple, automática y uniforme independientemente de las políticas de certificación empleadas.

La infraestructura propuesta específica para Internet consta de una estructura jerárquica con una raíz única raíz, que ha de definir todas las políticas globales a aplicar dentro de dicha jerarquía. Las autoridades de certificación ACs son las encargadas de gestionar los certificados de los usuarios finales y deben hacer públicas sus políticas de seguridad y servicios.

El formato más extendido para el uso de certificados es el X.509. Los campos habitualmente presentes en un certificado que sigue este formato son:

- **Versión.** Indica la versión del certificado (habitualmente es la 3)
- **Número de serie.** El número de serie es un entero asignado por la AC emisora y que identifica unívocamente al certificado dentro del conjunto de certificados emitidos por la AC en cuestión.
- **Firma.** Identifica al algoritmo utilizado por la AC para firmar el certificado.
- **Emisor.** El nombre del emisor identifica a la entidad que ha firmado el certificado y sigue la nomenclatura de **nombres distinguibles** (DNs, *Distinguished Names*) de X.500
- **Validez.** Indica el intervalo de tiempo en el que el certificado es válido.
- **Usuario o sujeto.** Es un nombre distinguible X.500 que identifica de forma unívoca al poseedor del certificado.
- **Información de clave pública del usuario.** Contiene la clave pública del usuario junto con el identificador del algoritmo con el que se ha de utilizar.
- **Identificadores únicos de emisor y de usuario.** Es una cadena de bits opcional que identifica al emisor o al usuario en el caso de que su nombre haya sido reutilizado con el paso del tiempo. Se recomienda la no reutilización de nombres y que no se empleen los identificadores únicos.

- **Campos de extensión.** Permiten la adición de nuevos campos a la estructura sin que por ello se tenga que modificar la definición del certificado. Cada uno de estos campos consiste en:
  - un identificador de extensión,
  - un valor para indicar si es o no crítico, y
  - una codificación canónica de un valor de un tipo ASN.1 asociado con la extensión identificada.

#### 4.5.1 Generación y distribución de certificados

Las autoridades de certificación (ACs) tienen como misión la gestión de los denominados **certificados** (de clave pública). Un certificado está compuesto básicamente por la identidad de un usuario (subject), su clave pública, la identidad y la clave pública de la AC emisora (issuer) del certificado en cuestión, su periodo de validez y la firma digital del propio certificado. Esta firma, realizada por la AC emisora, permite que aquellas entidades que deseen realizar comunicaciones con la persona poseedora del certificado, puedan comprobar que la información que éste contiene es auténtica (suponiendo que confiemos en la AC emisora). Una vez que los certificados han sido firmados, se pueden almacenar en servidores de directorios o transmitidos por cualquier medio (seguro o no) para que estén disponibles públicamente.

#### 4.5.2 Validación de certificados

Antes de enviar un mensaje cifrado mediante un método asimétrico, el emisor ha de obtener y verificar los certificados de los recipientes de dicho mensaje. La validación de un certificado se realiza verificando la firma digital en él incluida mediante el empleo de la clave pública de su signatario, que a su vez ha de ser validada usando el certificado correspondiente, y así sucesivamente hasta llegar a la raíz de la jerarquía de certificación. En el proceso de verificación se ha de comprobar el periodo de validez de cada certificado y que ninguno de los certificados de la cadena haya sido revocado. Esto último se realiza utilizando las CRLs (*Certificate Revocation Lists*). El esquema global de validación se muestra en la figura 3.6, donde **CERT** representa el certificado de la raíz de la jerarquía de certificación, firmado por ella misma y que se supone confiable.

Una vez validado el certificado del recipiente, se puede extraer de él la clave pública que será utilizada para realizar la cifrado. En la mayoría de los casos, esta clave se empleará para cifrar una clave de cifrado de datos (DEK, *Data Encryption Key*) que será la realmente usada para cifrar el mensaje.

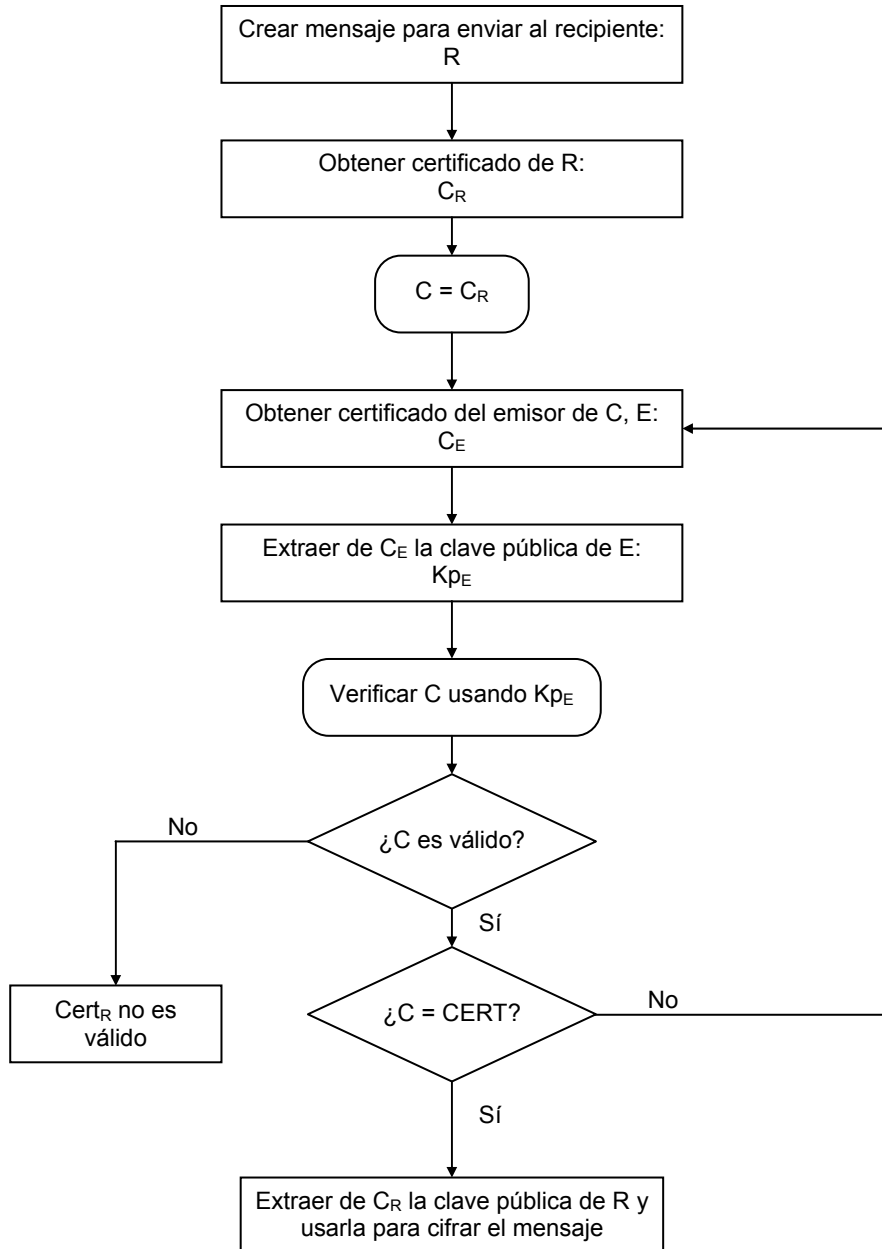


Figura 4.7. Validación de la cadena de certificación.

### 4.5.3 Revocación

Los certificados tienen un periodo de vida limitado, el cual está especificado en el propio certificado y que viene determinado por la política de la AC emisora. Sin embargo, en algunas ocasiones especiales la seguridad de la clave privada asociada puede haberse visto comprometida, por lo que la utilización de la correspondiente clave pública ha de ser evitada. También puede ocurrir que el propietario del certificado cambie de nombre, hecho que implica que ha de modificarse el certificado. En tales casos, la AC emisora puede **revocar** el certificado para prevenir su uso. La decisión de revocar un certificado es responsabilidad de la AC emisora, generalmente en respuesta a la petición de una entidad autorizada, como por ejemplo, el propio dueño del certificado.

## 5. Cortafuegos e IDS. Seguridad perimetral

### 5.1 Sistemas firewall (cortafuegos)

La traducción de firewall al español es **Cortafuegos**. Básicamente podemos decir un firewall es un software que controla las conexiones que se realizan a Internet desde o hacia nuestro ordenador.

Para explicarlo podemos establecer un símil entre las puertas de una habitación y los puertos de un ordenador. Las conexiones a nuestro ordenador se hacen a través de puertos. Los puertos son como puertas de acceso a nuestro ordenador; un firewall lo que hace es cerrar con llave esa puerta para que nadie pueda entrar ni salir por ahí. Esto es, ningún programa podrá enviar datos a través de ese puerto ya que está cerrado. Las conexiones pueden ser de entrada o salida, lo que implica que la puerta puede utilizarse para entrar o para salir, es decir si un programa de nuestro ordenador envía datos a Internet la estará usando para salir, pero si estamos recibiendo datos desde Internet estamos usando la puerta para entrar. El firewall, podría cerrar la puerta sólo en un sentido, de forma que sólo se pueda entrar, o bien solo salir.

Esto nos proporciona un gran nivel de seguridad y nos protege de muchos posibles ataques, pero tiene 2 inconvenientes. Si se utiliza un programa que necesite comunicarse con Internet, dicho programa necesitará que los puertos que utiliza para comunicarse estén abiertos, sino no podrá funcionar. Es decir, deberemos informar al firewall que hay una serie de programas a los que les permitimos que envíen datos desde nuestro ordenador. Normalmente el firewall detecta que el programa quiere comunicarse a través de un determinado puerto y lo que hace es preguntar al usuario si desea permitirlo. Nosotros decidiremos si el programa es de confianza y necesitamos que pueda comunicarse con Internet. De esto podemos deducir los dos inconvenientes de un firewall:

El usuario tiene la responsabilidad de decidir cuidadosamente que programas permitimos comunicarse y cuales no. Esto requiere un pequeño mantenimiento o esfuerzo del usuario.

Cuando se permite a un programa utilizar un puerto, recae sobre este programa la responsabilidad de evitar cualquier ataque de seguridad a través de él.

Con el firewall, estamos evitando muchos posibles problemas de seguridad. Si entra algún virus o troyano en nuestro ordenador, no podrá comunicarse con el exterior, enviando posible información privada de nuestro ordenador a algún intruso malintencionado. Todo esto a no ser que seamos descuidados y cuando el firewall nos pregunte si le permitimos su comunicación le digamos que sí (esto hace referencia al inconveniente (1)).

Pero por tener un Firewall no vamos a estar seguros al 100% ni mucho menos. Por ejemplo, todos los usuarios tienen un navegador instalado que inevitablemente necesita comunicarse con Internet. Asimismo es habitual usar programas como eMule que también se comunican con Internet. Esto implica un factor importante a tener en cuenta: podría ser que un hacker encuentre algún agujero de seguridad en el eMule y logre acceder al ordenador. La moraleja es que da igual que tengamos instalado un Firewall con excelentes prestaciones si los programas que se conectan a Internet son un auténtico coladero.

Debido a todo lo anterior, un 'Firewall' + 'Actualizaciones periódicas del software' + 'Responsabilidad' hace que en conjunto hagan una gran defensa.

Como ha quedado más o menos claro, un cortafuegos es un sistema destinado a prevenir accesos no autorizados desde o hacia una red segura, es decir, protege una red de otra en la que no se tiene confianza. Para proporcionar una robusta seguridad un firewall debe seguir y controlar la comunicación que pasa a través de él. Para alcanzar el control de decisiones (aceptar, rechazar, autenticar, cifrar y/o guardar un registro los intentos de

comunicación) un firewall debe obtener, almacenar, recuperar y manipular la información derivada desde todas las capas de comunicación y otras aplicaciones.

Así pues, podemos decir que un firewall es un elemento de hardware o software utilizado en una red de ordenadores para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las directrices que haya definido la organización responsable de la red (conocidas como política de seguridad).

La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

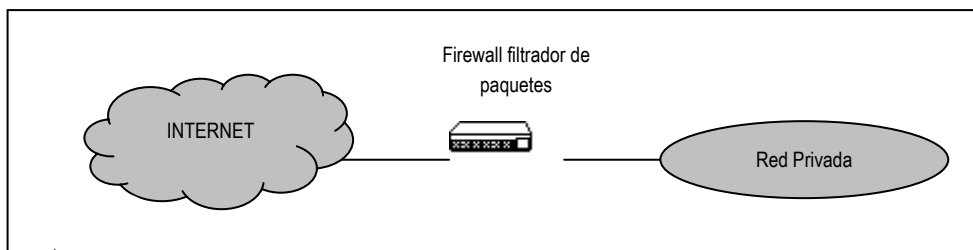


Figura 5.1. Esquema de un firewall

Así pues, un firewall se puede definir como un dispositivo o conjunto de elementos o sistemas ubicados entre dos redes, con las siguientes propiedades:

- Todo el tráfico que sale y entra de una red debe pasar a través del firewall. Cuando decimos esto, nos referimos a los datos transportados según el conjunto de protocolos de Internet
- En el firewall se define una política de seguridad que regula que datos son autorizados y sólo estos pueden pasar a través del firewall.
- El sistema por sí mismo es altamente resistente a las penetraciones.

Es decir, se trata de un mecanismo que permite proteger a una red fiable de las redes no fiables con las que ésta se encuentra conectada (típicamente Internet), permitiendo el tráfico de datos entre ambas. Un firewall está compuesto de diferentes componentes, incluyendo filtros, que bloquean la transmisión de cierta clase de tráfico y una pasarela que se puede definir como una máquina o conjunto de máquinas que transmiten servicios entre las redes internas y externas.

Tal como se ha mencionado anteriormente, el uso de firewalls está estrechamente relacionado con la política de seguridad implementada en la organización que los utiliza y en especial con la política de control de acceso definida. Existen dos tipos de políticas de red que influyen directamente en la implementación, configuración y uso de un firewall: La política de acceso a servicios de red y la política de diseño de un firewall.

La política de acceso a servicios define los servicios que serán permitidos o denegados explícitamente desde las redes restringidas, además de especificar la manera en la que los servicios serán usados. Para que un firewall funcione de la manera que las organizaciones desean, la política de acceso a servicios debe existir antes de que se implemente el uso del firewall. Esta política debe ser realista, en el sentido de que debe mantener un balance entre la protección de una red y los servicios a los que se podrán acceder. Es decir, debe permitir que las redes se protejan con el uso de firewalls pero sigan siendo útiles a los usuarios.

La política de diseño de firewalls especifica como un firewall restringirá el acceso a una red y como se implementará el filtrado de paquetes según lo especificado en la política de

acceso a servicios. Es por eso que debe definirse primero la política de acceso a servicios y luego la política de diseño de firewalls.

La política de diseño de firewalls es específica y define las reglas a ser usadas para implementar la política de acceso a servicios.

Las políticas de diseño de los firewalls siguen una de estas guías:

- Permitir el acceso a cualquier servicio, a no ser que se especifique explícitamente lo contrario. Esta alternativa es conocida como permisiva. En este caso, los firewalls permiten que todos los servicios accedan a la red protegida, a excepción de aquellos que son identificados como no permitidos por la política de acceso a servicios.
- Denegar cualquier servicio, a menos que se especifique explícitamente lo contrario. Esta alternativa es conocida como restrictiva. Los firewalls que implementan esta alternativa deniegan, por defecto, cualquier servicio, a excepción de aquellos que se definen en la política de acceso a servicios como permitidos.

En definitiva, para la implementación de firewalls debe tenerse en cuenta la política de seguridad definida y saber identificar cuales son los servicios que serán permitidos y cuales son los que deben ser denegados.

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	jet	ftp	User Auth	Short	Gateways	probes
2	localnet	Any	ftp http https telnet	accept		Gateways	Any
3	Any	firewall	Any	drop	Mail	Gateways	Any
4	Any	Any	Any	drop	Long	Gateways	Any

Figura 5.2. Ejemplo de política de acceso restrictiva.

En el anexo 2, destinado a usuarios con un mayor conocimiento, se detalla una clasificación de firewalls en función del modo de operación.

## 5.2 Detección de intrusiones

Los sistemas de detección de intrusión permiten identificar las amenazas dirigidas hacia una entidad o usuario y establecer un método para evitar que esa amenaza tenga el efecto deseado por el atacante. La siguiente figura muestra el esquema genérico de comportamiento de un IDS.

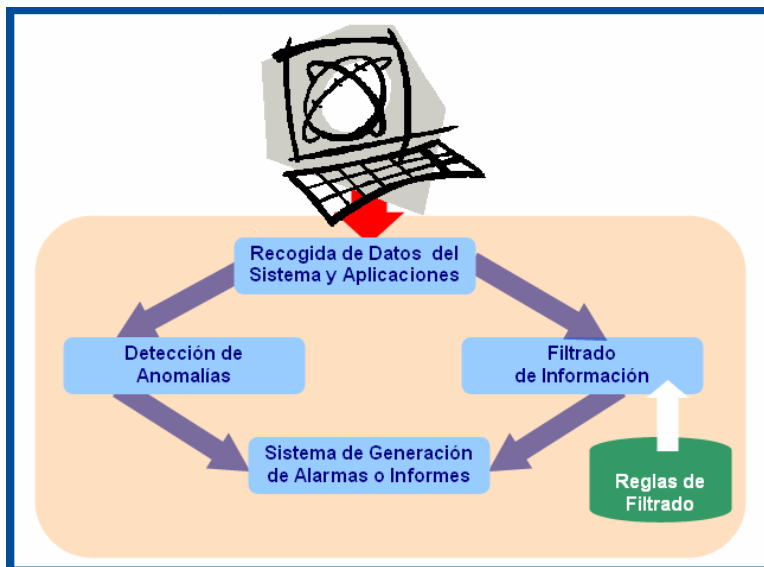


Figura 5.3. Esquema de un sistema de detección de intrusiones

Las primeras investigaciones sobre detección de intrusos tuvieron sus inicios en 1980 en un trabajo de consultoría realizado para el gobierno norteamericano por James P. Anderson, quien trató de mejorar la complejidad de la auditoría y la habilidad para la vigilancia de sistemas informáticos. Es el primero que introduce el término “amenaza” en la seguridad informática, y lo define como la *potencial posibilidad de un intento deliberado de acceso a información, manipulación de la misma, o hacer que un sistema sea inutilizable*. Anderson presentó la idea de que el comportamiento normal de un usuario podría caracterizarse mediante el análisis de su actividad en los registros de auditoría. De ese modo, los intentos de abusos podrían descubrirse detectando actividades anómalas que se desviarán significativamente de ese comportamiento normal.

Se puede definir intrusión como la *violación de la política de seguridad de un sistema*, o como la *materialización de una amenaza*. Heady definió intrusión como *cualquier conjunto de acciones que tratan de comprometer la integridad, confidencialidad o disponibilidad de un recurso*. Una de las definiciones más populares de intrusión es: *fallo operacional maligno, inducido externamente*, aunque es bien sabido que muchas de las intrusiones proceden del interior del sistema de información. Finalmente, el NIST (National Institute of Standards and Technology) define detección de intrusos como *el proceso de monitorización de eventos que suceden en un sistema informático o red y análisis de dichos eventos en busca de signos de intrusiones*.

El primer modelo de detección de anomalías fue el propuesto por Dorothy Denning, con la idea básica de monitorizar las operaciones estándares de un sistema objetivo, observando desviaciones en su uso. Su trabajo provee un enmarque metodológico que más tarde inspiraría a muchos investigadores. Entre 1988 y 1990 el Instituto de Investigación SRI International desarrolla la propuesta de Denning. De ese modo surge IDES (Intrusion Detection Expert System), un sistema experto que detecta las desviaciones a partir del comportamiento de diferentes sujetos. IDES fue el primer sistema de detección de anomalías en host. Al mismo tiempo, en 1988, en los laboratorios Lawrence Livermore de University of California en Davis, se realiza el proyecto Haystack para las fuerzas aéreas de EE.UU. Haystack era el primer IDS que analizaba los datos de auditoría y los comparaba con patrones de ataque predefinidos. De

este modo nacía el primer sistema de detección de usos indebidos basado en firmas, el tipo de IDS más extendido en el mercado actual.

En 1990, surgen los primeros proyectos de IDS basados en red. Todd Heberlein introduce tal idea y desarrolla NSM (Network Security Monitor) en University of California at Davis. En esa misma fecha, en Los Alamos National Laboratory de EEUU realizan un prototipo de un sistema experto que monitoriza la actividad de red. Su nombre es NADIR (Network Anomaly Detector and Intrusion Reporter). A partir de este momento, comienzan una gran variedad de proyectos de investigación que hacen uso de diferentes técnicas y algoritmos para el análisis del comportamiento de un sistema informático.

### 5.2.1 Clasificación de los Sistemas de Detección de Intrusos

La clasificación o taxonomía de los sistemas de detección de intrusos ha sido tratada en numerosos trabajos, de los que destacan los de Hervé Debar y Stefan Axelsson de Chalmers University of Technology en Suecia.

La clasificación más común se realiza en base a tres características funcionales de los IDS:

- **Fuentes de información.** Se refiere al origen de los datos que se usan para determinar si una intrusión se ha llevado a cabo.
- **Análisis.** Se trata del método de detección utilizado. La información recogida en el paso anterior puede ser analizada mediante diferentes estrategias.
- **Respuestas.** Una vez se ha determinado si ha sucedido alguna intrusión, los IDS pueden o bien responder de forma activa ante la misma, o bien registrar la detección y no realizar acción alguna.

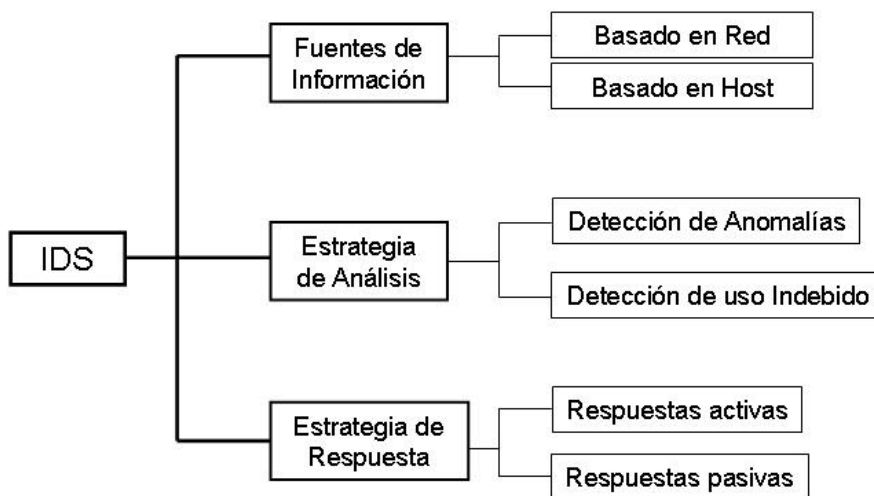


Figura 5.4. Clasificación de los sistemas de detección de intrusión

#### 5.2.1.1 Fuentes de información

Desde el inicio de los IDS, se ha trabajado con multitud de datos provenientes de diferentes fuentes para tratar de identificar la existencia de una intrusión. Estos datos se pueden diferenciar en dos grandes grupos; aquellos datos obtenidos de una máquina o host, y aquellos datos obtenidos a partir de la monitorización de una red. Dentro de cada grupo, se pueden identificar diferentes enfoques que se pueden tomar:

**Host:**

- **Logs** o registros de auditoría

- Llamadas del sistema o system calls de procesos en ejecución
- Métricas de uso del sistema
- Comandos del teclado

**Red:**

- Comunicación de datos (Ethernet, Token Ring, ...).
- Nivel de red (normalmente IP)
- Nivel de Transporte/control (TCP, UDP, RTP, ICMP,...)
- Nivel de Aplicación (HTTP, DNS, Telnet, FTP, SSH, SMTP,...)
- Wireless

### 5.2.1.2 Estrategia de Análisis

La estrategia de análisis se refiere al método de detección que utilizan los IDS.

La siguiente clasificación de las técnicas de detección desde el punto de vista de la estrategia de análisis está principalmente basada en las prospecciones realizadas en [Noe02] y [Laz04]. Un esquema podría ser el siguiente:

#### **Detección de uso indebido**

Un IDS basado en detección de uso indebido monitoriza las actividades que ocurren en un sistema y las compara con firmas de ataques, las cuales se encuentran almacenadas en una base de datos. Cuando las actividades monitorizadas coinciden con las firmas, genera una alarma. La detección de intrusos basada en uso indebido se atiene al conocimiento a priori de las secuencias y actividades que forman un ataque. Con este método se detectan las tentativas de explotación de vulnerabilidades conocidas o patrones de ataque típicos. Esta estrategia es la más utilizada en los IDS comerciales.

Típicamente, un sistema de detección de uso indebido contiene dos componentes principales:

- Un lenguaje o modelo para describir o representar las técnicas utilizadas por los atacantes.
- Programas de monitorización para detectar la presencia de un ataque basado en las representaciones o descripciones dadas.

La *ventaja* de los IDS basados en uso indebido es la fidedigna detección de patrones de ataques conocidos. Al igual que un software antivirus, el comportamiento malévolo puede identificarse con una precisión aceptable.

Como *desventaja*, cabe mencionar el hecho de que el patrón del ataque ha de ser conocido con anterioridad, lo que hace que nuevas intrusiones pasen desapercibidas ante el detector, o que el sistema pueda ser fácilmente engañado con pequeñas variantes de los patrones de ataques conocidos. Otra desventaja es que hay que adaptar manualmente el IDS al sistema en el que se implanta si no queremos que se dispare el número de falsos positivos.

Una variante habitual de este tipo de IDS es la **Detección de Firmas**. Esta variante, también conocida como Sistema de Razonamiento Basado en Modelos, observa la ocurrencia de cadenas especiales (o patrones de cadenas) que puedan ser consideradas como sospechosas. La detección de firmas compara los eventos que ocurren, con las cadenas o firmas almacenadas en una base de datos de escenarios de ataque (almacenada como una secuencia de comportamientos o actividades) en busca de coincidencias. Su principal inconveniente es la necesidad de desarrollar e incorporar a la base de datos una firma nueva para cada nuevo tipo de ataque o vulnerabilidad descubierta.

### **Detección de anomalías**

Una anomalía se puede definir como la *discrepancia de una regla o de un uso* [Rae04]. De ese modo, el primer paso de un sistema de detección de anomalías comienza por establecer lo que se considera comportamiento normal de un sistema (usuarios, redes, registros de auditoría, llamadas del sistema de los procesos, etc.). Una vez definido esto, clasificará como sospechosas o intrusivas aquellas desviaciones que pueda detectar sobre el comportamiento normal.

La detección de anomalías depende mucho de la suposición de que los usuarios y las redes se comportan de un modo suficientemente regular, de forma que cualquier desviación significante pueda ser considerada como evidencia de una intrusión.

La gran ventaja de la detección de anomalías es que el sistema es capaz de aprender el comportamiento normal del objeto de estudio, y a partir de ahí detectar desviaciones del mismo, clasificándolas como intrusiones. De este modo, se demuestra que es capaz de detectar tipos de ataques hasta el momento desconocidos.

Como *desventaja*, por definición únicamente señala comportamientos inusuales, pero éstos no tienen necesariamente por qué ser ilícitos. Por ello, destaca el problema de su alta tasa de falsos positivos. Otra desventaja de este proceso es la falta de claridad (es un proceso borroso). Un intruso podría actuar lentamente y realizar sus acciones cuidadosamente para modificar el perfil de los usuarios de modo que sus actividades serían aceptadas como legales cuando en realidad deberían lanzar una alarma (falsos negativos). Otras veces, no es o debería ser suficiente el hecho de simplemente avisar de un comportamiento anómalo sin explicar los posibles orígenes.

Al igual que ocurre con la detección de uso indebido, se pueden encontrar diferentes variantes en el método de implementar los sistemas de detección de anomalías. Se hacen uso de mecanismos heurísticos y estadísticos para adaptarse a los cambios en el comportamiento del objeto a estudio así como para detectar cambios imprevistos. Otras aproximaciones tratan de incorporar otras técnicas para realizar esta función.

#### **5.2.1.3 Respuesta**

La gran mayoría de los IDS cuentan con un método de respuesta básico cuando identifican un ataque: la notificación. A este tipo de respuesta se le llama **respuesta pasiva**, y su función es la de notificar al administrador de la ocurrencia de un ataque. La notificación suele realizarse por medio de mensajes, correo electrónico, sms, etc.

Sin embargo, en los últimos años ha tomado fuerza la posibilidad de responder a los ataques de forma automática. Son las llamadas **respuestas activas** o **respuestas automáticas**. Las respuestas activas son un campo activo de la investigación, debido a que por un lado, las respuestas que se implementan hoy en día ignoran el coste que puede suponer una intrusión. De este modo podría ocurrir que las respuestas causaran mayor daño que las propias intrusiones. Por el otro lado, los IDS actuales reportan un gran número de falsos positivos, por lo que pueden causar acciones de respuesta numerosas, innecesarias y costosas [Bal03] pudiendo llegar a causar denegación de servicio a usuarios legítimos del sistema.

### **5.3 Integración**

La siguiente figura muestra un posible esquema de una red con firewalls e IDS. El IDS1 se encargaría de avisar del rastreo de puertos, y si es de respuesta activa podría enviar un "aviso" tanto al que está rastreando (por ejemplo un ping a la dirección que emite el paquete) como al encargado de la seguridad de la organización. El IDS2 se encargaría de vigilar la zona desmilitarizada y analizar el tráfico que reciben tanto el servidor web como el servidor de correo. Los otros dos IDS se encargarían de la red interna, el IDS3 de la totalidad de la red, y el

¿Cómo funciona la seguridad en Internet?

IDS4 de una subred, en este caso la de RRHH. Estos dos NIDS internos (el IDS3 y el IDS4) podrían ser sensores que recogiesen la información y lo enviasen a una consola dónde se realizarían los cálculos.

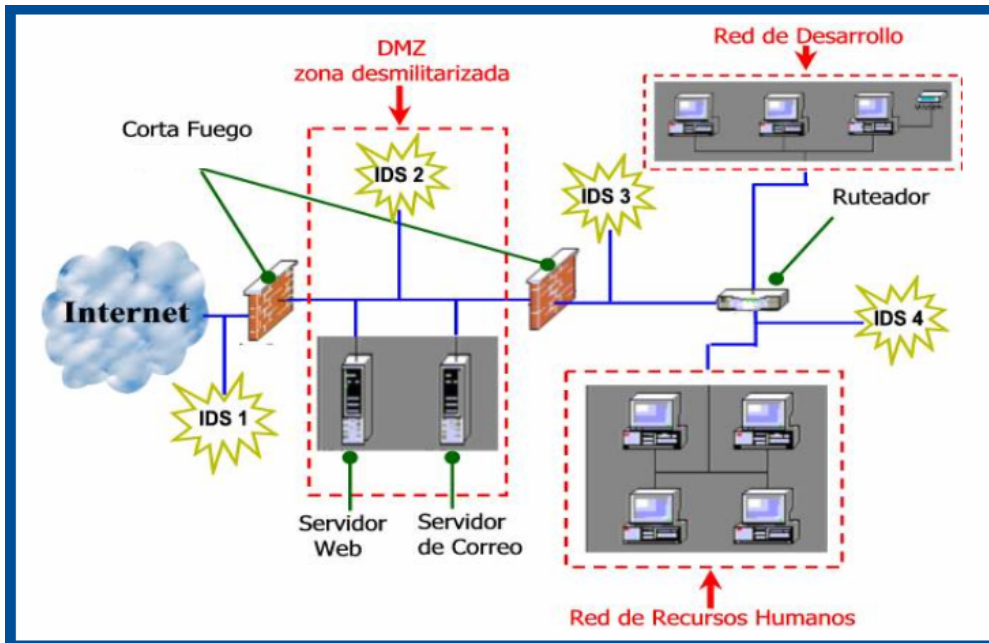


Figura 5.5. Ejemplo de integración en una red.

## 6. Seguridad en servicios Web

### 6.1 Introducción

La seguridad en Internet se puede desarrollar a nivel de aplicación (ej: SSH, PGP, S/MIME, ...) transporte (TLS) y red (IPSec). En la actualidad, la seguridad a nivel de transporte, utilizando TLS es la más empleada, puesto que es la usada en servicios Web seguros. Es por ello, que en este capítulo se detalla este tipo de soluciones, presentando la seguridad a nivel de red en el anexo C.

### 6.2 Conceptos básicos de TLS

El protocolo TLS (*Transport Layer Security*) ha sido diseñado para proporcionar confidencialidad, integridad y autenticación en las comunicaciones que se realizan a través de Internet de forma que sea independiente de los protocolos de aplicación que lo utilizan, aunque típicamente se utiliza en aplicaciones Web. Las características que tienen las comunicaciones que utilizan TLS son las siguientes:

- La conexión es privada. El cifrado se utiliza después de una “negociación inicia” para definir una clave simétrica secreta. La criptografía simétrica se utiliza para el cifrado de los datos (DES, AES, etc.)
- El uso de certificados digitales permite garantizar la identidad de sus emisores.
- La comunicación es íntegra. El transporte del mensaje incluye una comprobación de la integridad del mensaje. Para ello se usan funciones hash seguras (SHA-1, MD5, etc.)

TLS se basa en la especificación de SSL 3.0 publicada por Netscape. Aunque las diferencias con éste no son grandes, sí son lo suficientemente significativas para que no pueda existir interoperabilidad entre ambos protocolos, aunque TLS incorpora un mecanismo que le permite funcionar como SSL 3.0.

#### 6.2.1 ¿QUÉ ES EL PROTOCOLO TLS?

El protocolo TLS ha sido universalmente aceptado como el protocolo estándar de autenticación y comunicación cifrada entre clientes y servidores a través de la web

El transporte y encaminamiento de datos en Internet siguen los estándares establecidos mediante los protocolos TCP e IP (Transmission Control Protocol/Internet Protocol). Otros protocolos como HTTP, LDAP o IMAP pueden ser interpretados como usuarios de TCP/IP para realizar tareas propias de Internet como mostrar paginas web o acceder a la gestión del correo electrónico.

El servicio de autenticación en el servidor permite “firmar” los datos transmitidos utilizando algoritmos de criptografía de clave pública que permiten al cliente comprobar que el certificado y la clave pública del servidor (conceptos vistos en el capítulo 4) son los que pretenden ser y que han sido emitidos por una autoridad de certificación (AC) que está registrada por el cliente como una de las autoridades de certificación fiables. Esta autenticación puede ser crítica en aquellos casos en los que por ejemplo, es necesario enviar los datos de la tarjeta de crédito a un servidor y queremos asegurarnos de que el receptor es en realidad quien dice ser.

Por otra parte, en el cliente, la autenticación permite que el servidor pueda comprobar la identidad real del cliente. Los mecanismos de chequeo son los mismos que en el caso del servidor y la autenticación se realiza comprobando que el cliente posee una certificación expedida por una AC que está registrada por el servidor. Habitualmente, sólo el servidor es

autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes.

Además, hay que reseñar que cualquier conexión TLS requiere que la información enviada sea cifrada por el emisor y que pueda ser descifrada por el receptor. Esta información debe ser robusta a alteraciones “tampering” para garantizar la confidencialidad e integridad de los datos entre los dos interlocutores.

TLS está compuesto por dos sub-protocolos: el subprotocolo TLS de registro y el subprotocolo TLS de negociación o “handshake”. El subprotocolo de registro define el formato utilizado para la transmisión mientras que el subprotocolo de negociación se encarga de intercambiar una serie de mensajes ente el servidor TLS y el cliente TLS al iniciarse la conexión. Es decir, antes de intercambiar los datos de usuario, se ejecuta el protocolo de negociación, cuyas principales funciones son las siguientes:

- Autenticar al servidor frente al cliente, y opcionalmente autenticar al cliente frente al servidor. Para ello se hace uso de los certificados digitales.
- Negociar entre cliente y servidor el algoritmo que se usará en la comunicación.
- Generar una clave secreta de sesión TLS (que será utilizada por el protocolo de registro para el cifrado de los datos de usuario).

El proceso de negociación o “handshake” es explicado con más detalle en el punto 6.2.3 del presente capítulo.



Figura 6.1 Estructura de protocolos

### 6.2.2 Algoritmos criptográficos soportados por TLS

El protocolo TLS soporta la utilización de diversos algoritmos criptográficos para la autenticación mutua, la transmisión de certificados o el establecimiento de las claves de sesión entre otras operaciones.

Cliente y servidor pueden soportar algoritmos de cifrado muy dispares dependiendo de factores muy diversos: versión TLS soportada, suministrador de claves o sometimiento o no a los estándares de exportación de encriptación de algunos países como Estados Unidos. Es función del protocolo de negociación determinar como deben ponerse de acuerdo las partes a la hora de seleccionar el algoritmo común de cifrado más adecuado. Algunos de los algoritmos de cifrado más utilizados por TLS son los siguientes:

- Criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza;
- Cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard);
- Funciones hash: MD5 o de la familia SHA.

Los algoritmos de intercambio de clave como RSA determinan la manera en que servidor y cliente acuerdan claves simétricas que utilizarán durante toda la sesión TLS.

### 6.2.3 El sub-protocolo de negociación o “handshake”

El protocolo SSL utiliza mecanismos criptográficos simétricos y de clave pública. El cifrado simétrico es mucho más rápido que el de clave pública pero como contrapartida ésta última facilita enormemente el proceso de autenticación. Una sesión TLS siempre se inicia con un intercambio de mensajes del protocolo TLS de negociación o “handshake”. La negociación permite al servidor identificarse de cara al cliente utilizando técnicas de clave pública y así posteriormente cliente y servidor pueden cooperar para la generación de claves simétricas utilizadas para un rápido cifrado/descifrado y protección frente a la alteración de datos o “tampering”. Como ya se ha comentado, una vez decidido este punto, opcionalmente se puede proceder a la autenticación del cliente frente al servidor.

Los pasos seguidos durante el protocolo de negociación son los siguientes:

1. El cliente envía al servidor su número de versión TLS, los parámetros de cifrado, datos generados aleatoriamente y otra información que el servidor necesita para comunicar con el cliente utilizando TLS.
2. El servidor envía al cliente su número de versión TLS, los parámetros de cifrado, datos generados aleatoriamente y otros datos que el cliente necesita para comunicarse con el servidor utilizando TLS. Además el servidor envía su propio certificado y, (si está configurada la opción de identificación de cliente), una petición de identificación por parte del cliente.
3. El cliente utiliza parte de la información recibida para autenticar al servidor (ver autenticación del servidor en el punto 6.2.4 de este capítulo). Si el servidor no puede ser identificado correctamente, se envía un aviso al usuario informando acerca de la imposibilidad de establecer conexión. En caso contrario se sigue con el punto 4.
4. A partir de todos los datos generados tras la negociación, el cliente (en cooperación con el servidor, dependiendo del código de cifrado utilizado) crea la plantilla provisional o “premaster” de la sesión. Este premaster se cifra con la clave pública del servidor (contenida en su certificado) y se le envía a él propiamente.
5. Si el servidor (opcionalmente) ha enviado una petición de identificación al cliente, éste debe firmar digitalmente otra sección de datos aleatorios enviados y conocidos por ambas partes. En este caso, el cliente envía los datos firmados digitalmente además de su propio certificado y el premaster.
6. Si el servidor (opcionalmente) ha solicitado autenticación del cliente, tratará de realizar el proceso de autenticación (ver punto 6.2.6 del presente capítulo). En el caso de que esta operación no finalice con éxito, la sesión termina, mientras que si se consigue autenticar al cliente, el servidor utiliza la clave privada de éste para descifrar el premaster. Tras el descifrado, se realizan una serie de pasos en colaboración con el cliente encaminados a la generación de la plantilla definitiva o “master” de la sesión.
7. Cliente y servidor utilizan este master para generar las claves de la sesión TLS que son claves simétricas y que se utilizarán para cifrar y descifrar la información que viaje por la red, garantizando la confidencialidad e integridad de los datos.
8. El cliente envía un mensaje al servidor notificando que cualquier información posterior será cifrada con las claves simétricas generadas. Además también

envía otro mensaje (ya cifrado con las claves de la sesión) donde da por finalizado el sub-protocolo de negociación.

9. El servidor realiza exactamente la misma operación que la realizada por el cliente en el punto anterior.
10. El sub-protocolo de negociación ha concluido y empieza el sub-protocolo de registro. Cliente y servidor se intercambiarán datos a partir de ahora cifrados con las claves de la sesión y utilizarán dichas claves para garantizar la integridad y confidencialidad de la información.

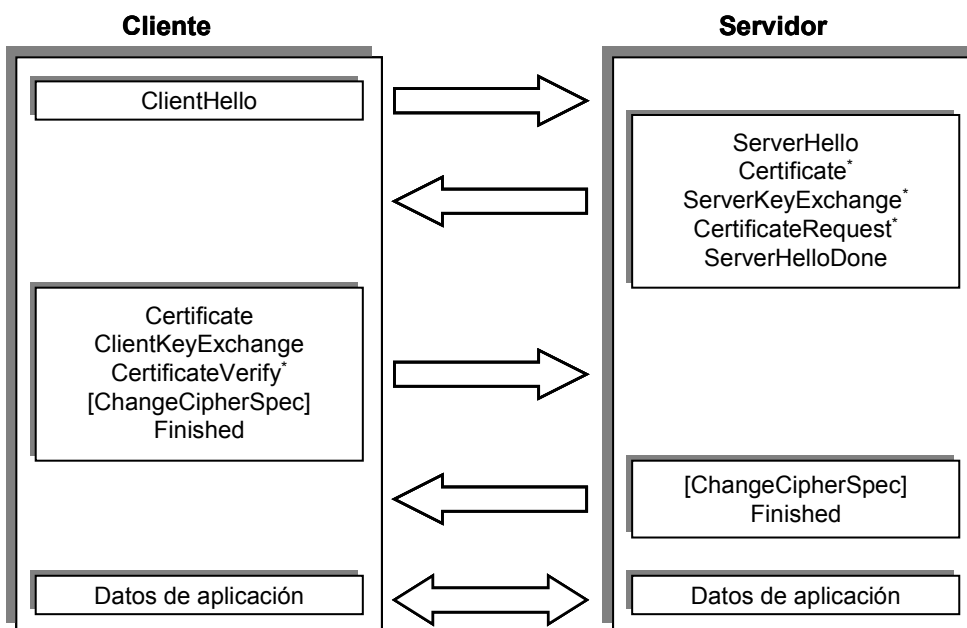


Figura 6.2 Protocolo de handshake o negociación

Llegados a este punto es importante aclarar que la autenticación de ambos interlocutores precisa del cifrado de datos con una de las dos claves del par clave pública/clave privada y el descifrado de esos mismos datos con la otra clave sobrante. En el caso de la autenticación del servidor, el cliente cifra la plantilla provisional (premaster) con la clave pública del servidor. Solo la clave privada de éste podrá, pues, descifrar la información. De esta manera el cliente se asegura de que el servidor es realmente quien dice ser ya que en caso contrario no podría descifrar el premaster y la sesión TLS no podría completarse de manera satisfactoria.

En el caso de la autenticación del cliente, el proceso es este:

- a): El cliente cifra algunos datos aleatorios con su clave privada (firma digital).
- b): El servidor busca en su repositorio de certificados el correspondiente a dicho cliente.
- c): El servidor valida la firma digital que le llega con la clave pública incluida en el certificado del cliente que estaba en el repositorio.

Nuevamente no hay posibilidad de que una tercera parte suplante la identidad del cliente ya que no sería posible que el servidor descifrara una firma digital realizada con otra clave privada distinta de la correcta. (Clave privada asociada a la clave pública que tiene registrada el servidor)

### 6.2.3.1 Proceso de autenticación del servidor

El cliente TLS siempre solicita autenticación por parte del servidor. Como ya se ha explicado en el punto 2 del protocolo de negociación, (6.2.3) el servidor envía al cliente su certificado y éste se encarga de validar la identidad.

Para comprobar la correspondencia entre la clave pública contenida en el certificado del servidor y la identidad de éste, el cliente realiza un pequeño protocolo consistente en cuatro preguntas que deben ser contestadas positivamente. Aunque estas preguntas no forman parte rigurosamente del protocolo TLS si que es necesario que el software del cliente las soporte para asegurar la identidad del servidor con el que conecta. Como veremos posteriormente en el punto 6.2.5, este mini-protocolo evita una conocida técnica de ataque al sistema de seguridad llamada "Man-in-the-Middle".

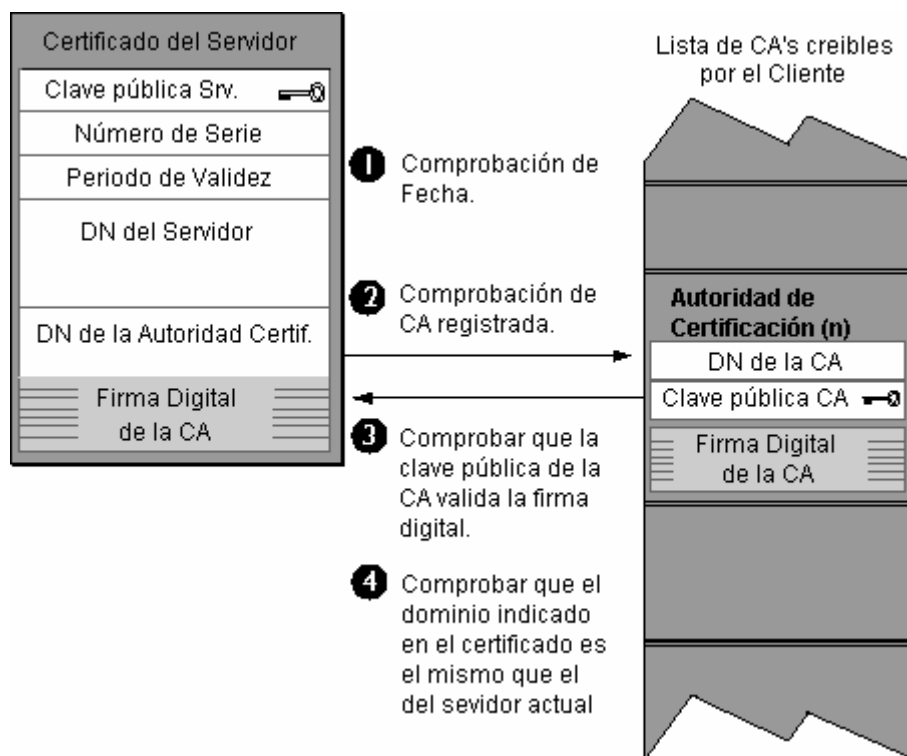


Figura 6.3 Modelo de autenticación del certificado de servidor por el cliente

Las etapas que sigue el cliente para autenticar al servidor son la siguientes.

1. Comprobación de la validez temporal del certificado. El cliente comprueba que las fechas de inicio y finalización de validez contenidas en el certificado del servidor comprenden la fecha actual.
2. Comprobación de Autoridad de Certificación (AC). El cliente mantiene una lista de certificados de AC en los que cree. Esta lista determina que certificados de servidor son aceptados por el cliente. Si el nombre de la AC coincide con el nombre de algún miembro de la lista de AC's fiables por el cliente, el resultado de la comprobación es positivo.

3. Comprobación de que la clave pública del certificado de la AC valida la firma digital ofrecida por el servidor. El cliente utiliza la clave pública que tiene en el certificado de la lista de AC's fiables para validar la firma digital de la supuesta AC que firma el certificado del servidor. Si la información del certificado del servidor ha cambiado desde que se realizó la firma digital por parte de la AC o si la clave pública contenida en el certificado de la AC no corresponde con la clave privada de la AC con la que fue firmado el certificado del servidor, la autenticación no puede ser completada. Si la firma de la AC puede ser validada, el certificado se utiliza como carta de presentación y se continua el proceso. Llegados a este punto, el cliente da como válido el certificado y es su responsabilidad continuar o no con el siguiente punto.
4. Comprobación de dominio. Se comprueba que el dominio mostrado en el certificado del servidor y el dominio en el que se encuentra el servidor con el que se conecta sea el mismo. Este paso no es parte del protocolo de autenticación propiamente dicho pero previene de ataques basados en el sistema "Man-in-the-Middle" (Ver apartado siguiente). Los clientes deben realizar este paso y rechazar, si procede, la autenticación de servidores que se encuentren en dominios diferentes de los indicados en su certificado.

Una vez identificado y autenticado el servidor, el cliente continua con el proceso de negociación. En caso contrario se envía una excepción al usuario indicando que una conexión cifrada y autenticada no puede ser establecida.

Tras realizar todos los pasos que han sido descritos aquí, el servidor puede utilizar su clave privada para descifrar el premaster o plantilla provisional que le envía el cliente (paso 4 del protocolo de negociación) con lo que hay una iteración más de seguridad que relaciona la clave pública del certificado mostrado con la clave privada utilizada para el descifrado y que no ha sido validada previamente.

#### **6.2.3.2 Técnica de ataque "man-in-the-middle"**

Como se ha sugerido en el punto 4 del apartado anterior, la comprobación de dominio del servidor previene los ataques basados en la técnica "Man-in-the-Middle". La técnica "Man-in-the-Middle" no es más que un programa que intercepta la comunicación entre cliente y servidor capturando las claves legítimas intercambiadas durante el proceso de negociación de la sesión TLS.

Una vez capturadas las claves, el intruso las sustituye por las suyas propias de manera que aparenta ser el servidor de cara al cliente y viceversa. La información cifrada que se intercambia en el protocolo de negociación está cifrada de hecho con las claves pública o privada de este programa ilegal de manera que en realidad establece dos sesiones distintas, una con el servidor y otra con el cliente, (ambas sesiones están establecidas con claves de sesión distintas). Esta técnica permite, no sólo acceder a los datos emitidos, sino alterarlos sin que el receptor pueda detectarlo. Es por ello por lo que es extremadamente importante para el cliente la comprobación de que el dominio indicado en el certificado es el mismo que el dominio donde está la máquina con la cual se está realizando la comunicación (además de los otros pasos comentados en los puntos anteriores).

#### **6.2.3.3 Autenticación del cliente**

Como ya se ha apuntado con anterioridad, el servidor puede ser configurado para que solicite al cliente confirmación de su identidad. Cuando esta opción está habilitada, (ver apartado 6 del protocolo de negociación), el cliente envía al servidor su certificado y una

porción de datos firmados digitalmente con su clave privada para facilitar la identificación. El servidor utiliza los datos firmados para validar la clave pública del certificado del cliente y asegurar la autenticidad del mismo.

El protocolo TLS requiere que el cliente cree una firma digital a partir de un código hash que obtiene por medio de la secuencia de datos aleatorios. Estos datos aleatorios sólo son conocidos por el servidor y el cliente y son intercambiados en el proceso de negociación. Una vez obtenida la secuencia hash, se cifra con la clave privada que corresponde con la clave pública que está en el certificado que se le presenta al servidor.

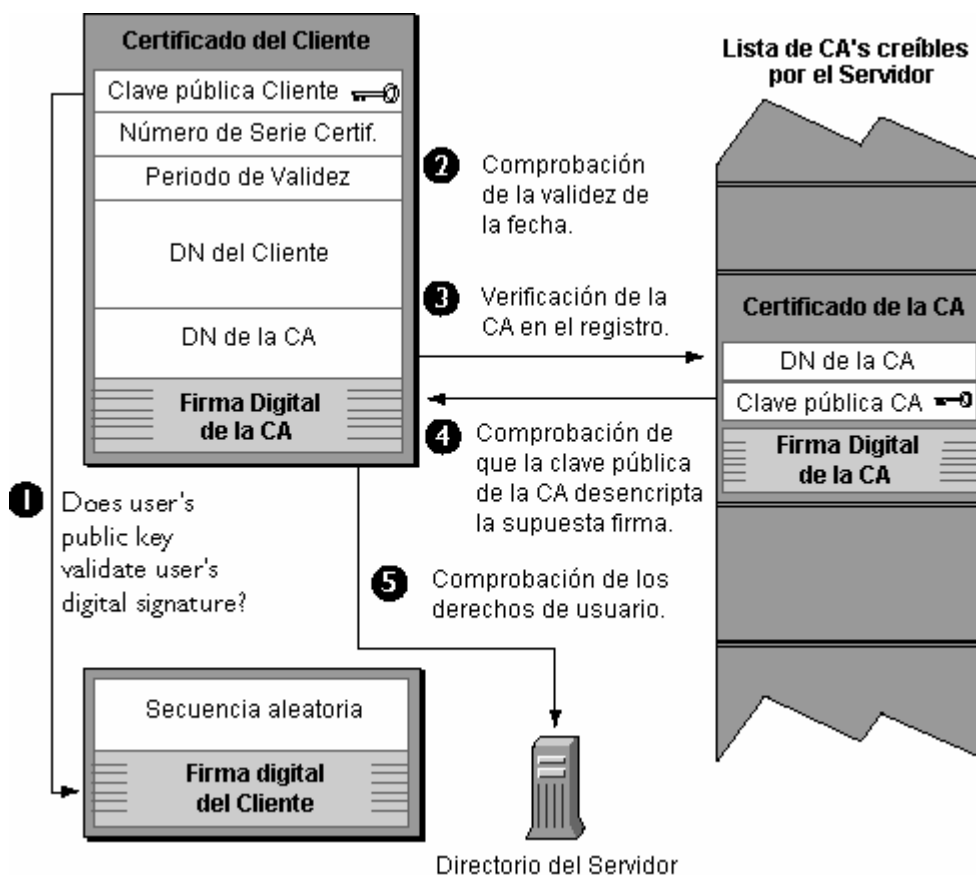


Figura 6.4 Modelo de autenticación del cliente por parte del servidor.

Los pasos seguidos por el servidor para autenticar al cliente son los siguientes:

1. Comprobar que la clave pública valida la firma digital. El servidor chequea que la firma digital puede ser validada con la clave pública incluida en el certificado que ha enviado el cliente. En caso afirmativo el servidor asume que la clave pública del certificado corresponde con la clave privada de cifrado de la firma digital y que los datos no han sido modificados desde la firma. En este punto, no obstante, la conexión entre la clave pública y el nombre de la autoridad certificadora que se especifica en el certificado no ha sido establecida aún y por tanto hay que considerar la posibilidad de que el certificado haya sido creado por alguna entidad que desea suplantar al cliente. Para validar este punto, es necesario completar los puntos 3 y 4.

2. Comprobar que la fecha de validez del certificado comprende la fecha de hoy. Este paso es el mismo que el realizado en el caso de la validación de servidor.
3. Comparación entre la autoridad de certificación que firma el certificado y la lista de AC's fiables. Cada servidor mantiene una lista de autoridades de certificación en las cuales confía y que determinan los certificados que el servidor creará o no. Si el nombre de la AC no se encuentra en la lista de AC's, ocurre lo mismo que en el caso de la autenticación de los clientes, y la única posible autenticación proviene de la posibilidad o no del servidor de consultar la jerarquía de AC's.
4. Comprobar que la clave pública de la autoridad de certificación valida la firma digital del cliente. El servidor utiliza la clave pública que se encuentra en el certificado correspondiente de su lista de AC's y la utiliza para validar la firma presente en el certificado del cliente. Si los datos han sido modificados posteriormente a la firma o la clave pública no corresponde con la clave privada utilizada para la firma, la autenticación no se lleva a cabo. Por otra parte si la identificación es positiva el certificado se considera válido y es un carta de presentación del cliente. Si esto ocurre se realiza el paso siguiente.
5. Verificar que el cliente autenticado está autorizado a acceder a los recursos que solicita. En este punto el servidor comprueba los recursos a los que tiene acceso el cliente a partir de las listas de control de acceso del servidor (ACL's) y establece la conexión en consecuencia. Si por algún motivo el usuario no puede ser autenticado en estas listas, no podrá acceder a ningún recurso del servidor que requiera permisos especiales.

#### 6.2.4 Protocolo de registro: transferencia de datos

El protocolo de registro es el utilizado para intercambiar los datos entre cliente y servidor. En la figura 6.5 se puede observar un esquema del manejo y el flujo de los datos dentro de esta capa.

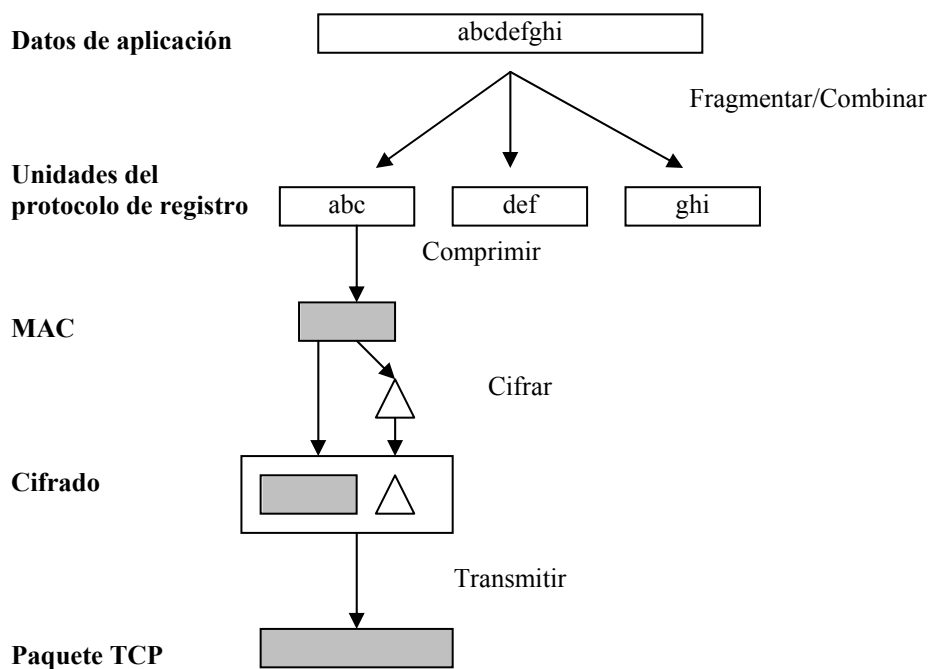


Figura 6.5. Protocolo de registro

¿Cómo funciona la seguridad en Internet?

Lo primero que hace es fragmentar los datos que le proporciona la aplicación en unidades más pequeñas. Luego comprime cada una de estas (opcionalmente y sólo en teoría ya que en la actualidad no existe ningún navegador -el encargado de las capas superiores hasta en TCP- que ofrezca la posibilidad de comprimir dichas unidades). Una vez comprimida se realiza un hash (MAC) que será utilizado más tarde con el fin de verificar la integridad de la unidad. Todo junto se encripta (unidad + hash) y se transmite.

En recepción se utiliza el proceso inverso. Luego, si por alguna razón los hashes no coincidiesen, entonces se generaría un mensaje de alerta a través del protocolo de alerta.

## 7. Comercio electrónico seguro

Se puede definir comercio electrónico como: intercambio electrónico de datos e informaciones correspondientes a una transacción. Sin embargo, dependiendo de cada caso, puede tener diferentes definiciones:

- Desde el punto de vista de las comunicaciones es el transporte de información, productos/servicios o pagos, mediante líneas telefónicas y redes de ordenadores.
- Desde la perspectiva de las empresas, es una aplicación de las nuevas tecnologías para la automatización de las transacciones entre organizaciones.
- Desde la perspectiva de los servicios, es una herramienta que presenta la oportunidad de rebajar los costes, al tiempo que se aumenta la calidad y la velocidad del servicio prestado.
- Finalmente, desde el punto de vista del internauta, es la posibilidad de comprar y vender productos y servicios en Internet, sin tener que desplazarse.

En realidad, el comercio electrónico no incluye sólo la compra y venta electrónica de bienes, información o servicios, sino también el uso de la red para actividades anteriores o posteriores a la venta como son la publicidad, búsqueda de información sobre productos, proveedores, etc., atención al cliente antes y después de la venta...

Para que el comercio electrónico se desarrolle debe crearse un ambiente de confianza para todos los participantes. El auge de la banca online ya es un hecho real, cada día hay mas personas que acceden y usan este servicio para realizar sus transferencias bancarias, pagos, consultas etc. Por este motivo no tenemos que bajar la guardia en cuanto a "proteger" nuestras operaciones bancarias de posibles manipulaciones, de posibles robos de nuestras finanzas y salvaguardar nuestros datos, tal y como hacemos diariamente en la vida normal o "no virtual".

En el mundo informático, en cuanto al dinero, el peligro es muy similar al que podemos encontrarnos en el mundo "tangible". El único problema es el desconocimiento por parte del usuario; tomando las precauciones adecuadas es incluso comparativamente más seguro. Igual que no se nos ocurre perder de vista nuestra tarjeta de crédito cuando compramos, o que miramos bien antes de sacar dinero de un cajero automático y tenemos cuidado de que nadie vea nuestra clave al teclearla en esos terminales, etc. pues lo mismo ocurre con las transacciones a través de internet. Debemos por tanto quitarnos ese "miedo" y tomar como rutina una serie de pasos para que podamos estar seguros y nuestro dinero a salvo de ladrones.

### 7.1 Ventajas e inconvenientes del comercio electrónico

Evidentemente el comercio electrónico, en su situación actual y en cualquiera de sus modalidades, presenta ventajas e inconvenientes, que se resumen a continuación:

#### Para el cliente

A modo de resumen tiene las siguientes ventajas:

- Evita desplazamientos, ahorra tiempo y puede ahorrar dinero.
- Es un medio interactivo que permite comparar precios y obtener información sobre vendedores y artículos.
- Es espontáneo.

Y los siguientes inconvenientes:

- Existen problemas de seguridad.

¿Cómo funciona la seguridad en Internet?

- Las comunicaciones en España son lentas y caras.
- No es posible comprar todo en la Red

### **Para el comerciante**

A modo de resumen tiene las siguientes ventajas:

- Permite acceder a nuevos mercados con nuevos negocios.
- Permite acceder a nuevos mercados en español.
- Supone una mejora en las acciones y comunicaciones de marketing.
- Ahorra de infraestructuras físicas, tiendas, etc.
- Permite mejorar la relación con el cliente.
- Situación de igualdad con las grandes empresas.
- Modernización de las estructuras organizativas.

Y los siguientes inconvenientes:

- Exige una nueva estrategia, plan de negocio y elegir bien los productos.
- Exige montar una logística de distribución.
- Exige llegar a nuevos acuerdos con los proveedores.
- Exige nueva infraestructura “electrónica” en un entorno tecnológico muy cambiante.
- Existen nuevos intermediarios.
- Insuficiente uso de Internet en España y escasa costumbre de compra electrónica.
- Nuevos entrantes en los mercados locales.

## **7.2 Modelos de comercio**

El comercio electrónico sólo contempla la información concerniente a la entrega del producto por un vendedor a un comprador, es decir, información sobre fecha de flete, número de expedición, nombre del transportista, etc., y en dirección contraria, los datos correspondientes al pago del producto. La entrega física del producto, si es tangible, se realiza en otro momento.

En este modelo, la entrega del producto vendido, si no es tangible, ha sido substituida por un conjunto de información que hace referencia a la descripción del producto y a su entrega, fecha de envío, etc.

El comercio electrónico elimina la comunicación física entre comprador y vendedor, la cual queda substituida por un flujo de información que describe las características del bien vendido. Dicho flujo, se produce también en los dos sentidos, ya que el comprador también facilita información al vendedor.

El comercio electrónico implica unos determinados cambios a todos los niveles, incluso sociales. Entre otros, desaparecen (especialmente en el B2C, Business to Consumer) los intermediarios clásicos, ya que la compra es directa. Sin embargo, aparecen otros nuevos intermediarios clasificados de la siguiente forma:

- Tecnología: expertos en informática y telecomunicaciones.
- Información: expertos en catálogos, directorios y buscadores.
- Acceso a la Red: proveedores de sitio en la red, hosting.
- Logística y distribución: expertos en la distribución de productos.
- Medios de pago: pasarelas con bancos y emisores de tarjetas de crédito.

- Seguridad y certificación: entidades y sistemas que aseguran la confidencialidad de las comunicaciones.

### **7.3 Necesidades, requisitos y riesgos**

El comercio electrónico se desarrolla dentro de un entorno de comunicaciones en un ambiente:

- Hostil
- Vulnerable
- Con desconfianza mutua entre los comunicantes

El Comercio electrónico necesita mecanismos eficaces para garantizar la privacidad y la seguridad de las redes abiertas. Estos mecanismos deben proporcionar confidencialidad, autenticación y fidelidad o no repudio, es decir, información encriptada, permitir a cada parte que intervenga en una transacción asegurar la identidad de la otra parte, y asegurar que las partes que intervienen en una transacción no puedan posteriormente negar su participación, respectivamente. Ya que el reconocimiento de mecanismos de seguridad y privacidad depende de certificaciones de una tercera parte cualificada (tales como el cuerpo gubernamental), el comercio electrónico requiere el establecimiento de un sistema de certificación global.

A modo de resumen son necesarios estos cuatro requisitos:

- Privacidad (confidencialidad). Un usuario no autorizado no puede conocer el contenido.
- Autenticidad. El destinatario tiene la certeza de que la comunicación proviene del origen supuesto.
- La integridad de la información transmitida en cada sentido.
- No repudio (verificabilidad) una vez aceptada. El destinatario tiene la capacidad de demostrar ante terceros el contenido y procedencia de una comunicación.

Es por medio de la criptografía como se consiguen los requisitos anteriores. Sin embargo, existen diversos ataques para romperlos. Sobretodo hay que vigilar los ataques a la información que rompen los sistemas criptográficos conocidos como criptoanálisis (violación de los sistemas criptográficos).

### **7.4 Métodos de pago y seguridad: los participantes**

El tema del pago en redes abiertas ha adquirido una gran relevancia en los últimos años debido al creciente desarrollo del comercio electrónico. Los sistemas de pago electrónicos deben proporcionar la infraestructura necesaria para facilitar el pago en las transacciones realizadas a través de la red Internet. Son tan importantes y necesarios que, de no llegar a soluciones satisfactorias, el desarrollo del comercio electrónico se podría ver seriamente frenado.

Sin duda uno de los más importantes temores de los usuarios es la seguridad, relacionada con el envío por la red de los datos de las tarjetas de crédito. Si se realiza una compra en Internet utilizando una tarjeta de crédito como medio de pago, la transacción comercial se ordena en la red, pero la validación y la realización efectiva del pago se efectúan a través de los circuitos tradicionales de procesamiento de las operaciones con tarjeta de crédito. Los que intervienen son los siguientes actores:

- El comprador.
- El vendedor (merchant).
- El banco emisor (issuer) de la tarjeta de crédito o débito que presenta el cliente.

- El banco (acquirer) que recibe la transacción en nombre del vendedor y en el que reside la cuenta en la que a éste se le va a liquidar el pago.
- La red de medios de pago como por ejemplo VISA.

TLS es un protocolo generalista para intercambios seguros utilizando el protocolo de transporte TCP. La gran mayoría de sistemas de pago utilizados actualmente para efectuar pagos a través de Internet, utilizan TLS para proteger los datos.

Básicamente podemos encontrar tres tipos de arquitectura: la lineal, la triangular y el modelo 3D (tres dominios).

### 7.4.1 Arquitectura lineal

La arquitectura lineal (figura 7.1) es la implementación en Internet del comercio tradicional. El procedimiento es el siguiente:

- Se accede a la página Web. Se busca el producto y finalmente se compra, es decir, realiza el pedido.
- Una vez realizado el pedido, el comprador proporciona su número de tarjeta al vendedor a través de la cumplimentación de un formulario en la Red.
- El servidor donde reside la aplicación del vendedor envía la transacción al banco que actúa en nombre del vendedor. Este envío suele producirse fuera de la red pública, en forma análoga a como se produciría desde un terminal punto de venta (TPV) que existiese en una tienda física o real.
- El banco asociado al vendedor pide autorización al banco emisor de la tarjeta, a través de la red de medios de pago.
- Si la transacción se autoriza, se realiza la transferencia de dinero desde la cuenta del comprador en el banco emisor hasta la cuenta del vendedor.

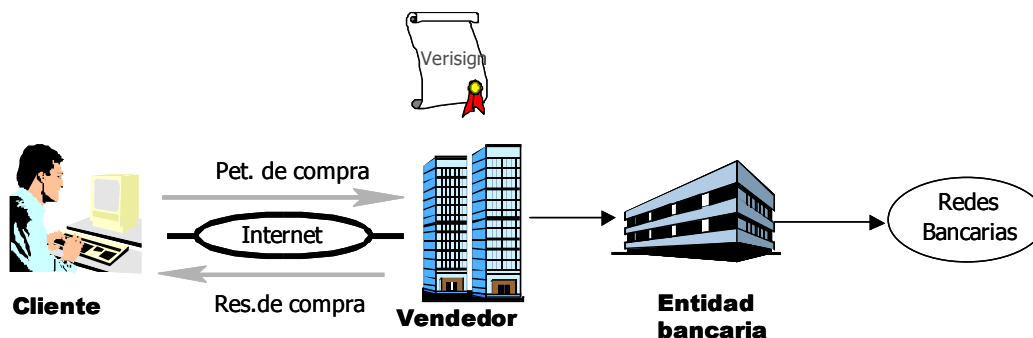


Figura 7.1. Modelo de pago con arquitectura lineal.

Este esquema presenta, entre otros, los siguientes inconvenientes:

- Aunque durante el transporte la confidencialidad e integridad de los datos está garantizada por el uso de TLS, el comercio podría modificar los datos antes de transmitirlos a la entidad financiera.
- El comprador no se autentica. Este es el tipo de más habitual. El hecho de conocer un determinado número de tarjeta y su fecha de caducidad no garantiza ser el propietario de aquella tarjeta. Este aspecto se solucionaría con certificados para todos los participantes.

### 7.4.2 Arquitectura triangular

La arquitectura triangular (figura 7.2) resulta de la evolución de la anterior, con el objetivo de resolver algunos de los problemas de seguridad mencionados. La siguiente figura ilustra todo el proceso.

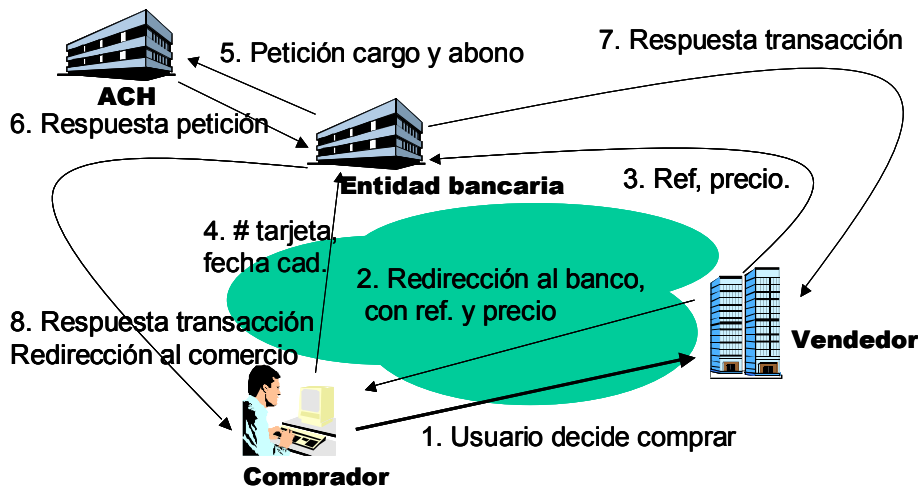


Figura 7.2. Modelo de pago con arquitectura triangular.

A modo de resumen, podemos decir que la principal diferencia radica en el hecho que el comercio redirecciona al comprador hacia la pasarela de pago cuando decide comprar tras asignar una referencia a la operación. El comprador introduce sus datos financieros en la pasarela, de manera que el comercio no puede acceder a ellas. En paralelo el comercio también se comunica con la pasarela y le indica la referencia y el precio. La pasarela de pago verifica que los datos que le llegan del comprador y del comercio (referencia de compra y precio) coinciden, garantizando de esta forma la integridad. Sin embargo, el problema de autenticación sigue presente en este esquema.

### 7.4.3 Modelo 3 dominios

La idea básica es la siguiente: El comprador debe utilizar una red insegura para poder efectuar el pago. El principal problema, como se ha visto anteriormente, es la falta de mecanismos (prácticos, ya que a nivel teórico el certificado de usuario lo podría resolver) para llevar a cabo la autenticación del cliente o comprador. La solución adoptada consiste en el uso concatenado de los tres dominios en que hay confianza entre los participantes. Así pues, cuando se desea realizar la compra los pasos a seguir son los siguientes:

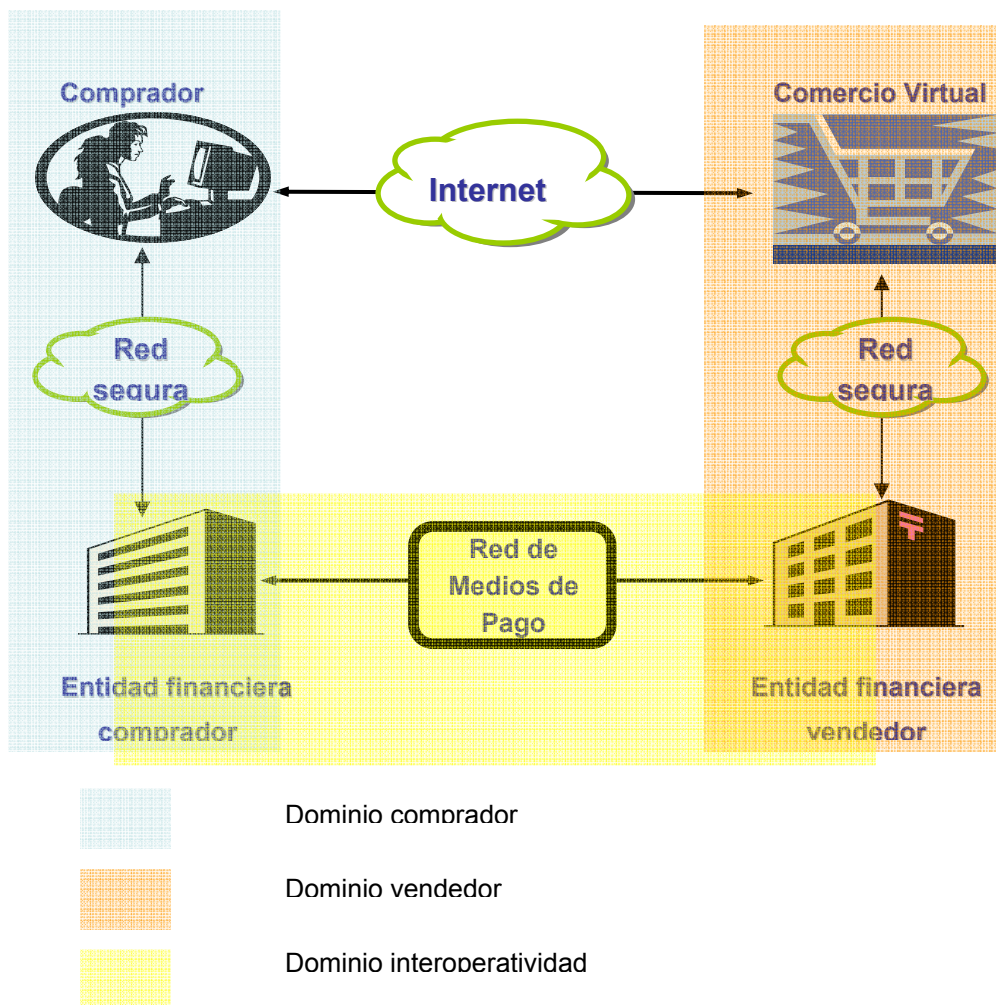


Figura 7.3. Modelo de confianza en la arquitectura 3 dominios

- El comprador selecciona los productos deseados y se le indica el importe. Cuando está de acuerdo en la compra, pulsa el botón correspondiente.
- El comercio redirecciona al comprador hacia una pasarela de pago de la entidad financiera con la que trabaja el vendedor (acquirer). En dicha pasarela, el comprador introducirá el número de su tarjeta financiera.
- Una vez se han introducido esos datos, en función del número de tarjeta se invoca al emisor correspondiente y éste pide datos de autenticación (apertura de ventana pop-up). Es decir, el cliente se encuentra frente a una ventana correspondiente a su propia entidad financiera.
- El cliente se autentica y recibe una firma de la operación. La autenticación se puede hacer de la forma que dicha entidad financiera establezca (ej. CIP, código de identificación personal, Móvil IVR: llamada de voz a un móvil, Móvil USSD: llamada de datos a un móvil, Link a la Banca Virtual del emisor, Certificado X-509...)
- El cliente hace llegar la firma al comercio, que inicia una petición de autorización a su entidad financiera.

Dicha entidad financiera solicita autorización a la entidad financiera del comprador, acompañada de la firma correspondiente. Si todo el proceso ha sido correcto, se autoriza la operación, y se le comunica al vendedor.

La figura 7.3. muestra la idea básica de confianza en el modelo 3D (tres dominios)

Aunque estos son los sistemas de pago electrónico más habituales, también existen otros como son:

- El contrareembolso. Único medio que incluye dinero en metálico.
- El cargo en cuenta.
- Las tarjetas chip de prepago o tarjetas inteligentes (smart card). Requieren la incorporación en el equipo informático de un dispositivo especial para leerlas (lector de tarjetas inteligentes).
- El dinero electrónico o dinero virtual. Idea parecida a la anterior pero el dinero no reside en la tarjeta.

## 8. Herramientas del hacker

Es difícil describir el ataque "típico" de un hacker debido a que los intrusos poseen diferentes niveles de técnicos por su experiencia y son además son motivados por diversos factores. Algunos hackers son intrigosos por el desafío, otros mas gozan de hacer la vida difícil a los demás, y otros tantos substraen datos delicados para algún beneficio propio.

### 1. Recolección de información

Generalmente, el primer paso es saber en que forma se recolecta la información y además que tipo de información es. La meta es construir una base de datos que contenga la organización de la red y coleccionar la información acerca de los servidores residentes. Esta es una lista de herramientas que un hacker puede usar para coleccionar esta información:

- El programa TraceRoute puede revelar el número de redes intermedias y los routers en torno al servidor específico.
- El protocolo Whois que es un servicio de información que provee datos acerca de todos los dominios DNS y el administrador del sistema responsable para cada dominio. No obstante que esta información es anticuada.
- Los Servidores DNS nos pueden permitir obtener una lista de las direcciones IP y sus correspondientes Nombres (Programa Nslookup).
- El protocolo Finger puede revelar información detallada acerca de los usuarios (nombres de login, números telefónicos, tiempo y última sesión, etc.) de un servidor en específico.
- El programa Ping puede ser empleado para localizar un servidor particular y determinar si se puede alcanzar. Esta simple herramienta puede ser usada como un programa de escaneo pequeño que por medio de llamadas a la dirección de un servidor haga posible construir una lista de los servidores que actualmente son residentes en la red.

### 2. Sondeo del sistema para debilitar la seguridad

Después que se obtienen la información de red perteneciente a dicha organización, el hacker trata de probar cada uno de los servidores para debilitar la seguridad. Estos son algunos usos de las herramientas que un hacker puede utilizar automáticamente para explorar individualmente los servidores residentes en una red:

- Una vez obtenida una lista de la vulnerabilidad de servicios en la red, un hacker bien instruido puede escribir un pequeño programa que intente conectarse a un puerto especificando el tipo de servicio que esta asignado al servidor en cuestión. La ejecución del programa presenta una lista de los servidores que soportan servicio de Internet y están expuestos al ataque.
- Existen varias herramientas del dominio publico, tal es el caso como el Rastreador de Seguridad en Internet (ISS) o la Herramienta para Análisis de Seguridad para Auditar Redes (SATAN) , que pueden rastrear una subred o un dominio y ver las posibles fugas de seguridad. Estos programas determinan la debilidad de cada uno de los sistemas con respecto a varios puntos de vulnerabilidad comunes en un sistema. El intruso usa la información recuperada por este tipo de rastreadores para intentar el acceso no-autorizado al sistema que quiere atacart. Un administrador de redes hábil puede usar estas herramientas en su red privada para descubrir los puntos más débiles en cuanto a su seguridad y así determinar que servidores necesitan mayor protección.

### 3. Acceso a sistemas protegidos

El intruso utiliza los resultados obtenidos a través de las pruebas para poder intentar acceder a los servicios específicos de un sistema. Después de conseguir el acceso al sistema protegido, el hacker tiene disponibles las siguientes opciones:

- Puede atentar destruyendo toda evidencia del asalto y además podrá crear nuevas fugas en el sistema o en partes subalternas con el compromiso de seguir teniendo acceso sin que el ataque original sea descubierto.
- Pueden instalar paquetes de sondeo que incluyan códigos binarios conocidos como "caballos de Troya" protegiendo su actividad de forma transparente. Los paquetes de sondeo colectan las cuentas y contraseñas para los servicios de Telnet y FTP permitiendo al hacker expandir su ataque a otras máquinas.
- Pueden encontrar otros servidores que realmente comprometan al sistema. Esto permite al hacker explotar vulnerablemente desde un servidor sencillo todos aquellos que se encuentren a través de la red corporativa.
- Si el hacker puede obtener acceso privilegiado en un sistema compartido, podrá leer el correo, buscar en archivos

En cuanto a ataques estilo phishing, algunas técnicas adicionales que pueden usar los atacantes para intentar engañar a los usuarios son:

- Man-in-the-middle (hombre en el medio). En esta técnica, el atacante se sitúa entre el usuario y el sitio web real, actuando a modo de proxy. De esta manera, es capaz de escuchar toda la comunicación entre ambos. Para que tenga éxito, debe ser capaz de redirigir al cliente hacia su proxy en vez de hacia el servidor real. Existen diversas técnicas para conseguirlo, como por ejemplo los proxies transparentes, el DNS Cache Poisoning (Envenenamiento de Caché DNS) y la ofuscación de URLs.
- Aprovechamiento de vulnerabilidades de tipo Cross-Site Scripting en un sitio web, que permiten simular una página web segura de una entidad bancaria, sin que el usuario pueda detectar anomalías en la dirección ni en el certificado de seguridad que aparece en el navegador.
- Aprovechamiento de vulnerabilidades del navegador en el cliente, que permiten mediante el uso de exploits falsear la dirección que aparece en el navegador. De esta manera, se podría redirigir el navegador a un sitio fraudulento, mientras que en la barra de direcciones del navegador se mostraría la URL del sitio de confianza. Mediante esta técnica, también es posible falsear las ventanas pop-up abiertas desde una página web auténtica. Algunos ataques de este tipo también hacen uso de exploits en sitios web fraudulentos que, aprovechando alguna vulnerabilidad del navegador o del sistema operativo del cliente, permiten descargar troyanos de tipo keylogger que robarán información confidencial del usuario

## 9. Anexo A. Algoritmo criptográfico RSA

### 9.1 Introducción

El algoritmo RSA fue diseñado en 1978 por Ron Rivest, Adi Shamir y Len Adleman en el MIT; las letras RSA son las iniciales de sus apellidos. El algoritmo fue patentado por el MIT en 1983 en Estados Unidos, patente que expiró el 21 de septiembre de 2000.

El sistema RSA se basa en el hecho matemático de la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más lógico consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4,..., y así sucesivamente, buscando que el resultado de la división sea exacto, es decir, de resto 0, con lo que ya tendremos un divisor del número.

Ahora bien, si el número considerado es un número primo (el que sólo es divisible por 1 y por él mismo), tendremos que para factorizarlo habría que empezar por 1, 2, 3,..... hasta llegar a él mismo, ya que por ser primo ninguno de los números anteriores es divisor suyo. Y si el número primo es lo suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo.

### 9.2 Generación de claves

El primer paso es la generación de la clave pública y privada del usuario. El proceso se basa en la exponenciación modular de exponente y módulo fijos, el sistema RSA crea sus claves de la siguiente forma:

1. Se buscan dos números primos grandes distintos,  $p$ , y  $q$  (de entre 100 y 300 dígitos).
2. Se obtiene  $n = p \cdot q$
3. Se calcula  $\varphi(n) = (p-1) (q-1)$
4. Seleccione un entero positivo  $e$  tal que el máximo común divisor entre  $e$  y  $\varphi(n)$  sea 1
5. Calcule  $d$  tal que  $e \cdot d = 1 \pmod{\varphi(n)}$

Para poder determinar si un número es primo, debe usarse un test de primalidad (test probabilístico). El cálculo del inverso modular se realiza mediante el algoritmo extendido de Euclides

La clave pública consiste en:

$n$ , el módulo.

$e$ , el exponente público

La clave privada consiste en:

$n$ , el módulo, el cual es público y aparece en la clave pública

$d$ , el exponente privado que debe permanecer oculto.

El cálculo de estas claves se realiza en secreto en la máquina en la que se va a guardar la clave privada, y una vez generada ésta conviene protegerla mediante un algoritmo criptográfico simétrico.

En cuanto a las longitudes de claves, el sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 ordenadores trabajando juntos para hacerlo). Cuando un usuario ha generado sus claves, transmite la clave pública a su interlocutor, y guarda la clave privada

### 9.3 Cifrado de mensajes

Supongamos que un usuario A quiere enviar a otro usuario B un mensaje M secreto, de forma sólo B pueda leerlo.

El texto cifrado será  $C=M^e \pmod n$  siendo M el mensaje original

Para que el sistema sea correcto, n ha de ser mayor que cualquiera de los posibles mensajes o bloques de mensajes. Si M fuese mayor, debería dividirse en bloques, de forma que cada bloque fuese menor que n Para el cálculo de las potencias modulares se utiliza el método de la exponenciación binaria: se basa en la posibilidad de expresar el exponente en su forma binaria, y a partir de ahí multiplicar y potenciar la base según el número obtenido. Así, logramos descomponer las grandes potencias en otras más pequeñas, más manejables.

#### Ejemplo:

Supongamos que hemos escogido  $p=31$  y  $q=17$

Los valores de n y  $\phi(n)$  son respectivamente

$$n= 31* 17 = 527, \text{ y}$$

$$\phi(n) = 30*16 = 480$$

Elegimos como valor de  $e=7$ , ya que cumple el criterio de ser relativamente primo con  $\phi(n)$

n y e son las claves públicas. La clave privada es d (inverso de 3 módulo  $\phi(n)$ ). Usando el algoritmo extendido de Euclides, se obtiene que la clave privada d es 343

Supongamos que deseamos cifrar el número 9. Dado que 9 es menor que n (527), no hace falta que lo dividamos en bloques.

$$C=M^e \pmod n = 9^7 \pmod 527 = 444$$

Es decir, el mensaje cifrado es **444**

### 9.4 Descifrado de mensajes

Para descifrar debemos seguir el siguiente proceso:  $M=C^d \pmod n$

En el ejemplo anterior,  $C=444$

$$M=C^d \pmod n = 444^{343} \pmod 527 = 9$$

Para entender el funcionamiento del algoritmo, es preciso conocer el teorema pequeño de Fermat que establece que si p es un número primo, entonces, para cada número natural a coprimo con p,

$$a^p \equiv a \pmod p$$

El pequeño teorema de Fermat se puede generalizar mediante el teorema de Euler: para cualquier módulo n y cualquier entero a coprimo con n, se tiene:

$$a^{\phi(n)} \equiv 1 \pmod n$$

Puede verse que, dado que en RSA  $M=C^d \pmod n$ , y  $C=m^e \pmod n$

$$c^d \equiv (m^e)^d \equiv m^{ed} \pmod n$$

¿Cómo funciona la seguridad en Internet?

Al ser  $ed \equiv 1 \pmod{\varphi(n)}$ , mediante el teorema de Euler obtenemos que:

$$m^{ed} \equiv m \pmod{pq},$$

y por tanto

$$c^d \equiv m \pmod{n}$$

## 10. Anexo B. Tipos de firewalls

### 10.1 Tipos de firewalls

En el capítulo 3 se ha indicado la necesidad de definir una política de diseño de firewalls. Dicha política establece los diferentes tipos de firewalls que puede ser implementados.

### 10.2 Firewall de filtrado de paquetes

El filtrado de paquetes consiste en impedir que ciertos paquetes de información (paquetes IP en general) puedan acceder a la red que se esté protegiendo o que puedan salir de la red en cuestión. Básicamente es un mecanismo que permite impedir que ciertos paquetes accedan o salgan de una determinada red. De esta forma los administradores de redes pueden controlar el tráfico y de esta manera reducir la posibilidad de ataques externos.

Por ejemplo, los routers pueden filtrar paquetes IP basados en ciertas reglas, como lo son:

- Dirección IP fuente.
- Dirección IP destino.
- Puerto TCP/UDP fuente.
- Puerto TCP/UDP destino.

Las técnicas de filtrado permiten bloquear conexiones desde o hacia ciertos host o redes y pueden bloquear conexiones a puertos específicos. Por ejemplo, se podrían filtrar paquetes que provienen de direcciones que son consideradas no confiables o se podría impedir incluso que los usuarios de una red interna tengan acceso a ciertas direcciones.

Por ultimo, es importante destacar que el filtrado de paquetes puede ser estático o dinámico.

- Filtrado estático: En este caso el firewall permite el acceso del tráfico autorizado, según lo especificado en la política de acceso a servicios, a través de 'puertas' que están siempre abiertas.
- Filtrado dinámico: En este tipo de filtrado, el firewall permite el acceso de paquetes según la información contenida en la cabecera de los mismos.

Este tipo de firewalls presenta varias ventajas: a) permite mayor protección; b) soporta la mayoría de los servicios, y c) se tiene un mayor control de lo que entra a una red que se considera confiable. Como inconvenientes, podemos citar a) reduce el riesgo de ataques pero no los impide, ya que una vez que se tiene acceso a

la red se pueden explotar las vulnerabilidades de los host internos, y b) no posee autenticación de usuarios.

### 10.3 Servidores proxy

Para solucionar los problemas que tienen los firewalls de filtrado de paquetes y superar sus desventajas, se han desarrollado aplicaciones de software que pueden filtrar conexiones relacionadas con ciertos servicios (por ejemplo: TELNET, FTP, etc.). Estas aplicaciones son conocidas como servidores proxy o gateways de aplicación.

El objetivo de los servidores proxy es actuar como una especie de 'intermediario' entre dos redes interconectadas, permitiendo que los hosts que pertenecen a una red de confianza se comuniquen de manera indirecta con hosts de otras redes o servidores externos.

Las ventajas que tiene el uso de servidores proxy son las siguientes:

- Ocultación de identidad del host interno: La información propia de los hosts de una red (en particular su nombre) no debe darse a conocer al exterior (a través del uso de un servidor DNS) para poder establecer comunicaciones externas. Es decir, desde la red externa sólo se debe conocer la identidad del servidor proxy para poder comunicarse indirectamente con los hosts internos.
- Mecanismos de autenticación y login robustos: El proxy puede implementar un mecanismo de autenticación y login para que los hosts externos tengan acceso a la red que está siendo protegida por el servidor proxy.
- Menor complejidad en las reglas de filtrado: Las reglas de filtrado de paquetes que utiliza un router se tornan menos complejas, debido a que el router no tiene que controlar si los paquetes están dirigidos a los host individuales, simplemente controla que los paquetes estén dirigidos al servidor proxy.

Como ejemplo de servidor proxy puede considerarse un proxy de e-mails, encargado de centralizar los mails que llegan a una red interna y redirigirlos a los usuarios de la red. Todos los mails que llegan o salen deben pasar por el proxy y de esta manera se puede tener mayor control sobre la información que entra a una organización, por ejemplo, no permitiendo la llegada de los mails 'basura' controlando así el spam. Una función alternativa que cumplen los servidores proxy es la de actuar como un buffer que almacena la información que viaja entre las redes, permitiendo así una velocidad de acceso mayor ya que los datos pueden ser buscados primero en el proxy y sino se encuentran allí, pedirlos a los servidores externos.

#### **10.4 Firewalls de inspección de paquetes**

Algunos de los firewalls usados en las conexiones de redes organizacionales a Internet, combinan las dos técnicas vistas anteriormente: filtrado de paquetes y servidores proxy. Esta alternativa de diseño puede permitir un alto grado de control de acceso, pero pone límites en cuanto a la flexibilidad y transparencia de la conectividad; además de hacer más difícil y compleja la configuración de los firewalls que implementan ambos mecanismos.

Una alternativa de diseño consiste en inspeccionar los paquetes, es decir, considerar el contenido de los paquetes en lugar de filtrarlos únicamente según sus direcciones o números de puerto. Este tipo de firewalls utiliza un módulo de inspección de paquetes para los diferentes protocolos utilizados en cada una de las capas de la arquitectura de red (modelo TCP/IP).

Por ejemplo, los servidores proxy sólo tienen acceso a la información relacionada con la capa de aplicación, los routers tienen acceso a información relacionada con las capas inferiores (transporte y red) mientras que los firewalls que realizan inspección de paquetes tienen la capacidad de integrar la información obtenida desde todas las capas en un solo punto de inspección.

Este tipo de filtrado inteligente puede combinarse con la capacidad de poder monitorizar sesiones de red. Esto es lo que se conoce como filtrado de sesión. Con esta estrategia, el módulo que se encarga del filtrado utiliza reglas 'inteligentes' que permiten no solo inspeccionar los paquetes individuales sino que también, basándose en la información de inicio y fin de sesión, permite inspeccionar una sesión de red.

Algunas de las ventajas que ofrece este tipo de firewall son las siguientes:

- Un módulo de inspección puede manipular paquetes de forma más rápida que un servidor proxy, lo que permite reducir costos.
- Los firewalls de inspección pueden proveer traducción de direcciones, escaneo del contenido de los paquetes para la búsqueda de virus, entre otros servicios.

La principal desventaja de este tipo de firewall es que el nivel de procesamiento requerido en comparación con el filtrado de paquetes común, es mayor.

## **10.5 Firewalls híbridos**

Este tipo de firewall combina las técnicas de control de tráfico de paquetes vistas anteriormente. Por ejemplo, un firewall que utiliza técnicas de filtrado puede ser mejorado agregándole la capacidad de inspeccionar paquetes. El problema que tiene esta estrategia de agregar capacidades o métodos de seguridad a los firewalls es que no necesariamente se incrementa la seguridad.

## 11. Anexo C. Seguridad a nivel de red. IPSEC (Internet Protocol Security)

### 11.1 Introducción

En los últimos años, Internet ha experimentado un crecimiento sorprendente. Muchas organizaciones, pequeñas compañías y personas individuales, se conectan cada día. Esto ha traído dos consecuencias críticas relacionadas con la implementación del Protocolo Internet – el IPv4 – la seguridad y validez de las direcciones. Uno de los problemas de IPv4, es que utiliza direcciones de 32 bits; pero esto se solucionará con una nueva versión del protocolo que permitirá direcciones de 128 bits (IPv6). El otro problema más urgente, es la seguridad de los datos; o actualmente la falta de seguridad. IPv4 no proporciona medidas que puedan asegurar que los datos que han sido recibidos en el destino, no han sido alterados durante la transmisión; o que ellos vienen de una fuente fiable.

IPSec es un compendio de protocolos diseñados para proporcionar seguridad a las conexiones IP a través de Internet. Ha sido desarrollado por el Internet Engineering Task Force (IETF) IP Security Working Group. El objetivo del grupo de trabajo IPSec ha sido la definición de protocolos para dotar de ciertas características de seguridad de las cuales IPv4 carece. Actualmente IPSec es opcional para IPv4 y obligatorio para los desarrollos sobre IPv6 .

Podemos dividir los requisitos de seguridad en dos partes distintas:

- Autenticación & Integridad. La autenticación garantiza que los datos recibidos son los mismos que fueron enviados, y que el emisor es realmente quien dice ser. La integridad significa que podemos asegurar que los datos transmitidos han llegado a su destino sin alteraciones no detectadas. En IPSEC se consigue mediante la cabecera de autenticación (*Authentication Header – AH*)
- Confidencialidad. La confidencialidad es la propiedad de comunicarse de forma que únicamente los receptores interesados conozcan la información que ha sido enviada, y los demás individuos no puedan determinarla. IPSEC proporciona servicios de confidencialidad a través del “*Encapsulating Security Payload*” (**ESP**). ESP también puede proporcionar autenticación del origen de los datos, integridad en la conexión, y servicios anti-réplica. La confidencialidad puede ser seleccionada independientemente de los demás servicios.

Los dos mecanismos mencionados (AH y ESP) pueden usarse juntos o separados.

A continuación se proporcionan una serie de definiciones aplicables a IPSEC:

- **SPI** (Security Parameters Index): índice de parámetro de seguridad que se utiliza junto con la dirección destino (*destination address*) para identificar una asociación de seguridad (*Security Association*) en particular.
- **Security Association (SA)**: el conjunto de información sobre seguridad referido a una conexión de red dada, o grupo de conexiones.
- **Traffic Analysis**: el análisis del flujo de tráfico en la red con el propósito de deducir información que es útil para el adversario.

La cabecera de autenticación IP (AH), se ha diseñado para proporcionar a los datagramas IP integridad y autenticación, *sin confidencialidad*. La falta de confidencialidad asegura que implementaciones de la cabecera de autenticación serán ampliamente aprovechables en Internet, incluso en lugares donde la exportación, importación o uso de la criptografía para proporcionar confidencialidad está regulado, esto es debido a que los

algoritmos de confidencialidad tienen problemas legales de exportación. La cabecera de autenticación soporta seguridad entre dos o más hosts implementando AH, entre dos o más gateways implementando AH, y entre un host o gateway implementando AH y una serie de hosts o gateways.

El encapsulado de seguridad de la carga útil IP (ESP), se ha diseñado para proporcionar siempre confidencialidad, y dependiendo del algoritmo y del modo, integridad y autenticación. El ESP soporta seguridad entre dos o más hosts implementando ESP, entre dos o más gateways implementando ESP, y entre un host o gateway implementando ESP y una serie de hosts o gateways.

El concepto de “**Security Association**” es fundamental tanto para la IP AH como para el IP ESP. Una asociación de seguridad está identificada unívocamente por una dirección Internet y un índice de parámetro de seguridad (SPI). La combinación de un SPI y una dirección destino únicamente identifican a una única Asociación de Seguridad. Una implementación de la AH o de ESP debe soportar este concepto de asociación de seguridad. Una asociación de seguridad normalmente incluye los parámetros que se comentan a continuación, aunque también debe incluir parámetros adicionales:

**Requeridos:**

- Algoritmo de autenticación y modo de utilización del algoritmo con la AH
- Clave(s) utilizadas con el algoritmo de autenticación que está en uso con la AH.
- Algoritmo de cifrado, modo del algoritmo y transformación que se está utilizando la IP ESP.
- Clave(s) usada con el algoritmo de cifrado que está en uso con la ESP.
- Presencia o ausencia, y tamaño de la sincronización de criptografía o inicialización del campo vector para el algoritmo de cifrado.

**Recomendados:**

- Algoritmo de autenticación y modo usado con la transformación ESP.
- Clave(s) de autenticación usada con el algoritmo de autenticación que es parte de la transformación ESP.
- Tiempo de vida de la clave o tiempo en el que se debería cambiar la clave.
- Tiempo de vida de la SA.
- Dirección(es) origen de la SA.
- Nivel de sensibilidad (seguridad) de los datos protegidos.

Una implementación AH siempre podrá usar la SPI en combinación con la dirección destino para determinar la asociación de seguridad y otros datos de seguridad relacionados, para todos los paquetes de entrada válidos.

Una asociación de seguridad es normalmente unidireccional. En una sesión de comunicación entre dos hosts, normalmente se utilizarán dos SPIs. La combinación de un SPI concreto con una dirección destino concreta, únicamente identifica a la AS.

## 11.2 Modos IPSec

IPSec permite la posibilidad de creación de dos tipos de comunicación, en función de lo que queremos asegurar. Esto permitirá ocultar, o no, cierta información (direcciones IP de los nodos, protocolo utilizado, etc.) en función de nuestros intereses y también en función de los medios de que dispongamos:

**Modo Túnel:**

En este modo, los gateways proporcionan túneles para el uso de los clientes detrás de los gateways. Las máquinas de los clientes no necesitan realizar ningún proceso IPSec, todo lo que han de hacer es enrutar los paquetes hacia los gateways. En consecuencia, son los gateways de seguridad las entidades encargadas de soportar IPSec. Obviamente, es preciso realizar una traducción de direcciones en las cabeceras origen y destino del paquete original. Existe una cabecera IP externa que especifica el destino del procesamiento IPSec, además de una cabecera interna que especifica el (aparente) último destino del paquete. La cabecera del protocolo de seguridad aparece después de la cabecera IP externa y antes de la cabecera IP interna.



Figura 5.5.

### Modo Transporte

Las máquinas host, al contrario que las gateway, con implantaciones IPSec, deben también soportar el modo transporte. En este modo, el host realiza su propio proceso IPSec, y enruta los paquetes vía IPSec. En este modo, la cabecera del protocolo de seguridad aparece inmediatamente después de la cabecera IP y de cualquier opción, y antes de cualquier protocolo de nivel superior (p.e. TCP o UDP).



Figura 5.6.

## 11.3 Cabecera de autenticación (AH: Authentication Header)

Cuando se utiliza únicamente la cabecera de autenticación no se intenta proteger el contenido, sólo asegurar su integridad. AH permite confiar en que un paquete proceda de una máquina en particular y que su contenido no ha sido alterado en el camino. Existen algunos campos de la cabecera IP que AH no puede proteger ya que éstos varían durante el camino entre el emisor y el receptor.

El servicio de autenticación puede ser proporcionado separadamente de la confidencialidad añadiendo una cabecera de autenticación AH después de la cabecera IP, pero antes de otras cabeceras en el paquete.. Los detalles se encuentran desarrollados en el RFC 2402.

Las cabeceras en un paquete están conectadas por una lista de uniones donde cada cabecera contiene un campo de "protocolo siguiente" diciendo al sistema que cabecera sigue. Las cabeceras IP tienen generalmente en este campo el valor correspondiente a TCP o UDP. Cuando se usa autenticación IPSec, la cabecera IP tiene el valor correspondiente a AH en este campo y es la cabecera de autenticación quien tiene definido en su cabecera los valores correspondientes al siguiente protocolo, ya sea TCP, UDP o IP encapsulado.

La autenticación IPSec puede ser añadida en el *modo transporte*, como una modificación del transporte IP. Esto es lo mostrado en el diagrama: La autenticación puede ser usada en *modo túnel*, encapsulando el paquete IP bajo AH y una cabecera adicional IP.

**Antes de aplicar AH**



*Ping de 1 byte (transporte)*

```

----- Frame 1 -----
ADDR  HEX                                     ASCII
0000:  00 20 af 20 34 c9 00 20 af c4 35 29 08 00 45 00 | .....I...D.....
0010:  00 1d 00 af 00 00 40 01 5c 30 0a 00 00 01 14 00 | .....*.....
0020:  00 01 08 00 ed f5 0a 0a 00 00 00 00 00 00 00 00 | .....5.....
0030:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
    
```

**Después de aplicar AH (modo transporte)**



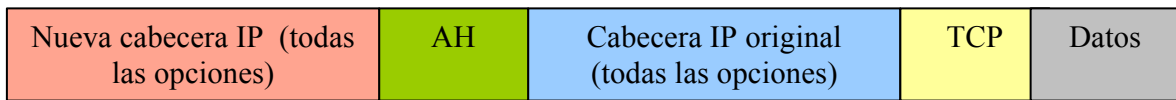
← Autenticado excepto los campos de valor variable →

```

----- Frame 1 -----
ADDR  HEX                                     ASCII
0000:  00 20 af 20 34 c9 00 20 af c4 35 29 08 00 45 00 | . . 4 . . .5) ..E.
0010:  00 35 00 ad 00 00 3f 33 5c e8 0a 00 00 01 14 00 | .5....?3\.....
0020:  00 01 01 04 00 00 00 00 02 00 00 00 00 02 91 21 | .....!\
0030:  a6 99 1a 1b 25 50 d5 c4 c3 17 08 00 be f6 39 09 | ....%P.....9.
0040:  00 00 00                                     |
    
```

**Después de aplicar AH (modo túnel)**

← Paquete IP original →



← Autenticado excepto los campos de valor variable →

*Ping de 1 byte*

```

----- Frame 1 -----
ADDR  HEX                                     ASCII
0000:  00 20 af 20 34 c9 00 20 af c4 35 29 08 00 45 00 | .....I...D.....
0010:  00 49 00 5e 00 00 40 33 5c 23 0a 00 00 01 14 00 | .;. . .*.....
0020:  00 01 04 04 00 00 00 00 02 00 00 00 00 02 db bb | .....
0030:  9f 73 25 1f 84 63 28 8b 24 db 45 00 00 1d 75 01 | .....d.....
0040:  00 00 1e 01 10 dd 0b 00 00 02 0c 00 00 01 08 00 | .....
0050:  90 ff 04 00 02 00 61                         | ...../
    
```

**Formato del Authentication Header**



- Authentication Data: Este es un campo de longitud variable que contiene el Integrity Check Value (ICV) para este paquete. Este campo tendrá una longitud de un integral múltiplo de 32 bits.

Los datos de autenticación incluidos en la Cabecera de Autenticación IP, normalmente se calculan utilizando un algoritmo de resumen del mensaje (como MD5). Sólo aquellos algoritmos que se consideran funciones unidireccionales criptográficamente fuertes, deben ser utilizados con una cabecera de autenticación IP. Debido a que los checksums convencionales no cumplen esta condición, no deben ser utilizados con la AH.

Cuando procesamos un paquete IP de salida, para su autenticación, el primer paso consiste en que el sistema de salida localice la asociación de seguridad. La SA elegida indicará el algoritmo y su modo, la clave, y otras propiedades de seguridad que se aplicarán al paquete de salida.

Aquellos campos que cambian en el trayecto de emisor a receptor, y cuyos valores no son conocidos con certeza por el emisor, están incluidos en el cálculo de los datos de autenticación, pero son procesados de forma especial. El valor que toman estos campos es el valor cero.

El emisor debe calcular la autenticación sobre el paquete, tal como el paquete aparecerá en el receptor. El emisor coloca la salida del algoritmo resumen del mensaje calculado, en el campo de datos de autenticación con la AH.

Los campos "TIME TO LIVE" (tiempo de vida) y "HEADER CHECKSUM" (suma de comprobación) son los únicos campos de la cabecera base de IPv4 que se utilizan para el cálculo de los datos de autenticación. Para el cálculo de los datos de autenticación estos dos campos deben ser cero. Todos los demás campos de la cabecera IPv4 son procesados con su contenido actual.

La "IP Security Option" (IPSO) debe ser incluida en el cálculo de los datos de autenticación siempre que esta opción está presente en un datagrama IP. Si un sistema receptor no reconoce una opción IPv4 que está presente en el paquete, esa opción esta incluida en el cálculo de los datos de autenticación. Eso significa que cualquier paquete IPv4 que contenga una opción IPv4 que cambia durante el trayecto de una forma imprevisible por el emisor, y cuya opción IPv4 no es reconocida por el receptor, fallará la comprobación de autenticación, y consecuentemente será suspendida por el receptor.

El campo "HOP LIMIT" (limite de saltos) es el único campo de la cabecera base de IPv6 que se utiliza para el cálculo de los datos de autenticación. El valor de este campo es cero para el cálculo de los datos de autenticación. Todos los demás campos de la cabecera IPv6 deben estar incluidos en el cálculo de los datos de autenticación usando los procedimientos normales para realizar este cálculo.

Una vez recibido el paquete con la cabecera de autenticación IP, el receptor primero utiliza la dirección destino y el valor ISP para localizar la Asociación de Seguridad correcta. El receptor entonces verifica que el campo Datos de Autenticación y que el paquete de datos recibidos son consecuentes. De nuevo el campo de datos de autenticación es considerado cero con el único propósito de realizar el cálculo de autenticación. Si el procesado del algoritmo de autenticación indica que el datagrama es válido, entonces este es aceptado. En caso contrario, el receptor debe descartar el datagrama IP recibido.

#### **11.4 Confidencialidad (ESP: Encapsulating Security Payload)**

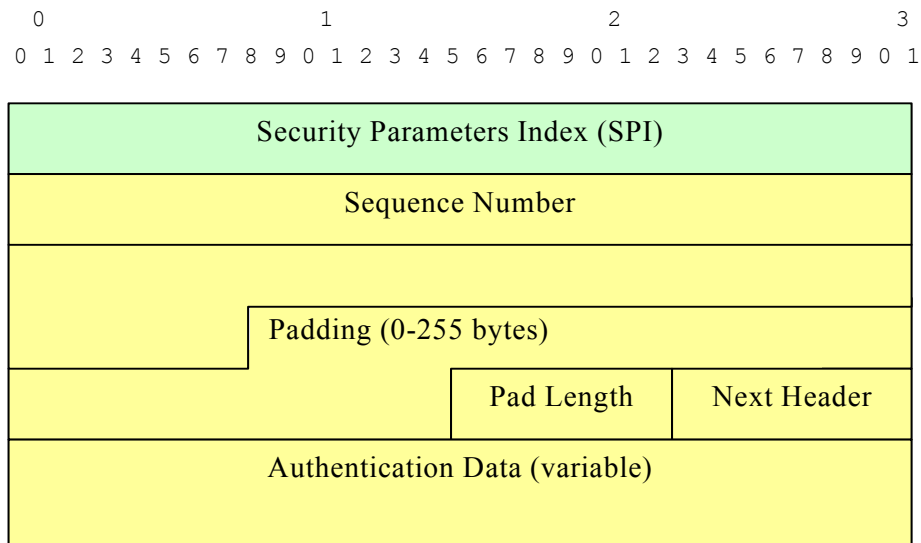
El protocolo IPsec que proporciona confidencialidad es el ESP, Encapsulated Security Payload. El algoritmo utilizado suele ser un cifrador de bloques (habitualmente Triple DES). En

las configuraciones más usuales, las claves son negociadas automáticamente, y periódicamente renegociadas, utilizando el protocolo IKE (Internet Key Exchange).

El protocolo ESP se encuentra definido en el RFC 2306. Éste proporciona servicios de confidencialidad, autenticación o ambos. Puede ser usado con o sin autenticación AH. Es importante que alguna forma de autenticación debe utilizarse cuando los datos son cifrados. Sin autenticación, la encriptación es vulnerable ante ataques activos. Por ello, ESP siempre debe incluir su propia autenticación o autenticación AH.

Formato del paquete Encapsulating Security Payload

La cabecera del Protocolo IPv4 previo a la cabecera ESP debe contener el valor 50.



```

----- Frame 1 -----
ADDR  HEX                                     ASCII
0000: 00 20 af 20 34 c9 00 20 af c4 35 29 08 00 45 00 | .....I...D.....
0010: 00 40 00 aa 00 00 3f 32 5c e1 0a 00 00 01 14 00 | . .....*.....
0020: 00 01 00 00 02 00 00 00 00 02 62 3e 1b 9e 86 e0 | .....f\
0030: 20 61 79 cd ef 31 74 bf ae 06 3d 18 bd da 66 25 | ./`.....
0040: 45 7b 19 19 7e 42 e1 08 f7 bf 28 fc c2 9f      | .#...=...7...B.
    
```

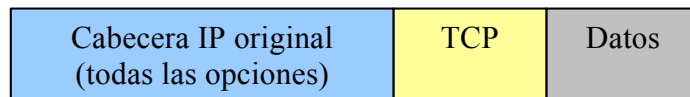
- Security Parameters Index (SPI): El SPI es un valor arbitrario de 32 bits que, en combinación con la dirección IP de destino y el protocolo de seguridad (ESP), identifica unívocamente la Asociación de Seguridad (SA) para este datagrama. El rango de valores del SPI es de 1 a 255 y éstos se encuentran reservados por la IANA (Internet Assigned Numbers Authority) si el valor del SPI no se encuentra ya especificado en algún RFC. Normalmente el valor es determinado por el sistema destino en el momento de establecerse la SA.
- Sequence Number: Este campo de 32 bits es simplemente un contador incremental. Este campo siempre se encuentra presente aunque el receptor no utilice sus valores para el servicio anti-replay en alguna SA. Los contadores de origen y destino son puestos a cero en el momento de establecerse la SA. No se permite establecer ciclos en los valores del contador, los contadores deben ponerse a cero, estableciendo una nueva SA antes de que se llegue al paquete 232 en la transmisión.

- **Payload Data:** Es un campo de longitud variable que contiene los datos descritos por el campo Next Header. Si el algoritmo usado para la encriptación del Payload requiere datos de sincronización criptográfica, pe. Initialization Vector (IV), estos datos han de estar incluidos en este campo. Cualquier algoritmo de cifrado que necesite explícitamente esta sincronización por paquete, deberá incluir la longitud, cualquier estructura para estos datos y la localización de estos datos como parte de un RFC especificando como es usado este algoritmo por ESP. Si los datos de sincronización se encuentran de forma implícita, es necesario que el algoritmo para derivar los datos sea parte del RFC.
- **Padding:** Existen diversos factores que requieren la existencia de un campo de relleno, como el uso de algoritmo de cifrado en bloque (lo cual exige que la longitud del campo de datos a cifrar sea un múltiplo de un determinado número de bytes) y la necesidad que los campos de Pad Length y Next Header se encuentren alineados a la derecha con una palabra de 4 bytes.
- **Pad Length:** Este campo indica el número de bytes de relleno utilizados en el campo anterior. El rango de valores válido es de 0 a 255, donde el valor 0 indica que no se está utilizando relleno. Este campo es obligatorio.
- **Next Header:** Este campo tiene una longitud de 8 bits e identifica el tipo de datos contenidos en el campo Payload Data, por ejemplo el tipo de protocolo de nivel superior incluido en el paquete. Estos valores son tomados de los IP Protocol Numbers definidos por la IANA.
- **Authentication Data:** Este es un campo de longitud variable que contiene el ICV (Integrity Check Value) calculado a partir del paquete ESP excepto el campo Authentication Data. La longitud de este campo viene determinada por la función de autenticación seleccionada. Este campo es opcional y por tanto sólo está incluido si el servicio de autenticación se ha seleccionado en el establecimiento de la SA. El algoritmo de autenticación seleccionado debe especificar la longitud del ICV así como las reglas de comparación y los pasos a seguir para la validación.

### Localización de la cabecera ESP

Al igual que el Authentication Header, ESP también puede ser empleado de dos formas, modo transporte y modo túnel. En modo transporte, ESP se encuentra insertado después de la cabecera IP y antes que el protocolo de nivel superior (TCP, UDP, ICMP, etc.)

#### Antes de aplicar ESP

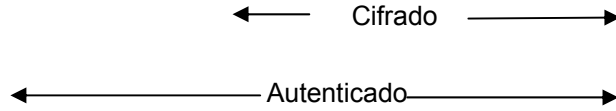


*Ping de 1 byte (transporte)*

```

- - - - - Frame 1 - - - - -
ADDR  HEX                                     ASCII
0000: 00 20 af 20 34 c9 00 20 af c4 35 29 08 00 45 00 | .....I...D.....
0010: 00 1d 00 af 00 00 40 01 5c 30 0a 00 00 01 14 00 | .....*.
0020: 00 01 08 00 ed f5 0a 0a 00 00 00 00 00 00 00 00 | .....5.....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
    
```

#### Después de aplicar ESP (modo transporte)



*Ping de 1 byte (transporte)*

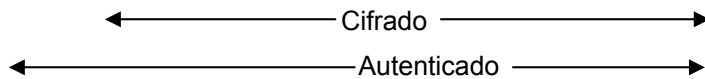
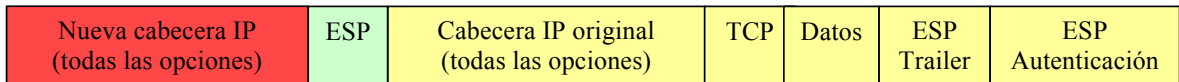
```

----- Frame 1 -----
ADDR  HEX                                     ASCII
0000: 00 20 af 20 34 c9 00 20 af c4 35 29 08 00 45 00 | .....I...D.....
0010: 00 40 00 aa 00 00 3f 32 5c e1 0a 00 00 01 14 00 | . . . . . * . . . . .
0020: 00 01 00 00 02 00 00 00 00 02 62 3e 1b 9e 86 e0 | . . . . . f \
0030: 20 61 79 cd ef 31 74 bf ae 06 3d 18 bd da 66 25 | . / \ . . . . .
0040: 45 7b 19 19 7e 42 e1 08 f7 bf 28 fc c2 9f      | . # . . = . . 7 . . B .
    
```

El modo túnel puede ser empleado tanto en hosts como en gateways de seguridad. En este modo todo el paquete IP original con sus opciones, incluida la dirección de destino final, queda protegido.

La forma del paquete en modo túnel sería la siguiente:

**Después de aplicar ESP (modo túnel)**



*Ping de 1 byte (túnel)*

```

----- Frame 1 -----
ADDR  HEX                                     ASCII
0000: 00 20 af 20 34 c9 00 20 af c4 35 29 08 00 45 00 | .....I...D.....
0010: 00 50 00 a8 00 00 40 32 5b d3 0a 00 00 01 14 00 | . & . y . . $ L . . . . .
0020: 00 01 00 00 02 00 00 00 00 01 bf 73 38 35 c5 f0 | . . . . . E 0
0030: 3f 07 ed 5a 50 b0 2a 00 3b c7 a3 63 38 e2 9b 27 | . . . ! & . . . G t . . S . .
0040: e0 0c 4e 99 c7 58 fe f1 77 88 3a b5 53 26 44 2e | \ . + r G . . 1 . h . . . . .
0050: 24 c0 90 4c 2f 98 b6 d0 6e 41 90 74 a1 d4      | . { . < . q . } > . . . ~ M
    
```

**11.5 Autenticación más Confidencialidad**

Los dos mecanismos de seguridad IP estudiados, se pueden combinar para transmitir un paquete IP que tenga autenticación y confidencialidad. Se pueden utilizar dos técnicas diferenciadas por el orden en el que se aplican los dos servicios.

La figura 1.16 muestra el caso del cifrado aplicado antes de la autenticación (modo transporte o túnel).

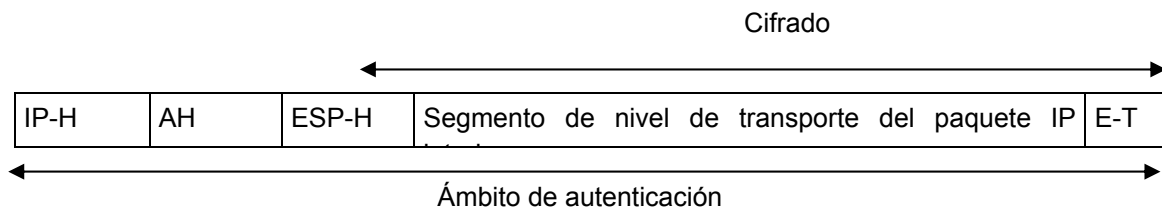


Figura 1.16. Modelo de cifrado antes de la autenticación.

Los campos de la trama tienen los siguientes significados.

- IP-H: Cabecera de IP más cabeceras de ampliación.
- ESP-H: Cabecera de la carga útil de seguridad de encapsulamiento.
- AH: Cabecera de autenticación.
- E-T: Campo de cierre de la carga útil de seguridad de encapsulamiento.

En este caso, el paquete IP entero transmitido se autentifica, incluyendo ambas partes, la cifrada y la no cifrada. En esta técnica el usuario primero aplica ESP a los datos que se van a proteger, después incorpora al principio la cabecera de autenticación y la(s) cabecera(s) IP en texto nativo. Existen dos subcasos:

- ESP en modo transporte: la autenticación se aplica al paquete IP entero entregado al destino, pero solamente el segmento de la capa de transporte se protege por el mecanismo de confidencialidad.
- ESP en modo túnel: la autenticación se aplica al paquete IP entero entregado a la dirección IP destino externa (por ejemplo, un cortafuegos), y la autenticación se lleva a cabo en el destino. El paquete IP interno se protege por el mecanismo de confidencialidad, para su entrega al destino IP interno.

En caso que se aplique la autenticación antes del cifrado, el resultado sería como se muestra en la figura 5.7.

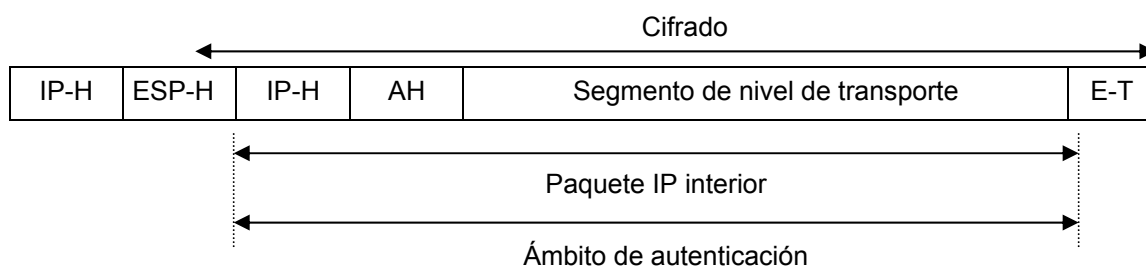


Figura 5.7. Modelo de autenticación antes del cifrado.

Esta técnica sólo es adecuada para ESP en modo túnel. En este caso la cabecera de autenticación se sitúa dentro del paquete IP interno. Este paquete interno es autenticado y protegido por el mecanismo de confidencialidad.

Las funciones de autenticación y cifrado se pueden aplicar en cualquier orden para ESP en modo túnel. El uso de la autenticación antes del cifrado puede ser preferible por varias razones. Primero, ya que AH se protege por ESP, es imposible que cualquiera intercepte el mensaje y altere AH sin ser detectado. Segundo, puede ser deseable almacenar la información de autenticación con el mensaje y el destino para una referencia posterior. Es más conveniente

¿Cómo funciona la seguridad en Internet?

hacer esto si la información de autenticación se aplica a un mensaje no cifrado; de otra forma el mensaje tendría que ser cifrado de nuevo para verificar la información de autenticación.