CAPÍTULO 1

INTRODUCCIÓN

1.1 MOTIVACIÓN

Debido a la amplia aceptación de los estándares y protocolos del Internet en todo el mundo, las limitaciones de comunicación entre las empresas han ido desapareciendo. La mayor parte de las empresas en el mundo reconocen los beneficios de abarcar mercados cada vez más grandes con un mínimo de infraestructura a través de medios electrónicos. Estos nuevos enlaces de comunicación son capaces de fortalecer las relaciones comerciales, mejorar la eficiencia de procesos y productos, y proporcionar un acceso rápido y confiable a gran cantidad de información. Recientemente, el número de puntos de venta electrónicos se ha incrementado, lo que ha permitido el intercambio de información entre organizaciones. A medida que este comercio electrónico negocio-negocio se vuelva más común, las relaciones entre las empresas y sus proveedores, clientes u otros agentes tendrán un fuerte impacto en el éxito a

largo plazo de este tipo de comercio. De hecho, Glover Ferguson, de la empresa Andersen Consulting dedicada al comercio electrónico, indica que la implementación de una estrategia efectiva de comercio electrónico es uno de los factores críticos para la supervivencia de la empresa durante los dos años posteriores a su inicio de operaciones [1].

El uso del Internet ha provocado un aumento de la necesidad del envío de productos y servicios más rápidos y eficientes, así como a proporcionar información instantánea a los empleados, los consumidores, los proveedores y los intermediarios. Con el creciente uso del comercio electrónico, las organizaciones se deben adaptar a nuevos requerimientos de negocios en forma continua y flexible. Resulta obvio que para explotar al máximo los beneficios de esta nueva forma de hacer negocios, es necesario que exista una integración transparente entre los sistemas y aplicaciones de la tecnología de información (TI) con los distintos participantes, lo que significa que una organización debe cambiar la forma fundamental de hacer negocios.

La mayoría de los usuarios piensa que el Internet no es un medio seguro debido a que se trata de una red pública. Es un hecho que la conexión de una red privada al Internet expone los recursos y la información de una empresa al riesgo que representan los accesos no autorizados. La transmisión de un documento entre dos entidades a través del Internet requiere que la información circule a través de diferentes redes de comunicación, cada una de las cuales puede ser administrada por entidades distintas.

La seguridad de los sistemas de comunicación utilizados en el comercio electrónico es un problema de negocio, y no solo un problema asociado a la tecnología. Las organizaciones no solo requieren implementar políticas de seguridad para proteger sus recursos, sino para permitirles tomar ventajas ante nuevas oportunidades de mercado. Por lo tanto, las organizaciones requieren desarrollar los mismos niveles de seguridad en un ambiente electrónico, similar a los alcanzados en las transacciones convencionales [2,3].

Con el objetivo de alcanzar los niveles de seguridad requeridos, es necesario diseñar una solución integral, donde se consideren los aspectos de seguridad a partir del envío y recepción de información con otros sistemas de comunicación [4]. Estos aspectos de seguridad abarcan el control de acceso y la seguridad de la información y transacciones. Los mecanismos del control de acceso deben asegurar que solo los usuarios autorizados y aplicaciones tengan acceso a las fuentes de información dentro del sistema (archivos, bases de datos, etc.); estos mecanismos incluyen la protección por passwords, tarjetas encriptadas y firewalls entre otros. Por el contrario, los esquemas de seguridad de la información y transacciones, como son los sistemas de encriptación con claves públicas y privadas, tienen por objetivo asegurar la privacidad, integridad y confidencialidad de las transacciones y mensajes comerciales.

La integración de estos mecanismos es la base para los diversos sistemas de pago electrónicos que existen actualmente. En muchos aspectos, los sistemas de comercio electrónico están sustentados en sistemas de pago electrónico. En

general, un pago electrónico es un intercambio financiero que se realiza en línea entre compradores y vendedores. El contenido del pago electrónico es un tipo de instrumento financiero digital (tarjeta de crédito, cheques electrónicos o dinero digital) que es respaldado por un banco o institución financiera.

La incorporación de capacidades de pago electrónico conlleva una considerable complejidad para los sistemas de TI. Primero, los sistemas de pago seguro deben ser capaces de proteger las aplicaciones del sistema de TI. Segundo, el sistema debe proporcionar un alto grado de integridad para cualquier tipo de transacción; esto incluye que las comunicaciones entre el consumidor, el proveedor y la institución financiera estén libres de intercepciones y alteraciones. Tercero, el sistema debe admitir diversas opciones de pago de acuerdo a las preferencias de los consumidores (tarjeta de crédito, tarjeta de débito, transferencias, etc.).

En el caso de los sistemas de pago por Internet, existen diversos mecanismos tanto convencionales como especializados. Actualmente, los métodos de pago convencionales como efectivo y cheques no son adecuados para sistemas de pago interactivo en tiempo real. Actualmente, la mayoría de los sistemas de pago por Internet utilizan dinero latente, como tarjetas de crédito, órdenes de compra con promesa de pago y transferencias de efectivo. También existen sistemas emergentes, algunos de los cuales basan sus operaciones en transacciones en dinero electrónico y micro pagos, que no tienen gran aceptación [1].

Esta diversidad de los sistemas de pago seguro por Internet, y la falta de un estándar único para la implementación de mecanismos de seguridad, ha ocasionado que la mayoría de los usuarios no tengan la suficiente confianza para realizar transacciones en forma electrónica. De ello se desprende la necesidad de explorar los diversos aspectos de seguridad en los sistemas de pago por Internet.

1.2 ANTECEDENTES

Son muchas las empresas que durante estos años han conocido las ventajas del Internet a través de páginas Web, correo electrónico, intranets corporativas, extranets y otras nuevas aplicaciones que hacen del Internet una ventaja competitiva; el número de usuarios no ha dejado de crecer en forma exponencial, dejando atrás el concepto de que Internet sería de uso exclusivo de personal de informática, investigadores y universidades. Actualmente existe un fuerte proceso de domesticación del Internet que sin duda se verá agravada con la llegada de los nuevos dispositivos, como los NCs y Web-TV, con precios inferiores a las computadoras y que operan con un simple mando a distancia.

A partir de la gran explosión del Web (a principios de los 90), el Comercio Electrónico ha sido motivo de interés y desarrollo para personal de mercadotecnia. Las páginas de Internet han aumentado muy rápido y actualmente permiten hacer pedidos por tarjetas de crédito en línea; los bancos y muchos comerciantes rehuían el comercio en Internet hasta que existiera una

infraestructura de transacciones por tarjeta de crédito segura y administrada por las principales compañías financieras.

Hoy día, son cada vez más los sistemas de pago donde se ha sustituido el dinero físico por cheques, cuentas o tarjetas de crédito, donde la garantía reside en la validación de los bancos y en las ventajas que brindan las redes interbancarias. También en el campo del Comercio Electrónico, se pueden encontrar estos medios de pago, aunque han surgido otros nuevos como los intermediarios electrónicos para sistemas basados en tarjetas de crédito o los que emplean moneda digital.

En cualquiera de los casos, se pueden clasificar en sistemas de pago anticipado (pay before), inmediato (pay now) o posterior (pay after). El escenario en el que se desarrolla el comercio electrónico contiene, al menos, un comprador y un vendedor. Además es difícil que pueda llevarse a cabo alguna transacción económica sin la intervención de un banco que se haga cargo del control efectivo del dinero. Es más, habitualmente aparecen dos bancos, el del comprador y el del vendedor, que liquidan entre ellos a través de sus redes y servicios interbancarios En algunas circunstancias hay que añadir un elemento más que es el certificador, una autoridad respetada por todas las partes, cuya intervención sirve para resolver conflictos [5].

En un escenario clásico existen, adicionalmente, diversos intermediarios que complican este proceso. Específicamente, se pueden mencionar las compañías

de crédito (con un papel análogo al del mundo real) y de administradores de "centros comerciales electrónicos" con diferentes grados de funciones.

Las posibilidades de establecer un solo estándar para realizar transacciones con tarjeta de crédito en Internet eran pocas cuando Mastercard y Visa Internacional se dividieron en una guerra comercial. La presión del sector bancario sobre Mastercard y Visa fue recompensada cuando anunciaron que trabajarían conjuntamente para forjar un nuevo estándar. El fruto de este acuerdo es SET (Secure Electronic Transactions) que representó un importante catalizador para propiciar el desarrollo en gran escala del comercio en Internet [6].

El acuerdo reunió a los principales contendientes de las transacciones en línea seguras: GTE, IBM, Microsoft, Netscape, SAIC, Terisa Systems, y VeriSign. Mientras GTE e IBM se interesaron por asegurar que sus controladores de hardware y redes bancarias pudieran manejar el protocolo, Microsoft y Netscape compitieron para proporcionar un browser (navegador) seguro y el software para la transacción del servidor. SAIC contribuyó con las técnicas de encriptación basadas en RSA que tanto S-HTTP como STT utilizaron en sus primeros esfuerzos, y Terisa Systems proporcionó las herramientas que los desarrolladores de software necesitarían para desarrollar las aplicaciones para el Comercio Electrónico. VeriSign (y GTE) proporcionaron el mecanismo de autenticación de certificado que usarían los vendedores, clientes y compañías de crédito y que permitirán el desarrollo del comercio en el seno de Internet y

otras redes públicas, de modo seguro para los participantes: usuario final, comerciante, entidades financieras, administradoras de tarjetas y propietarios de marcas de tarjetas.

SET describe tanto las relaciones y procesos entre las partes involucradas, como las estructuras informáticas que deberán ser desarrolladas, siempre dentro de un marco de interoperabilidad que garantizará procesos transparentes en las plataformas de hardware y sistemas operativos en los que se implemente.

Algunos de los protocolos de pago que se utilizan actualmente son el MIME, el PEM, el MOSS, el SSL, el S-HTTP y el iKP [7].

MIME es un protocolo de intercambio de objetos a través de Internet. Cada objeto se encapsula en una especie de concha que especifica tanto su semántica como el medio de codificación utilizado. La caracterización semántica permite asociar los datos con su mecanismo de transporte (codificación) y con su significado, de forma que el remitente y el destinatario utilicen coordinadamente los datos intercambiados. MIME se desarrolló inicialmente para intercambios de correo electrónico, habiéndose extendido a muchos otros protocolos.

PEM es un sistema similar a MIME y desarrollado en paralelo con éste para crear objetos de correo garantizados. Con el desarrollo de MIME, PEM es, de

alguna forma, repetitivo, por lo que se verá probablemente desplazado por MOSS, que no es más que una extensión de MIME que aporta exclusivamente lo que le falta a éste para obtener las garantías deseadas: claves, firmas, certificados, etc.

Secure Sockets Layer es una tecnología diseñada por Netscape Communications, que proporciona un nivel seguro de transporte entre el servicio clásico de transporte en Internet (TCP) y las aplicaciones que se comunican a través de él.

Las comunicaciones tienen lugar en dos fases. En una primera fase se negocia entre el cliente y el servidor una clave simétrica sólo válida para esta sesión. En la segunda fase, se transfieren datos cifrados con dicha clave. Este sistema es transparente para las aplicaciones finales, que simplemente saben que el canal se encarga de proporcionarles confidencialidad entre extremos.

La fase inicial se realiza muy cuidadosamente para evitar tanto la intromisión de terceras partes como para evitar suplantaciones de personalidad de parte del centro servidor. El cliente conoce de antemano las claves públicas de ciertos notarios electrónicos. Con esta información se pone en contacto con el servidor, el cual le envía su clave pública rubricada por el notario. La identificación se completa enviando al servidor un mensaje aleatorio que éste debe firmar. De esta forma el cliente sabe que al otro lado está quien dice estar.

Verificada la identidad del servidor, el cliente genera una clave de sesión y la envía cifrada con la clave pública del servidor. Conociendo ambos la clave de sesión, se intercambian datos con seguridad. En ciertas circunstancias puede ser necesario ejecutar una fase adicional para descubrir y legitimar la identidad del cliente.

SSL se utiliza fundamentalmente en los productos de la propia Netscape, concretamente con el Netscape Commerce Server y en el Netscape Navigator. Aunque la especificación permite diferentes algoritmos, el browser de Netscape sólo se exporta de EE.UU. usando algoritmos RC4 de cifrado simétrico restringidos a 40 bits. Esto da un nivel muy discutible de seguridad frente a ataques criptográficos.

Secure HTTP (S-HTTP) es un protocolo propuesto por Enterprise Integration Technologies (EIT) y patrocinado por el consorcio CommerceNet. Constituye una extensión del protocolo HTTP, incorporando cabeceras MIME para aportar confidencialidad, autenticación, integridad e irrenunciabilidad de las transacciones.

S-HTTP utiliza un sistema inspirado en PEM, añadiendo las cabeceras suficientes a cada transacción para lograr cada uno de los objetivos propuestos. Las transacciones HTTP constan simplemente de una petición de parte del cliente que induce una respuesta del servidor. S-HTTP especifica que el cliente envíe directamente toda la información pertinente: claves, certificados, códigos

de integridad, etc. (incluyendo la posibilidad de referenciar secretos compartidos obtenibles exteriormente como intercambios previos o bases de datos comunes). El servidor responde siguiendo la misma filosofía PEM.

A diferencia de SSL, S-HTTP sólo afecta a las transacciones HTTP, sin extender su cobertura a otros protocolos habituales en Internet. Por lo demás, S-HTTP y SSL pueden convivir, utilizándose uno u otro en diferentes instantes de una transacción comercial, o incluso utilizándose simultáneamente.

Los protocolos Internet Keyed Payment Protocols (iKP) han sido desarrollados en los Laboratorios de IBM en Zürich y tratan de proporcionar formas seguras de pago multiparte. Aunque tienen voluntad de no ligarse a instrumentos específicos de pago, están implementados para usarse sobre tarjetas de crédito, confiando en las redes financieras preexistentes para realizar la transferencia de dinero.

Están basados en criptografía de clave pública RSA para asegurar la privacidad de los números de tarjeta de crédito y de los PIN, proporcionando características de no- repudiación. iKP tiene tres opciones: dependiendo de los requerimientos, iKP implica una clave pública (pagador, 1KP), dos claves (pagador y vendedor, 2KP) y tres (pagador, vendedor y consumidor, 3KP).

La criptografía nos proporciona funciones matemáticas para dotar a los datos de ciertas propiedades interesantes. Su utilización sólo involucra a las partes

que intercambian información, si bien en ciertas situaciones se puede requerir la presencia de una tercera parte confiable que avale la transacción.

Además de las funciones matemáticas, que encriptan la información, ésta hay que transportarla. Para ello MIME proporciona un formato normalizado que se usa sobre objetos individuales (MOSS), sobre sesiones cliente-servidor (SSL) o sobre transferencias WWW (S-HTTP). No son técnicas incompatibles entre sí, sino más bien diferentes opciones de integración en un entorno transaccional.

1.3 OBJETIVOS DE LA TESIS

El objetivo de este trabajo de tesis es realizar un análisis de los diversos aspectos de seguridad de los sistemas de pago por Internet. Este análisis se enfoca a estudiar las características de operación, así como las ventajas y desventajas de sistemas de transacciones comerciales en forma electrónica. Para ello, primero se hará una revisión de los sistemas de pago tradicionales, y se describirán los distintos métodos de encriptación para resolver los problemas de los sistemas tradicionales. Posteriormente, se estudiarán las características de los nuevos sistemas de pago, su forma de operación y protocolos de seguridad. De este análisis de obtendrá una tabla comparativa de los esquemas de seguridad que actualmente están en operación a través del Internet.

1.4 LIMITACIONES

El desarrollo de este trabajo de tesis no tiene como objetivo el desarrollo de un nuevo protocolo de encriptación para sistemas de pago en tiempo real, más bien, se centra en un análisis cualitativo de los esquemas actualmente disponibles. De igual forma, este trabajo solo aborda los mecanismos de seguridad utilizados en transacciones a través del Internet, excluyendo del estudio los mecanismos de seguridad que se utilizan a nivel empresa para proteger la integridad de sus recursos e información.

1.5 ESTRUCTURA DE LA TESIS

En el primer capítulo se define el problema de seguridad asociado al intercambio de información privada a través de redes públicas. Se hace una revisión de los sistemas y protocolos de pago que se utilizan actualmente en el Internet.

En el capítulo 2 se definen las características del comercio electrónico y los conceptos básicos del procesamiento de información en una red de comunicaciones. Así mismo, se describe la actividad de comercio electrónico como una red de comunicación entre usuarios con distintos tipos de funciones.

En el capítulo 3 se describe la importancia de la seguridad en el proceso de intercambio de datos en redes públicas y privadas, y se proporcionan las bases

fundamentales de los sistemas de encriptación. Se describe el procedimiento para la transmisión de mensajes en forma segura, y se revisan las estrategias de seguridad que deben implementarse en una organización para mantener la privacidad, la integridad y la confidencialidad de la información.

En el capítulo 4 se hace un análisis de los diversos aspectos de seguridad de los sistemas de pago por Internet, con énfasis en su forma de operación y protocolos de seguridad. Se describirán los protocolos de pago y los esquemas de pago electrónico que actualmente están en operación a través del Internet.

En el capítulo 5 se realiza la comparación de los distintos esquemas de seguridad utilizados en los sistemas de pago electrónicos, sobre la base de las características descritas en el capítulo 4; se describen los resultados de esta comparación y se indican las tendencias futuras en el desarrollo de estos sistemas.

En el capítulo 6 se indican las principales conclusiones derivadas de este trabajo de investigación, así como las aportaciones y recomendaciones para trabajos futuros en esta área del conocimiento.

CAPÍTULO 2

CARACTERÍSTICAS DEL COMERCIO ELECTRÓNICO

2.1 ASPECTOS GENERALES

El Comercio Electrónico es un concepto general que engloba cualquier forma de transacción comercial o de negocios que se transmite electrónicamente usando las redes de telecomunicación y utilizando como moneda de cambio el dinero electrónico. Ello incluye intercambio de bienes, servicios e información electrónica. Incluye también las actividades de promoción y publicidad de productos y servicios, campañas de imagen de las empresas, marketing en general, facilitación de los contactos entre los agentes de comercio, soporte post-venta, seguimiento e investigación de mercados, concursos electrónicos y soporte para compartir negocios [2].

Desde una perspectiva muy simplista, el Comercio Electrónico puede entenderse como la automatización mediante procesos electrónicos de los

intercambios de información, así como de transacciones, conocimientos, bienes y servicios que en última instancia pueden conllevar o no la existencia de una contraprestación financiera, a través de un medio de pago.

Evidentemente, el Comercio Electrónico no se limita a Internet. Incluye una amplia gama de aplicaciones de banda estrecha (videotexto), difusión (telecompra) y entornos fuera de línea (venta por catálogo en CD-ROM), así como redes empresariales privadas (banca). Sin embargo, Internet, con sus robustos protocolos independientes de la red, está fusionando rápidamente las distintas formas de Comercio Electrónico. Las redes de empresa se convierten en intranets. Al mismo tiempo, Internet está generando numerosas nuevas formas híbridas de Comercio Electrónico que, por ejemplo, combinan publicidad televisiva digital (infomercials) con mecanismos de respuesta a través de la Red (para pedido inmediato), catálogos en CD-ROM con conexiones Internet (para actualizaciones de contenido y precios) y "Websites" comerciales con extensiones locales en CD-ROM (para demostraciones multimedia que precisan mucha memoria).

En este capítulo se presentan los conceptos generales del Comercio Electrónico, así como una descripción de las redes de cómputo utilizadas actualmente para este fin. También se hace una introducción a los problemas de seguridad asociados al intercambio de información a través de redes de comunicación.

2.2 REDES DE COMUNICACIÓN

El actual desarrollo en el área de computación ha sido acompañada por una evolución constante en las redes de comunicación de datos, siendo el Internet un claro ejemplo de ello. La Internet es una red de redes, compuesta por un gran número de computadoras conectadas entre sí por medios alámbricos e inalámbricos, como las señales de radio, LAN's, enlaces de fibra óptica, etc.. De esta forma cada una de las computadoras conectadas a la red está en la posibilidad de intercambiar información (audio, video, datos, etc.) con cualquiera otra computadora de la red, así como compartir recursos para tareas específicas. Los parámetros de operación de la Internet no son controlados por una entidad o empresa sino que cada uno de sus componentes son operados independientemente por sus usuarios y/o propietarios. La forma en que una computadora se vuelve parte de la Internet es a través del uso de un lenguaje de comunicación común, que en este caso es el protocolo TCP/IP. Por consiguiente cualquier computadora que opere bajo este protocolo está habilitada para conectarse a la Internet y explotar todas las ventajas de la conectividad que ésta ofrece.

Es evidente que la Internet representa la red de computadoras más grande a nivel mundial, sin embargo existen otros tipos de redes de computadoras que no forman parte de la Internet y que proporcionan servicios a un gran número de usuarios (sistemas comerciales, redes privadas, etc.). En este sentido la Internet ofrece una mayor ventaja para realizar funciones de transferencia de

información y manejo de transacciones comerciales, debido principalmente a que todo el procesamiento de información se realiza de forma distribuida y abierta. Esta ventaja puede convertirse en una debilidad si es que no se toman las medidas de seguridad para proteger los datos.

2.3 PROCESAMIENTO DE CÓMPUTO DISTRIBUIDO

Un ambiente de cómputo distribuido se representa mediante un conjunto de puntos de procesamiento (computadoras) que tienen la capacidad de realizar un mismo grupo de funciones, así como ejecutar bloques de actividades para llevar a cabo un proceso determinado. Por el contrario en un ambiente de sistema mainframe, los usuarios intercambian información a través de terminales conectadas en forma directa al mainframe, por lo que todo el proceso de cómputo se realiza por la computadora central (host), y las terminales se utilizan únicamente como interfaz para recibir y desplegar información. La Internet es un ejemplo de procesamiento distribuido donde no existe una computadora central y terminales, ya que cada una tiene capacidades de procesamiento independiente.

La diferencia entre una computadora host y terminal se basa en la función que ésta realiza, que puede ser de contenido y/o servicio. Una terminal típicamente establece una conexión con el host (servidor) e inicializa la solicitud de un servicio, como puede ser acceso a archivos específicos o aplicaciones (procesadores de texto, hojas de cálculos, programas de simulación, etc.). Sin

embargo, esta distinción entre un servidor y una terminal es arbitraria en términos relativos, ya que en una red de procesamiento distribuido, cada computadora conectada puede operar como terminal o servidor. Esta característica es una de las principales ventajas de la Internet, ya que el aumento en la conectividad gracias al procesamiento distribuido permite incrementar los volúmenes de información que pueden procesarse, así como la velocidad de transmisión de los datos a través de la red. En términos de mercado esto significa que cada computadora conectada a la red es un potencial proveedor de contenidos y/o servicios. En forma análoga al comercio tradicional, los clientes navegan en la red en forma similar a los espectadores de televisión y lectores de periódicos.

En términos comerciales el procesamiento de cómputo distribuido de la Internet permite establecer un ambiente interactivo donde los consumidores pueden ser también proveedores de servicios; esto queda de manifiesto con la proliferación de páginas personales de contenido comercial en la Internet. Además este ambiente interactivo da la posibilidad de realizar otro tipo de actividades, como la recopilación de los perfiles de los consumidores (usuarios de la Internet) para detectar preferencias acerca de productos y servicios. Esta es una clara ventaja sobre los medios de comunicación tradicionales (periódico, radio, televisión, etc.) debido a la interacción bidireccional que proporciona la Internet. En resumen, la Internet representa un sistema mundial de interacción para negocios y comunicaciones, donde las computadoras conectadas a la red representan puntos de presencia [8,9].

Debido a que no existe un criterio para definir si un usuario conectado a una red de procesamiento distribuido es un vendedor o un comprador, las transacciones comerciales tienen un comportamiento similar. Una transacción comercial típica involucra agentes y procesos (producción, ensamble, mercadeo, entrega, pago de impuestos, seguros, certificaciones, etc.). En este ambiente los agentes realizan uno o más de estos procesos. En el caso de una red de procesamiento distribuido, los agentes tienen la capacidad de llevar a cabo diferentes procesos en forma simultánea. Esto significa que el desempeño de los agentes en el comercio electrónico será muy diferente al realizado en mercados físicos. Por ejemplo, la diferencia tradicional entre un comerciante al por mayor y un minorista no está definido en el mercado digital porque un productor sólo necesita transmitir los requerimientos de un pedido a un agente determinado.

2.4 REDES ABIERTAS

En la actualidad existen grandes redes de computadoras compuestas de varias capas, muchas de las cuales están conectadas en redes de área local (LAN´s) a través de conexiones físicas. Las redes LAN pueden interconectarse con redes de área amplia (WAN) a través de líneas telefónicas o vía satélite. Por el contrario, las redes privadas de valor añadido (VAN) han operado durante más de dos décadas principalmente en transacciones compañía – compañía utilizando el protocolo de intercambio electrónico de datos (EDI). Sin embargo, los problemas de incompatibilidad en software y hardware, y las políticas de administración, han limitado las facilidades de conexión entre este tipo de

redes. Las redes VAN, por ejemplo, pueden ser accesadas sólo por miembros suscritos y usan estándares de comunicación propias. Existen diversas razones por las cuales es necesario superar estas diferencias y facilitar la comunicación entre redes, y la Internet es una de éstas.

La Internet es el único ambiente de red que está basado en estándares abiertos que permite que cualquier computadora o red de datos pueda conectarse empleando los protocolos TCP/IP. El protocolo de Internet (IP) es el protocolo básico que permite direccionar la transmisión de datos, mientras que el protocolo de control de transmisión (TCP) tiene la función de asegurar la integridad de los mensajes. Similar a los sistemas de comunicación postal, donde las direcciones y códigos postales hacen posible enviar y recibir mensajes sin restricción alguna, la dirección de Internet (IP o dominio) de una computadora permite comunicarse con cualquier computadora de la red [10].

La apertura de Internet facilita la interoperabilidad entre las diferentes plataformas de computadoras y soporta el intercambio de mensajes entre usuarios. Debido a esto, el potencial del comercio electrónico sobre el Internet supera al EDI o las redes VAN. El objetivo original de EDI fue reducir costos de operación, así como aumentar la eficacia y competitividad de las empresas, haciendo que las transacciones de negocios basadas en papel fueran obsoletas. No obstante, el nivel actual de aplicación de EDI no ha cumplido con estas espectativas debido en gran parte al requerimiento en la inversión para recursos específicos para este fin (software y hardware de características

especiales). Además, las transacciones EDI son limitadas a comunicaciones máquina-máquina basadas en lenguaje de máquina, hecho que ha limitado su aplicación. Debido a estos factores, EDI se ha limitado a un conjunto predeterminado de transacciones de datos.

Por el contrario, la Internet tiene un medio de comunicación más flexible y eficiente. La principal característica de Internet es su versatilidad para transmitir mensajes utilizando diferentes formatos, en un ambiente de una red de trabajo abierta. Usando una amplia variedad de software de aplicación, los usuarios de Internet tienen acceso a muchas actividades que el EDI no soporta, como la comunicación con contenido multimedia, disponibilidad de interfases amigables (navegadores Web) y capacidad de procesamiento distribuido. Estas ventajas han estimulado el uso de Internet como una herramienta para las comunicaciones y transacciones comerciales. En este sentido, es un hecho que el comercio electrónico basado en la Internet como red abierta propiciará una evolución de las tradicionales relaciones vendedor-comprador, produciendo una nueva área de investigación económica.

Sin embargo, a pesar de todas sus ventajas, la Internet tiene una serie de problemas potenciales. Aunque la apertura de los protocolos TCP/IP es la razón por la cual el Internet está creciendo tan rápido, también provee un problema serio en un medio comercial como son la falta de medidas de seguridad fundamentales en TCP/IP [11,12,13]. Comparado con las redes VAN's, el Internet tiene muchas debilidades en este respecto. Los mensajes pueden ser

fácilmente monitoreados y pueden ser accesados durante la transmisión. Los mensajes pueden ser alterados y retrasmitidos a otros usuarios. Debido a esto, ningún usuario de la red tienen la certeza completa de la integridad de los mensajes recibidos, así como del remitente de los mismos. El principal desafío en este aspecto es reunir los requisitos de seguridad esenciales para las transacciones computacionales: la confidencialidad, la autenticación, la integridad de los datos y la repudiación.

Actualmente, los métodos de encriptación y tecnologías de acceso digital proporcionan un adecuado nivel de seguridad, que actualmente está en uso para asegurar la privacidad de los mensajes transmitidos a través de Internet. Estas medidas de seguridad son aplicadas a cada mensaje que es transmitido, en forma similar en que un sobre con timbre postal protege el mensaje dentro de él. Alternativamente los medios de comunicación deben tener medidas de seguridad similares. Las nuevas generaciones de protocolos de Internet están incorporando medidas de seguridad en niveles TCP/IP asegurando la continuidad de la transferencia. En resumen un adecuado control de acceso y seguridad a través de métodos de encriptación permite que el Internet proporcione una seguridad más robusta aunque todavía imperfecta.

Aunque el nivel de funcionamiento garantizado por la Internet es menor con respecto a redes privadas, la posibilidad de un problema de grandes consecuencias es menor para la Internet en comparación a las redes privadas, las cuales son controladas y administradas por una autoridad central. Un

mensaje que está siendo transmitido en la Internet puede ser enviado por rutas alternas si una parte de la red falla. Al mismo tiempo el espionaje en la Internet no está dirigido a un objetivo específico como en el caso de las redes privadas. Como las redes privadas portan información clasificada sobre la misma red, el resultado de un error de seguridad es más severo que en el caso de la Internet, donde los paquetes de mensajes se transmiten entremezclados. Este problema se resolverá una vez que los estándares de Internet sean implementados utilizando técnicas de encriptación, como empieza a suceder actualmente.

A pesar de que la seguridad y la confiabilidad de la Internet se incrementará con los nuevos protocolos de comunicación, el incremento en el tráfico de mensajes originado por aplicaciones en tiempo real (video, audio, etc.) pueden ocasionar que estas mejoras no sean evidentes en términos de congestión de la red. Una solución en este sentido es incrementar el ancho de banda de la Internet a través de tecnologías de compresión más eficientes, módems con tasas de comunicación más elevadas, entre otras. Sin embargo actualmente existe un incremento en la demanda del poder de procesamiento en las computadoras originado por el rápido desarrollo de microprocesadores de bajo precio. Similarmente el problema de congestión se puede volver más crítico para el comercio electrónico que los problemas de seguridad que han preocupado a muchos futuros comerciantes electrónicos.

Así mismo las aplicaciones de comercio electrónico se están desarrollando en las distintas formas en las cuales se realiza el comercio actualmente, como son dentro de la empresa, empresa-consumidor, y empresa-empresa; estas aplicaciones incluyen: manejo de mensajes y correo electrónico interno, publicación de documentos corporativos en línea, búsquedas de información, distribución de información crítica y calendarizada a los empleados, manejo de finanzas, logística, inventarios, interacción con proveedores y consumidores, rastreo de órdenes de compra, etc.. Más importante que el número de áreas que están siendo afectadas por el comercio electrónico es el hecho de que estas actividades pueden ser integradas dentro de un proceso único. Esto significa que las áreas mencionadas no son aplicaciones individuales, sino que son un aspecto del entorno global del comercio electrónico. En resumen el potencial del comercio electrónico para los negocios reside en su capacidad de innovar e integrar los procesos de negocio y mercado, en este sentido el tener transacciones eficientes es uno de los usos más obvios e inmediatos del comercio electrónico.

2.6 COMERCIO ELECTRÓNICO COMO UNA RED DE COMUNICACIONES

En términos generales, el comercio electrónico tradicional consiste en el uso de medios electrónicos para realizar transacciones comerciales, con el objetivo de mejorar la eficiencia en los procesos y organizaciones. En este entorno, la implantación del comercio electrónico a través de Internet consiste básicamente en sistemas de pago en línea. Una definición más específica del comercio

electrónico establece que el comercio electrónico a través de Internet es un intercambio electrónico de datos en red (EDI por sus siglas en inglés, Electronic Data Interchange) con un sistema de manejo de mensajes más flexible. De manera tradicional, los EDI estaban limitados a un cierto grupo de datos que las computadoras podían procesar, y que correspondían a información en formas electrónicas utilizadas para transacciones de negocios. Por el contrario, una EDI abierta implementada a través de Internet significa que los mensajes EDI pueden ser enviados y recibidos a través de correo electrónico. En otro nivel de complejidad, las EDI pueden usar formas electrónicas disponibles para los consumidores en páginas Web. Esta forma de operación es considerada como comercio electrónico, donde el uso de Internet tiene el objetivo de mejorar la comunicación, especialmente en las transacciones del tipo negocio-negocio.

Acorde a ello, las formas de hacer negocios en el Internet estan enfocadas en problemas de organización y operación, que incluyen tópicos de seguridad, ventajas competitivas en el desarrollo de productos, investigación y desarrollo, y sistemas de automatización.

Actualmente, muchas empresas consideran que la implementación de actividades de empresa-empresa en Internet no presentan ventajas significativas con respecto a las tradicionales EDI. El principal problema es la seguridad de los datos; esto ha provocado la controversia entre la utilización de redes restringidas del tipo VAN que utilizan la forma tradicional de EDI con respecto a una red "menos segura" con un mayor nivel de flexibilidad y con

posibilidad de manejo de mensajes implementado a través del Internet. Sin embargo, cada día es mayor el número de empresas que ofrecen productos y servicios a través de Internet, con evidentes ventajas sobre los métodos de mercadeo tradicionales.

2.6.1 Comercio electrónico de productos digitales

A pesar de la apertura provocada por el comercio electrónico, el manejo del Internet en forma comercial aún es visto como un nuevo medio de comunicación. Sin embargo, el Internet es un medio de comunicación muy eficiente, por lo cual puede facilitar los procesos de mercadeo, compras en línea, y servicio al cliente, dejando a un lado los medios tradicionales. Con el desarrollo de los sistemas de cobro en línea, el significado de las transacciones ha cambiando en manera dramática, en especial a lo que se refiere al costo y velocidad por transacción. Estos cambios han comenzado a afectar a los mercados en forma física y en los productos digitales que se comercializan por Internet, incluyendo aspectos como los procesos de manufactura y sistemas de distribución.

El área de los negocios de productos digitales en Internet está avanzando en forma radical, y requiere cada vez mayores desarrollos en la estructura de comunicación, sistemas de cobro electrónico, elaboración de leyes de privacidad y derechos de autor, manejo de impuestos, entre otras áreas. Estos desarrollos requieren la definición de nuevos modelos para el análisis de

negocios y sus procesos asociados, utilizando para ello las nuevas tecnologías de multimedia disponibles en la actualidad. De esta forma, se llegará al concepto de negocios totalmente digitales.

La Fig. 2.1 muestra la diferencia entre la esencia del comercio electrónico y las aplicaciones electrónicas convencionales. En un mercado de negocios existen tres componentes: los agentes consisten de vendedores, compradores e intermediarios. La interacción entre los agentes y productos representa los procesos, que incluyen la selección de productos, producción, mercadeo, órdenes de compra, entre otras. Estos tres componentes se dividen a su vez en físicos (fuera de línea) y digitales (en línea). Un ejemplo de esta división puede aplicarse a los consumidores, de los cuales los consumidores "digitales" son aquellos que realizan las compras de un producto a través de Internet y los consumidores "físicos" son aquellos que visitan una tienda y realizan la compra. Ejemplos similares se aplican a los otros dos componentes, productos y procesos.

Los cubos sombreados en la figura indican el comercio tradicional (los tres componentes son físicos) y el comercio electrónico (componentes digitales). Los cubos no sombreados representan actividades de negocio que utilizan ambos enfoques. Sin embargo, como lo muestra el tamaño de los cubos indica el crecimiento evidente en el uso de procesos digitales para la realización de transacciones del tipo negocio-negocio. Esto se debe a que todos los procesos

y servicios tienen el potencial de convertirse en un intercambio de productos digitales a través de una red digital.

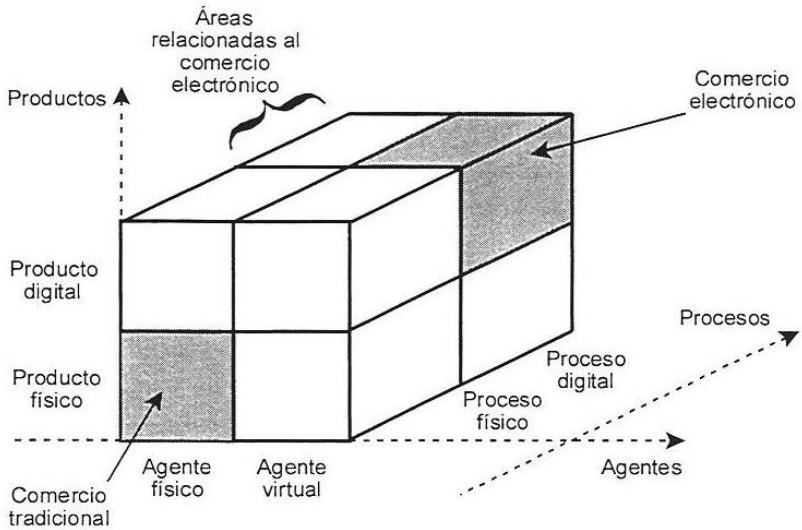

Fig. 2.1. Áreas del comercio electrónico.

En resumen, el actual comercio electrónico consiste de dos aspectos altamente relacionados: 1) la expansión en el uso de redes abiertas en lugar de las tradicionales EDI para interconectar redes privadas con Internet, y 2) nuevas oportunidades de mercado en el Internet a través de productos digitales [15]. Sin embargo, aún existen problemas por resolver como son el incremento en el ancho de banda para sistemas multimedia y aplicaciones en tiempo real y, el mejoramiento de la seguridad en la transmisión de datos a través de tecnologías de encriptación y nuevos protocolos para Internet. Esto incluye el desarrollo de sistemas de pago en línea.

2.6.2 Seguridad y privacidad en transacciones por Internet

El problema de seguridad en la transmisión de datos en Internet es citada como la principal limitante para el crecimiento del comercio electrónico. Aunque existen importantes avances en términos de seguridad, aún se considera que existen riesgos para la realización de transacciones comerciales.

Actualmente, las medidas de seguridad pueden ser implementadas en diferentes niveles. Los niveles de seguridad en la red aseguran el medio de intercambio de datos, mientras que los procesos de encriptación aseguran los datos que se transmiten por el medio.

Sin embargo, cada proceso exige diferentes medidas de seguridad; un sistema de pago seguro debe proteger información privada de manera que no sea "vista" o "robada". Por el contrario, una transacción solo puede ser segura si reune los requisitos de no-repudiación, autenticación, integridad y confidencialidad. La no-repudiación significa que ninguno de los agentes involucrados pueden negar la transacción una vez que ésta se realiza. La autenticación se refiere a la habilidad para verificar la identidad de los agentes involucrados en la transacción. Por otra parte, la integridad significa que los datos transferidos durante la transacción no pueden ser modificados o almacenados en el proceso, finalmente la confidencialidad está asociada al hecho de que la transacción es privada y solo está disponible para los agentes participantes.

Una forma de privacidad es el anonimato, donde la identidad de un agente que participa en una transacción no es conocida por los otros participantes. Los aspectos no-repudiación y autenticación están siendo explorados a través del desarrollo de tecnologías de certificación. Por otra parte los problemas asociados a la integridad de los datos y confidencialidad han sido ampliamente resueltos a través del uso de tecnologías de encriptación y firmas digitales [16]. Tanto la integridad como la confidencialidad están íntimamente relacionados con los derechos constitucionales de privacidad y la protección de la libre expresión [15], sin embargo estas implicaciones no son tratadas en este trabajo.

2.7 CONCLUSIONES DEL CAPÍTULO

El comercio electrónico se define como la automatización del conjunto de procesos electrónicos necesarios para intercambio de información, relacionada con transacciones, conocimientos, bienes y servicios a través de una red de comunicación pública o privada.

CAPÍTULO 3

SEGURIDAD EN REDES DE COMUNICACIÓN

3.1 INTRODUCCIÓN

Una de las características de las redes abiertas como el Internet son sus bajos niveles de seguridad o privacidad de los datos que se transmiten por la red. La mayoría de las violaciones de seguridad tienen su origen en una pobre implementación de los mecanismos de control de acceso de los distintos servidores conectados a la red.

En este capítulo se presentan los conceptos básicos de seguridad en redes abiertas. Se describe las bases de los sistemas de encriptación utilizados actualmente y se realiza una revisión de las distintas etapas para la transmisión de mensajes en forma segura y privada. Al final del capítulo se hace un análisis de las políticas de seguridad que deben implementarse en redes abiertas y/o redes privadas conectadas a Internet.

3.2 IMPORTANCIA DE LA SEGURIDAD

En general, todo sistema de información, conectado o no a una red abierta como el Internet, debe considerar los mecanismos de seguridad más apropiados para salvaguardar la privacidad de los datos. Estos mecanismos son más complejos a medida que se incrementa la confidencialidad de los datos a proteger, como por ejemplo los sistemas de pago con tarjeta de crédito y otras transacciones financieras.

Estos mecanismos de seguridad deben cumplir dos funciones: mantener la privacidad de la información contenida en los servidores y tener control de los accesos a la red de transmisión de datos para mantener la confidencialidad de los datos que se transmiten. Si alguna de estas dos funciones falla, el sistema completo es vulnerable. Por ejemplo, Kevin Mitnik obtuvo 20,000 números de tarjetas de crédito antes de ser detenido en 1995 [17]; en lugar de intentar monitorear las transacciones de pago en Internet, violó la seguridad de un servidor y tuvo acceso a los archivos donde se almacenaba esta información. De éste y otros ejemplos se puede concluir que los niveles de seguridad en redes abiertas como Internet son muy importantes, ya que la información tiene un valor significativo.

Debido a la evolución en los sistemas de cómputo, protocolos de comunicación, y al incremento del número de usuarios y servicios, los aspectos de seguridad

se han convertido en un problema dinámico. En general, los aspectos de seguridad están asociados a tres áreas principales [18]:

- Seguridad en la transmisión de archivos e información incluyendo transacciones seguras.
- Seguridad de la información contenida en los servidores conectados a Internet.
- Seguridad en redes privadas, especialmente cuando son utilizadas como parte del comercio electrónico.

El objetivo principal en la implementación de mecanismos de seguridad es minimizar el robo de información y los accesos a usuarios no autorizados tanto como sea posible, sin alterar la transparencia que deben tener los usuarios autorizados a tener acceso a la información.

Actualmente, las compañías que utilizan el Internet para actividades de comercio electrónico enfrentan dos retos. Uno de ellos es la necesidad de automatizar los esquemas de protección de archivos e información cuando los medios físicos y administrativos de seguridad son sustituidos por sistemas de cómputo. Esto se vuelve más evidente si los sistemas son accesados a través de una red pública. El segundo reto que afecta la seguridad es la diversificación de sistemas de información distribuidos así como la utilización de medios de comunicación para transmitir datos entre usuarios y servidores.

Estos problemas se conocen como seguridad de cómputo y red, y ésta se define como la protección de un conjunto de recursos conectados en red contra accesos no autorizados, y la modificación, utilización o destrucción de la información.

A medida que aumente el número de usuarios en Internet, el riesgo de violaciones de seguridad se incrementa. Existen diversas razones para violar la seguridad de un sistema, entre las que se encuentran las siguientes:

- Obtener información económica o de tendencia de mercados de organizaciones privadas líderes en su campo.
- Obtener información económica de dependencias del gobierno.
- Obtener información privada de otras personas.
- Realización de transacciones fraudulentas.
- Violación de los derechos individuales por parte del gobierno.

Las características del problema de seguridad en una organización varían en dependencia del tipo de información que se desea resguardar. En la Tabla 3.1 se enumeran algunas de las técnicas de acceso no autorizado utilizadas para obtener acceso a información restringida. Existen dos tipos de accesos no autorizados a una red, los pasivos y los activos (Fig. 3.1). En el caso de los pasivos, un usuario no autorizado monitorea la transmisión de datos a través de la red sin alterar los datos. En el caso de los activos, el usuario introduce

cambios en los datos o la incorporación de nuevos datos con un fin específico. Debido al tipo de actividad los usuarios pasivos son más difíciles de detectar, aunque existen medidas para prevenir su acceso al sistema.

Tabla 3.1. Técnicas de acceso no autorizado.

Robo de acceso	Acceso a contraseñas y passwords sin autorización.
Robo de recursos	Uso de recursos de la red para almacenar software y datos sin autorización.
Virus	Programas para enviar información al creador del programa o provocar algún tipo de daño.
Falsificación de correo electrónico	Envío de correo electrónico utilizando direcciones falsas.
Observación de correo electrónico	Acceso sin autorización para observar los mensajes de correo electrónico sin autorización en un punto de la red.
Espionaje de información	Observar el tráfico de información, y almacenar contraseñas y password para tener acceso posteriormente.
Suplantación	Asumir la identidad de un usuario a través del uso de direcciones IP y contraseñas de acceso.
Ataques	Acceso a datos cuando los programas están en ejecución en un servidor de la red.
Caballos de Troya	Virus almacenados dentro de programas, con el fin de rastrear información o realizar acciones destructivas en el sistema.
Puertas traseras	Creación de passwords secretos para tener acceso ilimitado a un servidor o aplicaciones instaladas en un servidor.

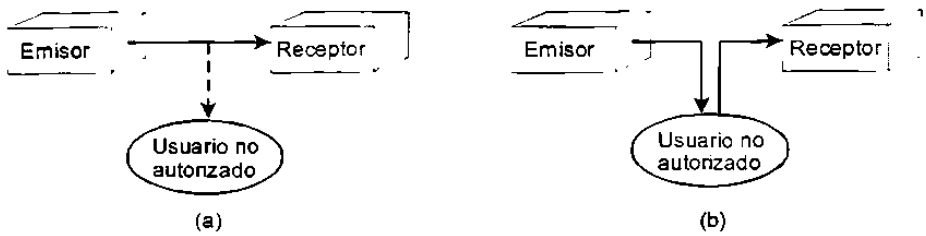

Fig. 3.1. Accesos no autorizados a una red, (a) pasivos, (b) activos.

Existen estrategias básicas de seguridad que pueden ser utilizadas para resolver los problemas de acceso no autorizado descritas previamente, tales como control de acceso y la verificación e integridad, confidencialidad y autenticación de la información. Adicionalmente es necesario que la organización estructure una política de seguridad adecuada.

3.3 CRIPTOGRAFÍA

El término criptología viene de dos palabras griegas krupto (κρυπτο) y grafh (γραΦη), *"escritura oculta"*, y ha evolucionado desde las antiguas técnicas de transposiciones y sustituciones de símbolos ya utilizadas en las antiguas civilizaciones griega y romana a los métodos basados en algoritmos matemáticos; estos algoritmos son los que se usan para garantizar la confidencialidad de la información y son la base de las técnicas de integridad de información y algunos métodos de autenticación, cifrar es otro término que se utiliza para la misma función. Encriptar consiste en aplicar un proceso matemático o algoritmo a un texto legible para convertirlo en algo totalmente

ininteligible [19,20]. Este proceso matemático (algoritmo) necesita de una clave de tal forma que al aplicar el mismo algoritmo a un texto con claves diferentes, el resultado es diferente y único para cada clave. Básicamente existen dos tipos de sistemas: simétricos y asimétricos.

3.3.1 Sistemas simétricos

Los sistemas simétricos de criptografía son los más sencillos, y se conocen como métodos de criptografía convencional; en los sistemas simétricos, la clave para descifrar la información es la misma que se utiliza para cifrar la información, o en algunos casos, es una variación directa de ella de la primera (Fig. 3.2).

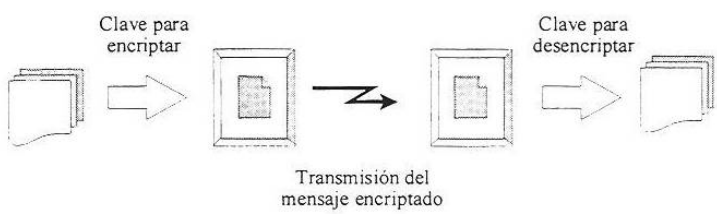

Fig. 3.2. Sistema de criptografía simétrico.

En estos sistemas, para encriptar un mensaje es necesario tener el algoritmo de encriptación (programa) y su clave personal, la cual debe ser distribuida a todos los usuarios que requieren enviar mensajes encriptados. El principal problema de este tipo de sistemas es la distribución de la clave personal, ya que tanto el emisor como el receptor de un mensaje deben utilizar la misma clave; esto hace

inseguro el envío de la clave independientemente del medio que se utilice (comunicación oral, correo electrónico, etc.). En definitiva, un usuario no autorizado que conozca esta clave tendrá acceso a todos los mensajes, lo que se considera una gran debilidad en la seguridad; debido a ello, la tendencia actual de los sistemas de clave simétrica es utilizarlos poco o en casos en que no se requiere un alto grado de protección.

Los principales algoritmos de encriptación simétrica son [21]: DES (Data Encryption Standard), 3DES (o Triple DES), IDEA (International Data Encryption Algorithm), RC2, RC4 y el Blowfish.

DES (Data Encryption Standard). Este algoritmo es el más conocido, y funciona de la siguiente manera: se divide el mensaje en su mitad izquierda y su mitad derecha (L, R), luego se transforma en un nuevo mensaje, según el procedimiento mostrado en la Fig. 3.3.

$$L_0, R_0$$

$$L_i = R_{i-1} \qquad i=0,\ldots,16$$

$$R_i = L_{i-1} + f(R_{i-1}, K_i)$$

$$f(R_{i-1}, K_i) = P(S(K_i + E(R_{i-1})))$$

Fig. 3.3. Algoritmo DES.

En este ejemplo, E es una función de expansión de 32 bits en 48 bits, K_i es la clave utilizada en cada ronda, S es la s-box que aplica una función aleatoria y P es una función de permutación final.

3.3.2 Sistemas asimétricos

El objetivo de los sistemas asimétricos es resolver los problemas de seguridad que presentan los sistemas simétricos; en estos sistemas cada usuario dispone de dos claves, una privada y otra pública, de tal forma que lo que una cifra la otra descifra y viceversa. Lo importante en este proceso es que la clave privada sólo la conoce el usuario propietario de ella, y la clave pública se distribuye a todos los usuarios autorizados para enviar mensajes cifrados; si un usuario sin autorización capta un mensaje no podrá descifrarlo ya que sólo se descifra con la clave privada de cada usuario. De esta forma la clave pública se utiliza para encriptar y la privada para desencriptar (Fig. 3.4)

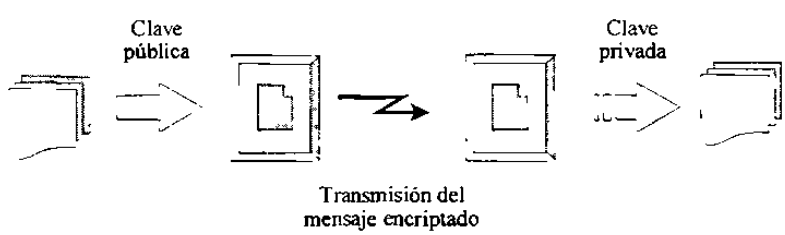

Fig. 3.4. Sistema de criptografía asimétrico.

Los algoritmos de clave pública, como RSA, están sustentados en una base matemática tal que cada una de las partes participantes dispone de un par de

claves: una se denomina clave pública, y está destinada a ser distribuida libremente. Es más, cuanto más ampliamente se haya distribuido esta clave, más garantías existen de que no es posible la "usurpación de personalidad". La otra clave, la clave privada será conocida solamente por su legítimo propietario, y debe ser custodiada con el mismo celo con que se haría para una clave DES. La base matemática aludida anteriormente hace que mientras que un mensaje puede ser encriptado con la clave pública, es necesaria la clave privada para su desencriptación. El mensaje original es encriptado con la clave pública del destinatario; este podrá obtener el mensaje original después de aplicar su clave privada al mensaje cifrado. Se resuelve así el problema de la distribución de claves sobre canales no seguros.

RSA (RIVEST-Shamir-Adelman) [22]. El algoritmo funciona sobre la base del Teorema de Fermat [23], que enuncia que si p es un número primo y a es un número positivo, cualquiera menor que p entonces $a^{(p-1)}=1$ (módulo p). Este criterio proporciona un método rápido para demostrar que un número es compuesto. Sin embargo, existe una gran dificultad en hallar los dos factores primos de un número de aproximadamente 126 cifras, obtenido de multiplicar dos números primos de 63 cifras. El tiempo de factorización se eleva a millones de años.

Para cifrar un texto primero se transforma en un único número mediante la clave típica: A=0, B=1, ... Z=26 y 00 para indicar el espacio entre dos palabras. El número completo se codifica elevándolo a una potencia fija s, módulo un

cierto número compuesto *n*. Este número *n* compuesto se obtiene eligiendo al azar dos números primos *p* y *q* y multiplicándolos. Se calcula la función de Euler *O*=(*p*-1)(*q*-1) y tras ello se seleccionan dos números, *e* y *d*, donde uno de ellos debe ser primo (al menos respecto de *O*) y encontrarse en el intérvalo (max(*p*,*q*)+1,*n*-1) de tal forma que se cumpla que *e***d*=1 mod *O*. Es decir, que exista un número *t* que haga que *e***d*=*t***O*+1. Todo esto hace que conociendo *O* sea fácil calcular *e* a partir de *d* y viceversa; sin embargo, para conocer *O* es necesario conocer *p* y *q*, lo cual sólo es posible factorizando *n*, que como ya hemos comentado es altamente complejo. Este es la base del algoritmo RSA, y es el más extendido y empleado en la actualidad para encriptación de datos y firma electrónica.

Se puede realizar un ejemplo práctico del funcionamiento de este algoritmo con números primos pequeños. Por ejemplo, sean *p*=5 y *q*=11, de lo que obtenemos *n*=5*11=55. De ahí, *O*=4*10=40=5*2^3. Podemos tomar *e* como 7 ya que no tiene factores comunes con *O*. Para calcular un valor de *d* se hace *d*=(*O***t*+1)/*e*=(40**t*+1)/*e*, que con *t*=0.5 tenemos *d*=3. Así, se obtiene que una clave es el par (7, 55) y la otra el par (3, 55).

Para el proceso de cifrado se toma la frase a codificar convertida en número y se eleva a la potencia (de 7 o de 3, dependiendo del par elegido para cifrar). El resultado se divide por 55 y se toma el resto; este es el mensaje cifrado. Para descifrar se toma el mensaje cifrado y se eleva a la potencia (de 3 o de 7, el contrario del elegido para cifrar), se divide por 55 y el resto será el mensaje

original. Para encriptar, por ejemplo 23, hacemos 23^7 mod 55 = 12 y para desencriptar 12^3 mod 55 = 23.

Resumiendo, el algoritmo RSA trabaja de la siguiente forma:

1. Se escogen dos números primos suficientemente grandes, p y q.
2. Se calcula $n = p^*q$
3. Se forman las claves: clave privada: $f(n,e)$; clave pública: $f(n,d)$, donde $(e,d) = f(p, q)$.

Otros algoritmos de criptografía asimétrica son el DSS (Digital Signature Standard) y el ECC (Elliptic Curve Criptography) [21].

3.4 AUTORIDADES DE CERTIFICACIÓN

El mecanismo de operación de los sistemas asimétricos soluciona el problema de seguridad de los sistemas simétricos, ya que no es necesario distribuir ninguna clave privada, sólo las claves públicas. Sin embargo, es necesario resolver el problema de "usurpación de personalidad", es decir, que alguien que no es realmente a quien se desea enviar el mensaje, se haga pasar por él, entregando su clave pública, y capturando todos los mensajes dirigidos al destinatario original; de esta forma, el intruso puede reenviar los mensajes al destinatario original, encubriendo su operación y haciendo difícil identificarlo

(Fig. 3.5). Para resolver este problema surgen las autoridades de certificación (AC).

Las Autoridades de Certificación cumplen con una función notarial en donde verifican la identidad y solvencia de usuarios y entidades proporcionando un "certificado digital" o "Digital ID". La certificación en redes abiertas utiliza certificados basados en el estándar X.509 [24] que permite a) firmar digitalmente los mensajes de tal forma que el receptor pueda descifrarlos y tener acceso a su contenido, garantizando la autenticidad y el no repudio, b) cifrar la información (encriptación) de tal forma que sólo el receptor pueda descifrarlos y tener acceso a su contenido, garantizando su integridad y confidencialidad, y c) dar seguridad y autenticar la identidad de acceso de los usuarios de sistemas intranets/extranets.

En general, un certificado digital contiene la clave pública de la persona o entidad para la que se emite, junto con información propia, y todo ello firmado electrónicamente por una autoridad de certificación. Actualmente, la principal autoridad de certificación que existe es "VeriSign" (*www.verisign.com*), la cual extiende certificados tanto para empresas como para personas, además de ofrecer servicios de seguridad completos, para redes de intranets, extranets y comercio electrónico.

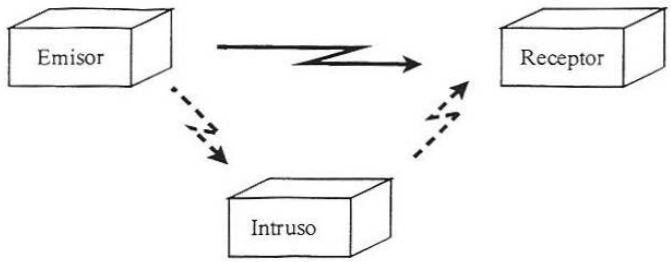

Fig. 3.5. Usurpación de personalidad.

3.5 INTEGRIDAD DE LOS DATOS: FUNCIONES HASH

Otro problema que se suscita en la transmisión de datos, es la integridad. Si bien no es posible leer el mensaje transmitido, ya que está encriptado, si puede ser modificado, ya sea quitándole o agregándole bits. El control de la integridad de la información se basa en el empleo de firmas digitales que son resumenes de mensajes cifrados. Una firma digital, asegura la autenticación de quien envía el mensaje, así como la integridad del mismo, ya que junto con la firma, se envía un código único el cual es calculado por una función denominada función Hash. Estas funciones comprimen el mensaje, y producen un "resumen", el cual es comprobado, para asegurar que se mantenga la integridad del mensaje original (Fig. 3.6).

Fig. 3.6. Función Hash.

Una función Hash (función de comprobación aleatoria) se define como una función capaz de reducir un mensaje determinado en un conjunto de datos, denominado resumen, de longitud mucho menor que el mensaje, usualmente de 128 ó 254 bits. Un valor Hash es generado por una función *H* de la forma :

$$h = H (M)$$

donde *M* es el mensaje de longitud variable, y *H*(*M*) es un valor Hash de longitud fija. El valor Hash es añadido al mensaje por el emisor , y el receptor autentifica el mensaje volviendo a generar el valor Hash y comparandolo con el recibido. Generalmente es necesario encriptar la función Hash, ya que no está protegida o considerada como secreta.

El propósito de una función Hash es producir una "huella digital" de un mensaje, o un bloque de datos. Para que una función Hash pueda utilizarse en los procesos de autenticación y firmas digitales, debe poseer las siguientes propiedades :

- *H* debe poder aplicarse a bloques de datos de cualquier longitud.
- *H* debe producir una salida de longitud fija.
- *H*(*M*) debe ser relativamente fácil de calcular a partir de *M*.
- Dado un valor Hash *h*, debe ser computacionalmente infactible encontrar *M* de la forma *H*(*M*) = *h*.

- Dado un mensaje cualquiera *M*, debe ser computacionalmente infactible encontrar un mensaje *N*, diferente de *M*, con $H(N) = H(M)$.
- Debe ser computacionalmente infactible encontrar un par (*M*,*N*) tal que $H(M)=H(N)$.

Las tres primeras propiedades son requeridas para poner en práctica sistemas de autenticación de mensajes en aplicaciones de comunicaciones. La cuarta propiedad es "one-way", es decir, es fácil generar un código dado un mensaje, pero virtualmente imposible generar el mensaje dado el código. La quinta propiedad garantiza que la realización de una función Hash a un mensaje alternativo no puede ofrecer el mismo valor que el mensaje original. En general, una función Hash que cumpla con las primeras cinco propiedades es una función débil. Si la función Hash cumple además con la sexta propiedad, ésta se denomina una función Hash fuerte.

Los algoritmos de funciones Hash deben de contar con dos propiedades adicionales: deben ser irreversibles e impredecibles. Esto significa que dado un resumen no se puede encontrar un mensaje que lo genere, ya sea invirtiendo el algoritmo o intuyendo la naturaleza del mensaje que lo produjo.

Por tanto, el mecanismo de control de integridad de un mensaje es el siguiente: una vez escrito el mensaje el autor genera el resumen mediante un algoritmo de resumen públicamente conocido. Luego cifra ese resumen con su clave privada e incluye el resumen cifrado al final del mensaje. Cuando alguien va a leer el

mensaje, para asegurarse de que no ha sido alterado; para ello toma el resumen cifrado del autor y lo decifra con su clave pública. Luego él mismo aplica el algoritmo de resumen sobre el mensaje y compara su resumen con el obtenido por el autor. Si los resumenes son iguales, significa que el mensaje es auténtico, de lo contrario, significa que ha sido alterado. En este mecanismo se deben resaltar dos aspectos fundamentales:

- Es esencial que el resumen sea cifrado por el autor, a fin de evitar que un intruso modifique el mensaje y genere un nuevo resumen. De este modo, el intruso no tiene posibilidades de cifrar de nuevo por desconocer la clave privada del autor.
- La seguridad del proceso se basa en que a partir del resumen no es posible encontrar el mensaje que lo genera; de esta forma es imposible que cualquier intruso sustituya el mensaje original por otro mensaje sin que los usuarios autorizados detecten la alteración.

Los algoritmos de resúmenes (Hash) más comunes son el MD5, el SHA, el HAVAL, y el SNEFRU [25]. A continuación se da una breve descripción de cada uno.

MD5. El MD5 es un algoritmo de resumen desarrollado por Ronald Rivest y distribuido por RSA Data Security, evolucionado de los anteriores MD2 y MD4. Este algoritmo genera resúmenes de 128 bits a partir de un bloque de texto de cualquier longitud. Para ello divide el texto en bloques de tamaño fijo y luego

realiza una serie de operaciones matemáticas en bloques sucesivos. Éste es el algoritmo de resumen más extendido, y actualmente se utiliza en el estándar de certificados digitales X.509v3 de ISO e ITU, lo cual hace que esté presente en muchas otras especificaciones y estándares, algunos tan importante como SSL, S/MIME y SET. Aunque es un algoritmo técnicamente bueno y rápido, los resumenes de 128 bits empiezan a verse limitados, ya se empieza a requerir algoritmos con un mayor tamaño de resumen.

SHA. El SHA (Secure Hash Algorithm) fue desarrollado en el NIST americano (National Institute of Standards and Technology) con ayuda de la NSA (National Security Agency). Está relacionado con el MD4, y la principal mejora es que usa resúmenes de 160 bits en lugar de 128.

HAVAL. Este algoritmo es una modificación del MD5 desarrollada por Zheng, Pieprzyk y Seberry. El tamaño del resumen es ajustable de 92 a 25 bits, y tiene también un número ajustable de interacciones del algoritmo interno. Esto hace que pueda configurarse para ser más rápido que el MD5, a costa de perder fortaleza.

SNEFRU. Este es un algoritmo diseñado por Ralph Merkle que produce resúmenes de 128 a 256 bits. Puede trabajar con cuatro u ocho iteraciones del algoritmo interno, pero se ha descubierto recientemente una debilidad del algoritmo que hace que sólo sea seguro con ocho iteraciones, lo que lo hace significativamente más lento que el MD5 y el HAVAL.

3.6 FIRMAS DIGITALES

Los mensajes de autenticación generados por las funciones Hash protegen a dos usuarios del intercambio de mensajes contra un tercer usuario. No obstante, no protege a los dos usuarios cuando se trata del enfrentamiento entre ambos.

Por ejemplo, en el caso de que el usuario A envíe un mensaje autenticado al usuario B mediante un sistema de autenticación con una función Hash, pueden ocurrir las siguientes disputas entre ambos: a) El usuario B puede crear un mensaje y reclamar que proviene de A. Para ello, B crea un mensaje falso, aplica la función Hash y encripta el resultado con la clave secreta de A y B, previamente intercambiada. b) El usuario A puede negar haber enviado un mensaje, porque es posible que B lo haya creado y no hay manera alguna de probar que A en realidad no ha enviado el mensaje.

Esta situación puede presentarse en casos de transferencias bancarias y otras operaciones monetarias, convirtiéndose en casos delicados debido al tipo de información que se esta transmitiendo. En estas situaciones donde no hay confianza entre el emisor y el receptor, el proceso de autenticación no es suficiente. La solución más utilizada es la firma digital (Fig. 3.7) [4,13,16]. La firma digital es semejante a la firma escrita de un documento. Ésta ha de tener las siguientes propiedades :

- Debe ser posible verificar el autor, la fecha y el tiempo de la firma.
- Deber ser posible autenticar los contenidos durante el proceso de firma.
- La firma debe ser verificada por tres partes, para resolver conflictos o disputas.

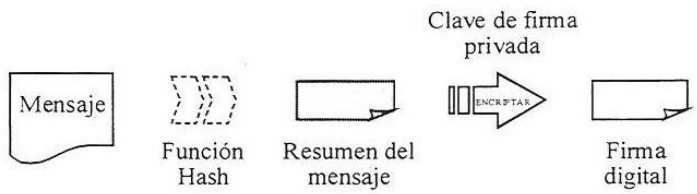

Fig. 3.7. Proceso de firma digital.

Por lo tanto, la función de firma digital debe incluir la función de autenticación (función Hash). En base a las tres propiedades anteriores, se pueden formular los siguientes requerimientos para una firma digital :

- La firma debe ser una parte extraída del mensaje que se quiere firmar.
- La firma debe utilizar información exclusiva del emisor, para evitar la creación de mensajes falsos y evitar conflictos.
- Debe ser relativamente fácil producir una firma digital.
- Debe ser relativamente fácil reconocer y verificar la firma digital.
- Debe ser computacionalmente infactible crear una firma digital, ya sea formando un nuevo mensaje para una firma digital existente o crear una firma digital falsa dado un mensaje.
- Debe de ser factible retener una copia de la firma digital almacenada.

3.7 PROCESO DE TRANSMISIÓN DE UN MENSAJE EN FORMA SEGURA

A continuación se analizará el proceso de transmisión de un mensaje entre dos usuarios, utilizando todos los métodos de seguridad descritos previamente.

En este caso se asume que el usuario A enviará un mensaje al usuario B de modo seguro. Para lograr este objetivo, el usuario A realiza el siguiente proceso (Fig. 3.8):

El usuario A utiliza la función Hash para crear una versión resumida del mensaje (1), y con su clave privada, firma digitalmente el mensaje (2). Posteriormente, reúne su mensaje, su firma y su certificado, y los encripta usando una clave privada simétrica (3), ya que resulta muchas veces mas económico la encriptación simétrica que la asimétrica. De esta forma, el usuario A tiene un mensaje encriptado. A continuación, usa la clave pública del usuario B para encriptar su propia clave privada (4), con el objetivo de que el usuario B pueda descifrar el mensaje encriptado. De esta forma, crea lo que se llama el "sobre" digital. Al final, el usuario A envía el mensaje firmado, encriptado con una clave privada, y un "sobre" con esta clave privada, que está encriptado con la clave pública del usuario B (5).

Una vez que el mensaje es recibido, el usuario B debe realizar el siguiente proceso (Fig. 3.9):

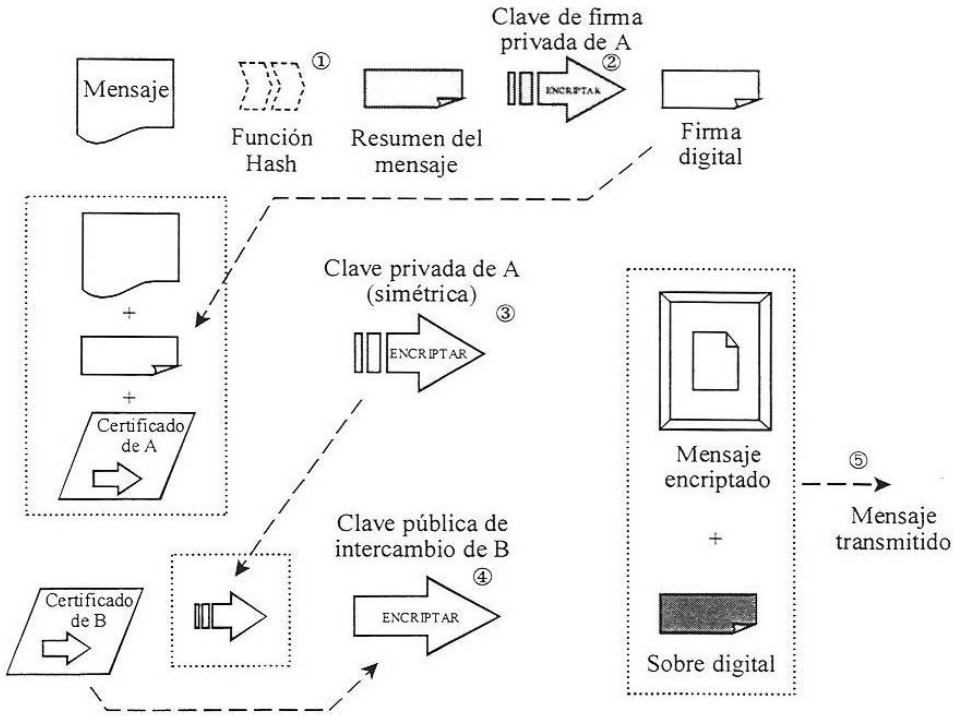

Fig. 3.8. Transmisión de un mensaje seguro entre dos usuarios: transmisión.

Primero, descifra la clave privada del usuario A, contenida en el "sobre" digital, con su propia clave privada (6). Con esta clave, descifra el mensaje encriptado con la clave privada del usuario A, obteniendo así el mensaje, la firma digital y el certificado (7). En este certificado esta contenida la clave pública del usuario A, con la cual se obtiene el "resumen" del mensaje creado por el usuario A (8). Aplicando la función Hash, el usuario B crea su propio resumen del mensaje (9), y lo compara con el resumen obtenido anteriormente. Si son iguales, el mensaje ha llegado íntegro al usuario B (10).

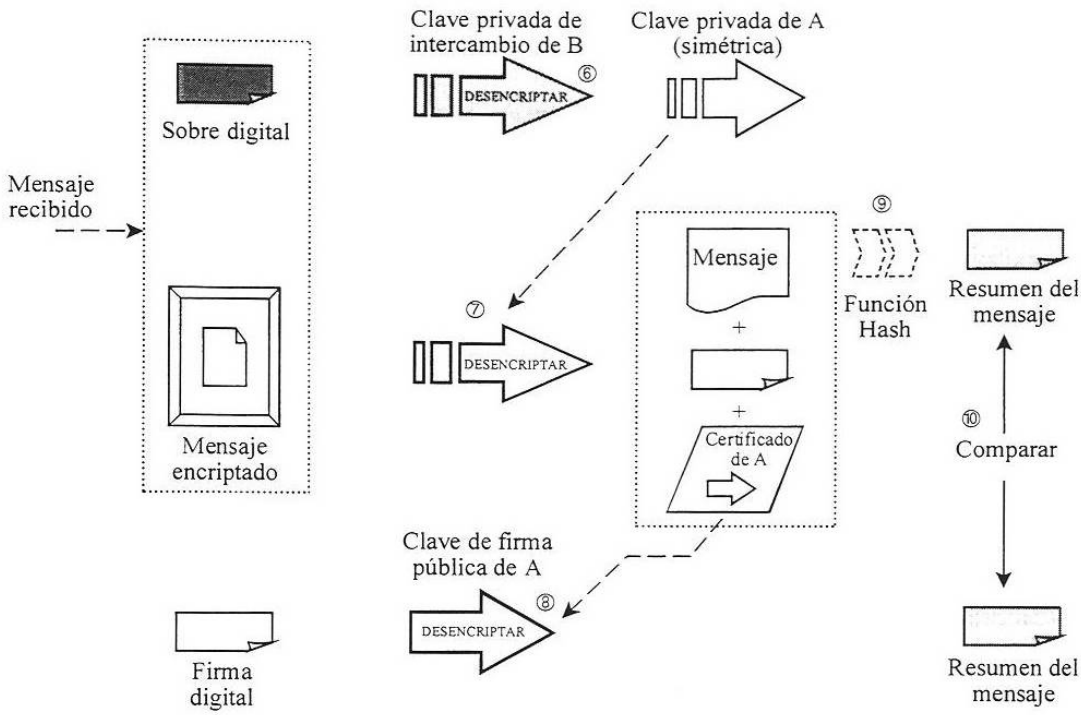

Fig. 3.9. Transmisión de un mensaje seguro entre dos usuarios: recepción.

Es importante señalar que estos sistemas de seguridad son confiables si son bien utilizados por los usuarios, ya que si no se comprueban los certificados digitales, o si no se toman las medidas correspondientes, el sistema completo es muy inseguro, razón que ha provocado la desconfianza que existe en las transacciones a través del Internet.

3.8 FIREWALL

Un firewall es un sistema o un grupo de sistemas que decide que servicios pueden ser accesados desde el exterior (Internet, en este caso) de una red

privada, por quienes pueden ser ejecutados estos servicios y también a que servicios tienen acceso los usuarios de la intranet hacia el exterior (Internet) [12,18]. Para realizar esta tarea, el firewall controla todo el tráfico entre las dos redes. Es importante no confundir la función de un firewall con un enrutador; en general un firewall no direcciona información (función que si realiza el enrutador), sino que solamente filtra información. Desde el punto de vista de política de seguridad, el firewall delimita el perímetro de defensa y seguridad de la organización (Fig. 3.10).

El diseño de un firewall, tiene que ser el producto de una organización consciente de los servicios que se necesitan, además hay que tener presente los puntos vulnerables de toda red, los servicios que dispone como públicos al exterior de ella (WWW, FTP, telnet, entre otros) y conexiones por módem (dial-in modem calling). Los firewalls son clasificados en tres principales categorías: a) packet filters, b) application-level gateways y c) proxy servers.

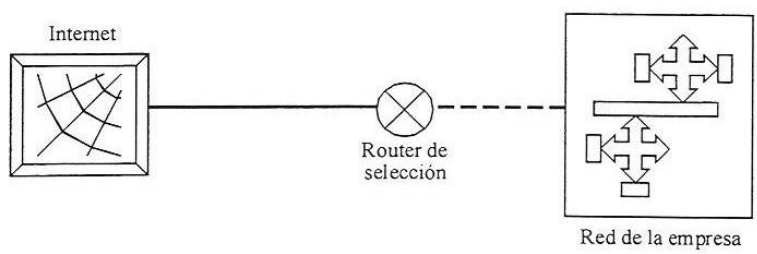

Fig. 3.10. Firewall.

3.8.1 Beneficios de un firewall

Una de las funciones de los firewalls es proteger los hosts de las redes de intranet contra accesos no autorizados desde hosts remotos en Internet. Esto significa que la seguridad de toda la red depende de que tan fácil fuera violar la seguridad local de cada máquina interna. De esta forma, el firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de acceso, que deben ser evaluados por el administrador de la red (Fig. 3.11 y 3.12).

Además de los aspectos de seguridad, el uso de los firewalls se ha extendido debido a la crisis de los últimos años en el número disponible de direcciones IP en Internet. Esto ha ocasionado que las intranets adopten direcciones CIRD (direcciones sin clase), las cuales se conectan a Internet por medio de un NAT (Network Address Traslator), que normalmente es alojado en el firewall. Los firewalls también han permitido generar estadísticas del ancho de banda "consumido" por el tráfico de la red, y determinar cuales procesos han influido más en ese tráfico; de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda.

Finalmente, los firewalls también son utilizados para albergar los servicios WWW y FTP de la intranet, ya que estos servicios se caracterizan por tener una interfaz al exterior de la red privada y se ha demostrado que son puntos vulnerables para acceder a ella.

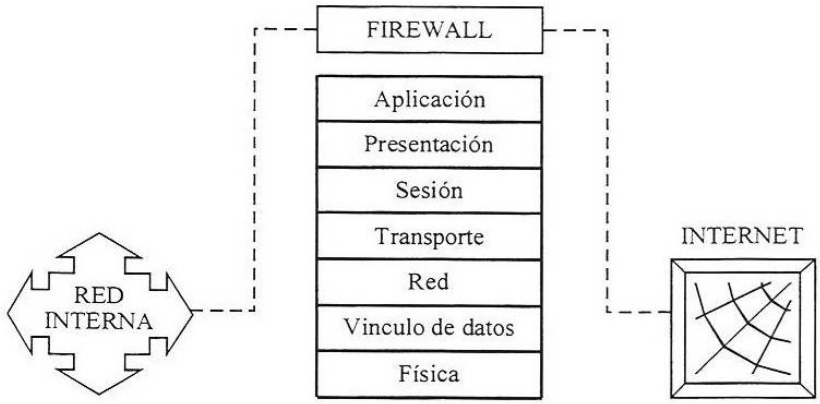

Fig. 3.11. Funciones de un firewall.

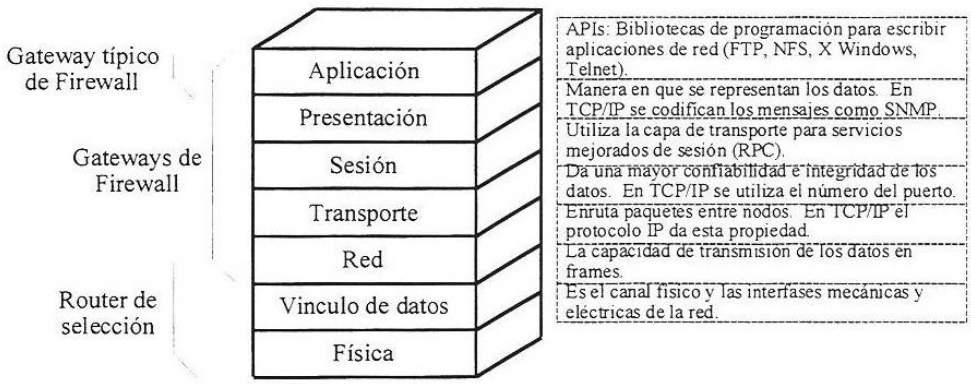

Fig. 3.12. Descripción de las funciones del Firewall.

3.8.2 Limitaciones del firewall

La principal limitación de un firewall son los accesos no cubiertos que permiten el acceso a la red de la organización. Los firewalls no son sistemas inteligentes, éstos operan de acuerdo a parámetros introducidos previamente definidos, por tanto, si un paquete de información no se encuentra dentro de estos parámetros

como una amenaza de peligro simplemente lo dejará pasar. En este sentido, un intruso que pueda tener acceso a la red, puede crear un acceso autorizado o "back door" que puede utilizar posteriormente para tener acceso ilimitado a la red de la organización (descubrir passwords, borra archivos, etc.) sin que el firewall lo detecte. Una situación similar ocurre con la filtración de software o archivos infectados con virus.

3.8.3 Decisiones de diseño básicas de un firewall

Existen ciertas consideraciones que se deben tomar en cuenta para implementar un firewall entre Internet y una intranet (red LAN). Algunas de estas consideraciones son:

Postura del firewall

- Todo lo que no es específicamente permitido se niega. Aunque es una postura radical es la más segura y la más fácil de implementar relativamente ya que no hay necesidad de crear accesos especiales a los servicios.
- Todo lo que no es específicamente negado se permite. Esta no es la postura ideal, por eso es más que todo usado para subdividir la intranet. No es recomendable para implementar entre una LAN e Internet, ya que es muy vulnerable.

Política de seguridad de la organización:

Depende de los servicios que ésta presta y del contexto en el cual está; no es lo mismo diseñar un firewall para una ISP o una Universidad que para proteger subdivisiones dentro de una empresa.

Costo del firewall:

El costo del firewall depende del número de servicios que se quieran filtrar y de la tecnología electrónica del mismo, además requiere de un soporte administrativo continuo, mantenimiento general, actualizaciones de software y actualizaciones de los códigos de seguridad.

Componentes de un firewall

Los componentes típicos de un firewall son (Fig. 3.12):

- Un enrutador que sirva única y exclusivamente de filtro de paquetes.
- Un servidor proxy o gateway a nivel de aplicación (debido al costo, se implementa en una máquina linux).
- El gateway a nivel de circuito.

3.9 ESTRATEGIAS DE SEGURIDAD

Antes de construir una barrera de protección, como preparación para conectar una red al Internet, es importante determinar los recursos de la red y los servicios a proteger. Una política de red es un documento que describe los asuntos de seguridad de red de una empresa u organización. Este documento se convierte en el primer paso para construir barreras de protección efectivas [26,27].

Una organización puede tener más de un servidor de información y cada uno contar con sus propias redes. Si los servidores están conectados por una red interna, la política de red deberá agrupar las metas de todos los servidores que estén interconectados. En este sentido, los recursos incluyen, pero no se limitan a los siguientes componentes:

- Estaciones de trabajo.
- Computadoras anfitrión y servidores.
- Dispositivos de interconexión: compuertas, enrutadores, puentes, repetidoras.
- Servidores de terminal.
- Software para red y aplicaciones.
- Cables de red.
- Información en archivos y bases de datos.

La política de seguridad debe tomar en cuenta la protección de estos recursos. El RFC 1244 discute la política de seguridad del sitio en detalle [28]. En general, la implementación de la política de seguridad involucra el análisis de los siguientes aspectos:

- ¿Qué recursos se quieren proteger?
- ¿De qué personas necesita proteger los recursos?
- ¿Qué tan reales son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?

Cada uno de estos aspectos determinará el tipo y severidad de la política de seguridad, la cual debe ser reevaluada periódicamente para verificar si los objetivos o circunstancias en la red han cambiado.

3.9.1 Análisis de riesgos

Al crear una política de seguridad, se debe saber cuáles recursos de la red vale la pena proteger, y entender que algunos son más importantes que otros. El análisis de riesgos implica determinar lo siguiente:

- ¿Qué necesita proteger?

- ¿De quién debe protegerlo?
- ¿Cómo protegerlo?

No se debe llegar a una situación donde se gaste más para proteger aquello que es menos valioso. En el análisis de riesgos es necesario determinar los siguientes factores:

- Estimación del riesgo de pérdida del recurso (R_i).
- Estimación de la importancia del recurso (W_i).

Es conveniente asignar un valor numérico a estos factores, de manera que sea factible realizar la cuantificación del riesgo de perder un recurso. Así, es posible calcular el riesgo general de los recursos de la red utilizando la siguiente fórmula:

$$WR = \frac{R_1W_1 + R_2W_2 + \ldots + R_nW_n}{W_1 + W_2 + \ldots + W_n}$$

donde n es el número total de recursos con que cuenta la red. Otros factores que debe considerar para el análisis de riesgo de un recurso de red son su disponibilidad, su integridad y su carácter confidencial.

El RFC 1244 lista los siguientes recursos de red que deben ser considerados al estimar las amenazas a la seguridad en la red:

- *Hardware:* procesadores, tarjetas, teclados, terminales, líneas de comunicación, enrutadores, etc.
- *Software:* programas fuente, programas objeto, utilerías, programas de comunicación, sistemas operativos, etc.
- *Datos:* durante la ejecución, almacenados en línea, bitácoras de auditoría, bases de datos, en tránsito sobre medios de comunicación, etc.
- *Gente:* usuarios, personas para operar sistemas.
- *Documentación:* sobre programas, hardware, sistemas, procedimientos administrativos locales.
- *Accesorios:* papel, formas, cintas, información grabada.

3.9.2 Aspectos de la implementación de una política de seguridad

Algunos de los aspectos más importantes para la implementación de una política de seguridad son los siguientes:

Identificación de usuarios

Debe hacerse una lista de los usuarios que requieren ingresar a los recursos de la red. La mayoría de los usuarios de la red se divide en grupos como usuarios

de cuenta, ejecutivos corporativos, ingenieros, etc. También se deberá incluir una clase de usuarios llamada usuarios externos. Estos son los usuarios que pueden tener acceso a la red desde cualquier parte, como las estaciones individuales de trabajo u otras redes.

Uso correcto de los recursos

El siguiente paso será el de proveer guías para el uso aceptable del recurso. Las guías dependerán de la clase de usuario y por consiguiente sus normas. La política debe establecer que tipos de uso de red es aceptable e inaceptable, y qué tipo de uso será restringido. La política que desarrolle se llamará política de uso aceptable (AUP) para la red. Si el acceso a un recurso se restringe, deberá considerar el nivel de acceso que tendrán las diferentes clases de usuarios.

Además, es necesario incorporar en la política restricciones concernientes al software con derechos de autor y con licencia. También se debe tener una política en la selección de una contraseña inicial de usuario. Por ejemplo, si la contraseña inicial es la misma que el nombre del usuario, se corre el riesgo de accesos no autorizados a las cuentas. También es necesario evitar que la contraseña inicial sea una función del nombre de usuario, o sea generada en forma de un algoritmo que pueda determinarse con facilidad.

Algunos usuarios utilizan su cuenta hasta mucho tiempo después de creada; otros nunca se registran. En estas circunstancias, si la contraseña inicial no es

segura, la cuenta y el sistema serán también vulnerables. Por tal razón se debe tener una política para inhabilitar total o parcialmente las cuentas que nunca se han introducido durante cierto tiempo. Si el sistema lo permite, deberá forzar a los usuarios a cambiar las contraseñas en el primer registro. Muchos sistemas tienen la política de caducidad de contraseña. Esto puede ser útil para proteger las contraseñas.

Responsabilidades de los usuarios

La siguiente es una lista de aspectos que definen las responsabilidades de cada uno de los usuarios de una red:

- Guías respecto al uso de recursos de red en caso de que los usuarios estén restringidos y cuáles son las restricciones.
- Restricciones en el uso de los recursos de red que afectan el desempeño del sistema y la red.
- Definición del uso de cuentas por parte de los usuarios.
- Definición de los procedimientos para el uso temporal de contraseñas de parte de usuarios no autorizados, que requieren acceso restringido cuando participan en proyectos.
- Definición de las políticas para la asignación de contraseñas a los usuarios.

- Asignación de responsabilidades durante los procedimientos de respaldo de información.
- Aspectos legales relacionados con la divulgación de información propietaria, y la privacidad del correo electrónico.
- Definición de una política sobre comunicaciones electrónicas, a fin de evitar problemas de seguridad como sería la falsificación de mensajes de correo.

Responsabilidades de los administradores del sistema

Cuando ocurren las amenazas a la seguridad de la red, el administrador del sistema podrá examinar los directorios y archivos privados del usuario para el diagnóstico del problema hasta cierto límite estipulado por la política del sistema o red.

Plan de acción cuando la política de seguridad ha sido violada

Si no ocurre un cambio en la seguridad de la red después de ser violada, entonces la política de seguridad deberá ser modificada para retirar aquellos elementos que no estén asegurados. Si la política de seguridad es demasiado restrictiva o no está bien explicada, es muy posible que sea violada.

Cuando se detecte una violación a la política de seguridad, se debe clasificar si la violación ocurrió por una negligencia del personal, por ignorancia de la política actual o ignorancia deliberada a la política, o es un accidente o error. En cada una de estas circunstancias, la política de seguridad debe ofrecer guías sobre las medidas a tomar de inmediato.

Estrategias de respuesta a violaciones

Hay dos tipos de estrategias de respuesta después de haberse detectado un incidente de seguridad:

- Proteger y proceder.
- Perseguir y procesar.

La metodología de la primera estrategia es proteger de manera inmediata la red y restaurarla a su estado normal para que los usuarios puedan seguir utilizandola. Para hacer esto, hay que interferir en forma activa con las acciones del intruso y evitar mayor acceso.

El segundo enfoque adopta la estrategia de que la mejor meta es permitir a los intrusos seguir con sus acciones mientras se observan sus actividades. Las actividades del intruso deberán registrarse. Una forma posible de vigilar a los intrusos sin causar daño al sistema es construir una "cárcel". Una cárcel, en

este caso, define un medio simulado con datos falsos para que lo utilice el intruso, para que sus actividades puedan ser observadas.

3.10 CONCLUSIONES DEL CAPÍTULO

Los mecanismos de seguridad deben satisfacer dos aspectos esenciales, mantener la privacidad de la información contenida en los servidores de una red, y tener el control de los accesos a la red para mantener la confidencialidad de los datos que se transmiten; en general, los esquemas de seguridad se han desarrollado en tres áreas, la protección de la transmisión de archivos a través de una red de comunicación, la protección de servidores conectados al Internet y la protección de redes privadas que se interconectan a través de redes públicas.