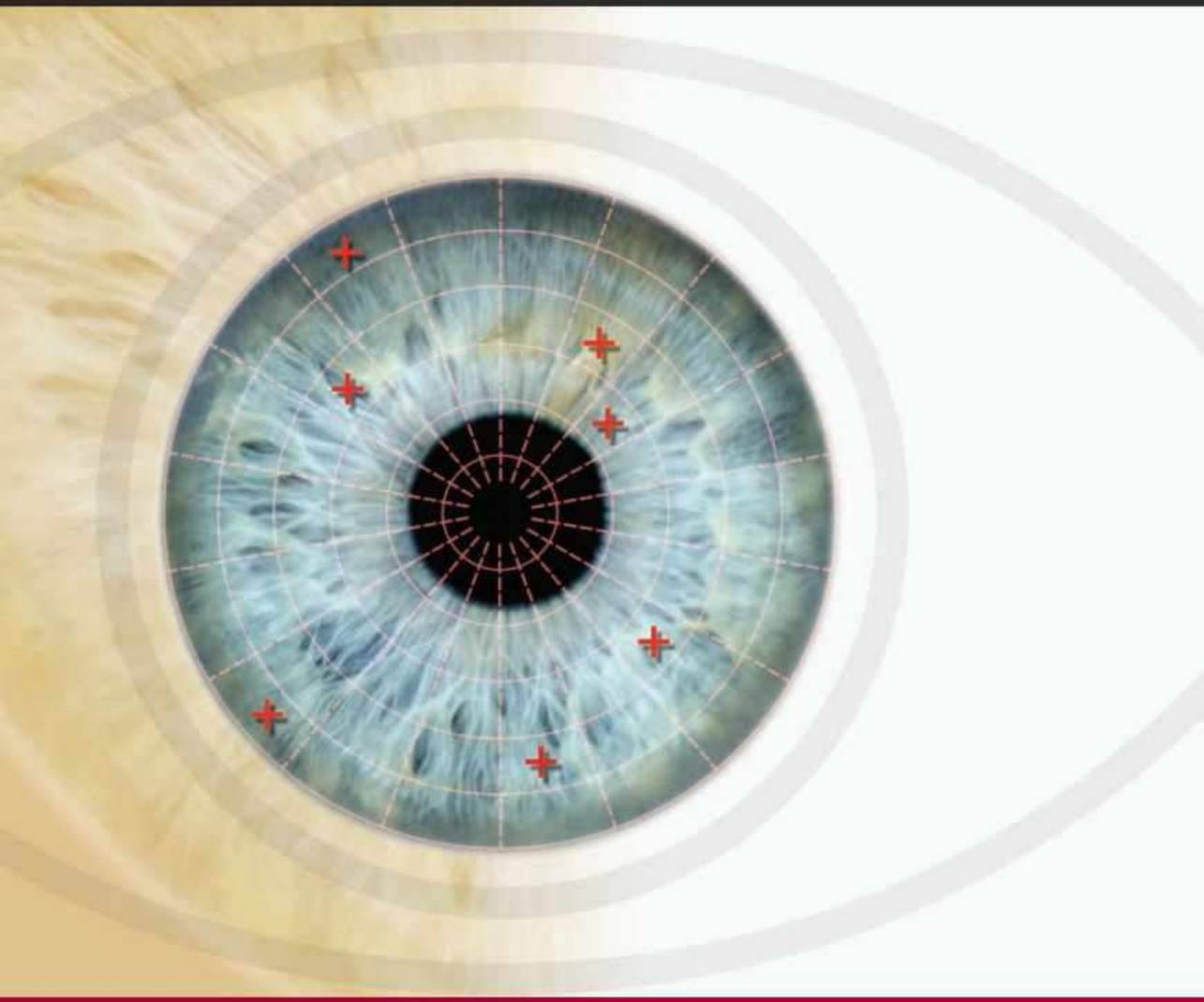
2ª Edición

Fundamentos de Seguridad en Redes

Aplicaciones y Estándares



PEARSON
Prentice Hall

William Stallings

FUNDAMENTOS DE SEGURIDAD EN REDES

APLICACIONES Y ESTÁNDARES

Segunda edición

FUNDAMENTOS DE SEGURIDAD EN REDES

APLICACIONES Y ESTÁNDARES

Segunda edición

William Stallings

Revisión técnica:

Manuel González Rodríguez
Facultad de Informática
Universidad de las Palmas de Gran Canaria

Luis Joyanes Aguilar
Universidad Pontificia de Salamanca, campus de Madrid

Traducción:

Laura Cruz García
Facultad de Informática
Universidad de Las Palmas de Gran Canaria

Manuel González Rodríguez
Facultad de Informática
Universidad de las Palmas de Gran Canaria

Madrid • México • Santafé de Bogotá • Buenos Aires • Caracas • Lima • Montevideo
San Juan • San José • Santiago • São Paulo • White Plains

Datos de catalogación bibliográfica

STALLINGS, W.
FUNDAMENTOS DE SEGURIDAD EN REDES. APLICACIONES Y ESTÁNDARES.
Segunda edición

PEARSON EDUCACIÓN, S.A., Madrid, 2004

ISBN: 84-205-4002-1
Materia: Informática 681.3

Formato: 170 × 240 Páginas: 432

FUNDAMENTOS DE SEGURIDAD EN REDES. APLICACIONES Y ESTÁNDARES. Segunda edición
STALLINGS, W.

ISBN: 84-205-4002-1
Depósito Legal: M-

PEARSON PRENTICE HALL es un sello editorial autorizado de PEARSON EDUCA CIÓN, S. A.

Traducido de:
Network Security Essentials. Applications and Standars. Second edition, by Stallings, William.
Published by Pearson Education, Inc., publishing as Prentice Hall.

Equipo editorial:
Director: David Fayerman Aragón
Técnico editorial: Ana Isabel García Borro
Equipo de producción:
Director: José Antonio Clares
Técnico: José Antonio Hernán
Diseño de cubierta: Equipo de diseño de Pearson Educación, S.A.
Composición: Claroscuro Servicio Gráfico, S.L.
Impreso por:

IMPRESO EN ESPAÑA - PRINTED IN SPAIN

Este libro ha sido impreso con papel y tintas ecológicos

Contenido

SEGUNDA PARTE
Aplicaciones de seguridad en redes

TERCERA PARTE
Seguridad de los sistemas

Prólogo

«La corbata, si me permite la sugerencia, señor, lleva el nudo más apretado. Se persigue el efecto mariposa perfecto. ¿Me permite?»

«¿Qué importa, Jeeves, en un momento como éste? ¿Es que no ves cómo se tambalea la felicidad doméstica de Mr. Little?»

«Señor, no hay momento en el que las corbatas no importen.»

***¡Muy bien, Jeeves!* P. G. Wodehouse**

En esta era de la conectividad electrónica universal, de virus y hackers, de escuchas y fraudes electrónicos, no hay un momento en el que no importe la seguridad. Dos tendencias han confluido para hacer de interés vital el tema de este libro. En primer lugar, el enorme crecimiento de los sistemas de computadores y sus interconexiones mediante redes ha hecho que organizaciones e individuos dependan cada vez más de la información que se almacena y se transmite a través de estos sistemas. Esto, a su vez, ha llevado a un aumento de la conciencia de la necesidad de proteger los datos y los recursos, de garantizar la autenticidad de los datos y los mensajes y de proteger los sistemas frente a ataques a la red. En segundo lugar, las disciplinas de la criptografía y la seguridad de la red han madurado, dando como resultado el desarrollo de aplicaciones prácticas, ya disponibles, para la seguridad de la red.

OBJETIVOS

El propósito de este libro es proporcionar un estudio práctico sobre las aplicaciones y los estándares relativos a la seguridad de la red. Se resaltan, por una parte, las aplicaciones que más se utilizan en Internet y en las redes corporativas y, por otra, los estándares más extendidos, especialmente los de Internet.

DESTINATARIOS

El libro está destinado a una audiencia tanto académica como profesional. Como libro de texto, está diseñado para cubrir un curso de un semestre sobre seguridad en redes para estudiantes universitarios de ciencias de la computación, ingeniería de la computación e ingeniería eléctrica. También sirve como libro básico de referencia y es adecuado para el aprendizaje autónomo.

ORGANIZACIÓN DEL LIBRO

El libro se divide en tres partes:

Primera parte. Criptografía: consiste en un estudio conciso de los algoritmos y protocolos criptográficos que subyacen a las aplicaciones de seguridad en la red, incluyendo el cifrado, las funciones *hash*, las firmas digitales y el intercambio de claves.

Segunda parte. Aplicaciones de seguridad en redes: cubre herramientas y aplicaciones importantes de seguridad en la red, incluyendo Kerberos, los certificados X.509v3, PGP, S/MIME, seguridad IP, SSL/TLS, SET y SNMPv3.

Tercera parte. Seguridad de los sistemas: observa los aspectos de seguridad en el ámbito de los sistemas, que incluyen las amenazas de intrusos y virus y sus contramedidas, y el uso de cortafuegos y sistemas confiables.

Además, el libro incluye un Glosario extenso, una lista de Acrónimos frecuentes y una Bibliografía. Cada capítulo ofrece problemas, preguntas de repaso, una lista de palabras que hacen referencia a conceptos fundamentales, así como lecturas y sitios web recomendados.

Al principio de cada una de las partes del libro se presenta un resumen más detallado de cada capítulo.

SERVICIOS DE INTERNET PARA DOCENTES Y ESTUDIANTES

Existe una página web para este libro que proporciona apoyo a los estudiantes y a los docentes. La página incluye enlaces a sitios relevantes, las transparencias en formato PDF (Adobe Acrobat) de las figuras y tablas que se muestran en el libro e información para registrarse en la lista de correo de Internet de este libro. La dirección de la página web es WilliamStallings.com/NetSec2e.html. Además, se ha creado una lista de correo para que los docentes que utilicen este libro puedan intercambiar, entre ellos y con el autor, información, sugerencias y preguntas. En WilliamStallings.com se dispone de una lista de erratas para incluir aquellos errores tipográficos o de cualquier otra índole que se detecten. También, la página *Computer Science Student Resource* (recursos para estudiantes de ciencias de la computación), en WilliamStallings.com/StudentSupport.html, proporciona documentos, información y enlaces útiles para estudiantes y profesionales.

PROYECTOS PARA LA ENSEÑANZA DE LA SEGURIDAD EN LA RED

Para muchos docentes, una parte importante de un curso sobre criptografía o seguridad lo constituye un proyecto o conjunto de proyectos mediante los cuales los estudiantes puedan realizar actividades experimentales para reforzar los conceptos del libro. Este libro proporciona un grado incomparable de apoyo para incluir un componente de proyectos en el curso. El manual del docente no sólo aporta una guía sobre cómo asignar y estructurar los proyectos, sino que también incluye una serie de propuestas de proyectos que cubren una amplia gama de temas que trata el texto:

- **Proyectos de investigación:** una serie de ejercicios de investigación que instruyen al alumno para investigar un tema en particular sobre Internet y escribir un informe.
- **Proyectos de programación:** una serie de proyectos de programación que cubren un amplio abanico de temas y que se pueden implementar en un lenguaje adecuado en una plataforma.
- **Ejercicios de lectura y redacción de informes:** una lista de artículos sobre el tema, uno para cada capítulo, que se pueden asignar para que los estudiantes los lean y después escriban un breve informe.

Véase Apéndice B.

RELACIÓN CON *CRYPTOGRAPHY AND NETWORK SECURITY*, TERCERA EDICIÓN

Este libro es un producto derivado de *Cryptography and Network Security,* Tercera Edición. Dicha obra proporciona un tratamiento sustancial de la criptografía, incluyendo, en 400 páginas, un análisis detallado de los algoritmos y el componente matemático significativos. *Fundamentos de Seguridad en Redes de Computadores: Aplicaciones y Estándares* ofrece una introducción concisa de estos temas en los Capítulos 2 y 3. También incluye todo el material restante del otro libro. Además, cubre la seguridad SNMP, que también se trata en *Cryptography and Network Security.* Así, este libro está diseñado para universitarios y para profesionales con un interés especial en la seguridad de la red, sin la necesidad o el deseo de ahondar en la teoría y los principios de la criptografía.

CAPÍTULO 1

Introducción

La combinación de espacio, tiempo y fuerza, que deben considerarse como los elementos básicos de esta teoría de la defensa, hace de ésta una cuestión complicada. Por consiguiente, no es fácil encontrar un punto fijo de partida.

***De la guerra*, CARL VON CLAUSEWITZ**

El arte de la guerra nos enseña a confiar no en la posibilidad de que el enemigo no venga, sino en nuestra propia disponibilidad para recibirlo; no en la oportunidad de que no ataque, sino en el hecho de que hemos logrado que nuestra posición sea inexpugnable.

***El arte de la guerra*, SUN TZU**

Las necesidades de **seguridad de la información** en una organización han sufrido dos cambios fundamentales en las últimas décadas. Antes de la expansión del uso de equipamiento de procesamiento de datos, la seguridad de la información que una organización consideraba valiosa se proporcionaba, por un lado, por medios físicos, como el uso de armarios con cierre de seguridad para almacenar documentos confidenciales y, por otro, por medios administrativos, como los procedimientos de protección de datos del personal que se usan durante el proceso de contratación.

Con la introducción del computador, se hizo evidente la necesidad de disponer de herramientas automatizadas para la protección de archivos y otros tipos de información almacenada en el computador. Esto ocurre especialmente en el caso de sistemas compartidos como, por ejemplo, un sistema de tiempo compartido; y la necesidad se acentúa en sistemas a los que se puede acceder por medio de una red telefónica pública, una red de datos o Internet. El nombre genérico que se da al grupo de herramientas diseñadas para proteger los datos y evitar la intrusión de los *hackers* es el de **seguridad informática**.

El segundo cambio que afectó a la seguridad fue la introducción de sistemas distribuidos y el uso de redes y herramientas de comunicación para transportar datos entre el usuario de un terminal y el computador, y entre dos computadores. Las medidas de seguridad de la red son necesarias para proteger los datos durante la transmisión. De hecho, el término **seguridad de la red** es engañoso, en cierto modo, ya que prácticamente todas las empresas, las instituciones gubernamentales y académicas conectan sus equipos de procesamiento de datos formando un grupo de redes conectadas entre sí. Este grupo se considera con frecuencia como una internet[1], y se emplea el término **seguridad de la internet**.

No existen unas fronteras bien delimitadas entre estas dos formas de seguridad. Por ejemplo, uno de los tipos de ataque a los sistemas de información a los que más publicidad se ha dado es el virus informático. Un virus se puede introducir físicamente en un sistema por medio de un disquete o llegar por una internet. En cualquier caso, una vez que el virus reside en un sistema informático, se necesitan las herramientas internas de seguridad del computador para detectarlo, eliminarlo y restablecer el sistema.

[1] Usamos el término *internet*, con «i» minúscula, para referirnos a cualquier grupo de redes conectadas entre sí. Una intranet corporativa es un ejemplo de internet. Internet con «I» mayúscula pude ser una de las herramientas que usa una organización para construir su internet.

Este libro se centra en la seguridad de la internet, que consiste en las medidas para impedir, prevenir, detectar y corregir las violaciones de la seguridad que se producen durante la transmisión de la información. Esta es una afirmación muy general que abarca una gran cantidad de posibilidades. Para que el lector se haga una idea de las áreas que trata este libro, considere los siguientes ejemplos de violaciones de la seguridad:

1. El usuario A envía un archivo al usuario B. El archivo contiene información confidencial que debe protegerse (por ejemplo, registros de nóminas). El usuario C, que no está autorizado a leer el archivo, observa la transmisión y captura una copia del archivo durante dicha transmisión.
2. Un administrador de red, D, transmite un mensaje a un computador, E, que se encuentra bajo su gestión. El mensaje ordena al computador E que actualice un fichero de autorización para incluir las identidades de nuevos usuarios a los que se va a proporcionar el acceso a ese computador. El usuario F intercepta el mensaje, altera su contenido añadiendo o borrando entradas y, posteriormente, lo envía a E, que lo acepta como si procediera del administrador D y, por tanto, actualiza su archivo de autorización.
3. Más allá de interceptar un mensaje, el usuario F construye su propio mensaje con las entradas deseadas y lo transmite a E como si procediera del administrador D. Por consiguiente, el computador E acepta el mensaje y actualiza su fichero de autorización sin percatarse de la intrusión.
4. Un empleado es despedido sin previo aviso. El jefe de personal envía un mensaje a un sistema servidor para invalidar la cuenta del empleado. Cuando la invalidación se ha llevado a cabo, el servidor ha de notificar la confirmación de la acción al archivo del empleado. El empleado intercepta el mensaje y lo retrasa el tiempo suficiente para realizar un último acceso al servidor y recuperar, así, información confidencial. A continuación, se envía el mensaje, se lleva a cabo la acción y se notifica la confirmación. La acción del empleado puede pasar inadvertida durante un período de tiempo considerable.
5. Un cliente envía un mensaje a un corredor de bolsa con instrucciones para realizar diferentes transacciones. Más tarde, las inversiones pierden valor y el cliente niega haber enviado dicho mensaje.

Aunque, de ningún modo, esta lista abarca todos los tipos posibles de violaciones de la seguridad, ilustra una serie de aspectos que afectan a la seguridad de la red.

La seguridad de la red se presenta como un tema fascinante a la vez que complejo. A continuación se exponen algunas de las razones:

1. La seguridad relativa a las comunicaciones y a las redes no es tan simple como podría parecer a los principiantes en este tema. Los requisitos parecen claros; de hecho, a la mayoría de los requisitos fundamentales que deben cumplir los servicios de seguridad se les puede asignar etiquetas de una sola palabra que se explican por sí mismas: confidencialidad, autentificación, no repudio, integridad. Pero los mecanismos empleados para satisfacer estos requisitos pueden ser muy complejos, y comprenderlos puede implicar un razonamiento un tanto sutil.
2. En el desarrollo de un mecanismo particular de seguridad o algoritmo, siempre se deben tener en cuenta los posibles ataques a esas características de seguridad.

En muchos casos, los ataques con éxito están diseñados analizando el problema de una forma totalmente diferente, explotando, por lo tanto, una debilidad inadvertida del mecanismo.

3. Como consecuencia del punto 2, los procedimientos empleados para proporcionar servicios particulares no suelen ser intuitivos; es decir, a partir de la afirmación de un requisito particular no es obvio que sean necesarias medidas tan elaboradas. Las medidas empleadas sólo cobran sentido cuando se han considerado las diferentes contramedidas.

4. Después de diseñar distintos mecanismos de seguridad, es necesario decidir dónde usarlos, tanto en lo que respecta a la ubicación física (por ejemplo, en qué puntos de una red se necesitan determinados mecanismos de seguridad) como a la ubicación lógica [en qué capa o capas de una arquitectura como la TCP/IP (Transmission Control Protocol / Internet Protocol) deberían estar localizados los mecanismos].

5. Los mecanismos de seguridad suelen implicar más de un algoritmo o protocolo. Con frecuencia también requieren que los participantes posean alguna información secreta (que podría ser una clave de cifrado), lo que da lugar a cuestiones sobre la creación, distribución y protección de esa información secreta. También hay una dependencia de los protocolos de comunicación cuyo comportamiento puede complicar la tarea de desarrollar mecanismos de seguridad. Por ejemplo, si el funcionamiento adecuado del mecanismo de seguridad requiere establecer unos límites de tiempo para la transmisión de un mensaje desde el emisor hasta el receptor, cualquier protocolo o red que introduzca retrasos variables e impredecibles podría hacer que estos límites temporales carecieran de sentido.

Por lo tanto, son muchas las cuestiones que han de tenerse en cuenta. Este Capítulo proporciona una visión general del tema, que se irá desarrollando a lo largo del libro. Empezaremos con una discusión general sobre los servicios y mecanismos de seguridad en las redes y los tipos de ataques para los que están diseñados. A continuación, desarrollaremos un modelo general en el que se podrán observar los distintos servicios y mecanismos de seguridad.

1.1 LA ARQUITECTURA DE SEGURIDAD OSI

Para analizar de forma efectiva las necesidades de seguridad de una organización y evaluar y elegir distintos productos y políticas de seguridad, el responsable de la seguridad necesita una forma sistemática de definir los requisitos de seguridad y caracterizar los enfoques para satisfacer dichos requisitos. Esto es bastante difícil en un entorno centralizado de procesamiento de datos, y con el uso de redes de área local y de área ancha, los problemas se agravan.

La recomendación X.800 de la ITU-T[2], *Arquitectura de seguridad OSI*, define este enfoque sistemático. La arquitectura de seguridad OSI es útil a los administradores de

[2] El Sector de Estandarización de Telecomunicaciones (ITU-T) de la Unión Internacional de Telecomunicaciones (ITU) es una agencia financiada por las Naciones Unidas que desarrolla estándares, denominados Recomendaciones, relativos a las telecomunicaciones y a la interconexión de sistemas abiertos (OSI).

red para organizar la tarea de proporcionar seguridad. Además, debido a que esta arquitectura fue desarrollada como un estándar internacional, los vendedores han desarrollado características de seguridad para sus productos y servicios conforme a esta definición estructurada de servicios y mecanismos.

Para nuestros propósitos, la arquitectura de seguridad OSI proporciona una visión general útil, aunque abstracta, de muchos de los conceptos que se tratan en este libro. La arquitectura de seguridad OSI se centra en los ataques a la seguridad, los mecanismos y los servicios, que se definen brevemente a continuación:

Tabla 1.1 Amenazas y ataques (RFC 2828)

Amenaza
Una posibilidad de violación de la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicio. Es decir, una amenaza es un peligro posible que podría explotar una vulnerabilidad.
Ataque
Un asalto a la seguridad del sistema derivado de una amenaza inteligente; es decir, un acto inteligente y deliberado (especialmente en el sentido de método o técnica) para eludir los servicios de seguridad y violar la política de seguridad de un sistema.

- **Ataque a la seguridad:** cualquier acción que comprometa la seguridad de la información de una organización.
- **Mecanismo de seguridad:** un mecanismo diseñado para detectar un ataque a la seguridad, prevenirlo o restablecerse de él.
- **Servicio de seguridad:** un servicio que mejora la seguridad de los sistemas de procesamiento de datos y la transferencia de información de una organización. Los servicios están diseñados para contrarrestar los ataques a la seguridad, y hacen uso de uno o más mecanismos para proporcionar el servicio.

En la literatura al respecto, los términos *amenaza* y *ataque* se usan frecuentemente para referirse más o menos a lo mismo. La Tabla 1.1 proporciona las definiciones extraídas de RFC 2828, *Internet Security Glossary.*

1.2 ATAQUES A LA SEGURIDAD

Una forma útil de clasificar los ataques a la seguridad, empleada en la recomendación X.800 y RFC 2828, es la distinción entre *ataques pasivos* y *ataques activos*. Un ataque pasivo intenta conocer o hacer uso de información del sistema, pero no afecta a los recursos del mismo. Un ataque activo, por el contrario, intenta alterar los recursos del sistema o afectar a su funcionamiento.

ATAQUES PASIVOS

Los ataques pasivos se dan en forma de escucha o de observación no autorizadas de las transmisiones. El objetivo del oponente es obtener información que se esté transmitiendo. Dos tipos de ataques pasivos son la obtención de contenidos de mensajes y el análisis del tráfico.

La **obtención de contenidos de mensajes** se entiende fácilmente. (Figura 1.1a). Una conversación telefónica, un mensaje por correo electrónico y un fichero enviado pueden contener información confidencial. Queremos evitar que un oponente conozca los contenidos de estas transmisiones.

(a) Obtención del contenido del mensaje

(b) Análisis del tráfico

Figura 1.1 Ataques pasivos

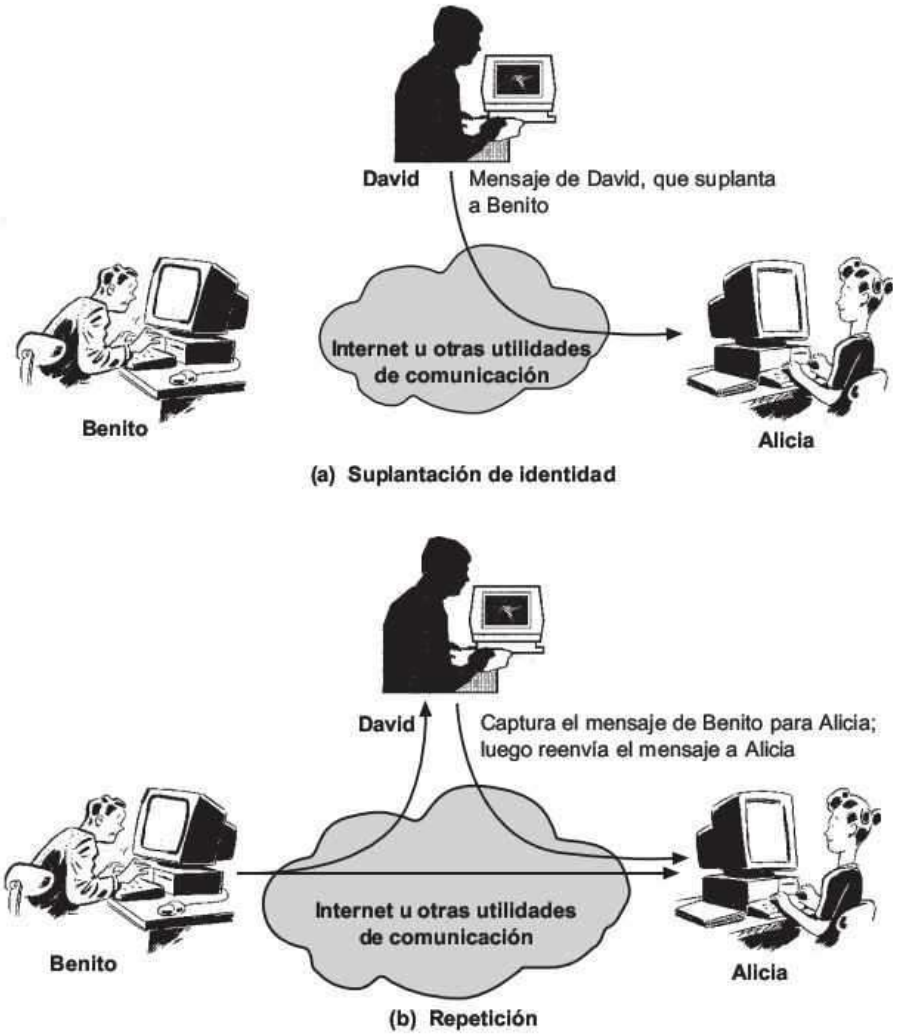


Figura 1.2 Ataques activos

Un segundo tipo de ataque pasivo, el **análisis de tráfico**, es más sutil (Figura 1.1b). Supongamos que hemos enmascarado los contenidos de los mensajes u otro tráfico de información de forma que el oponente, incluso habiendo capturado el mensaje, no pueda extraer la información que contiene. La técnica común para enmascarar los contenidos es el cifrado. Incluso si tuviésemos protección mediante cifrado, un oponente podría observar el patrón de los mensajes, determinar la localización y la identidad de los servidores que se comunican y descubrir la frecuencia y la longitud de los mensajes que se están intercambiando. Esta información puede ser útil para averiguar la naturaleza de la comunicación que está teniendo lugar.

Los ataques pasivos son muy difíciles de detectar ya que no implican alteraciones en los datos. Normalmente, el mensaje se envía y se recibe de una forma aparentemente

normal y ni el emisor ni el receptor son conscientes de que una tercera persona ha leído los mensajes o ha observado el **patrón del tráfico**. Sin embargo, es posible evitar el éxito de estos ataques, normalmente mediante el uso del cifrado. Así, al tratar con los ataques pasivos, el énfasis se pone más en la prevención que en la detección.

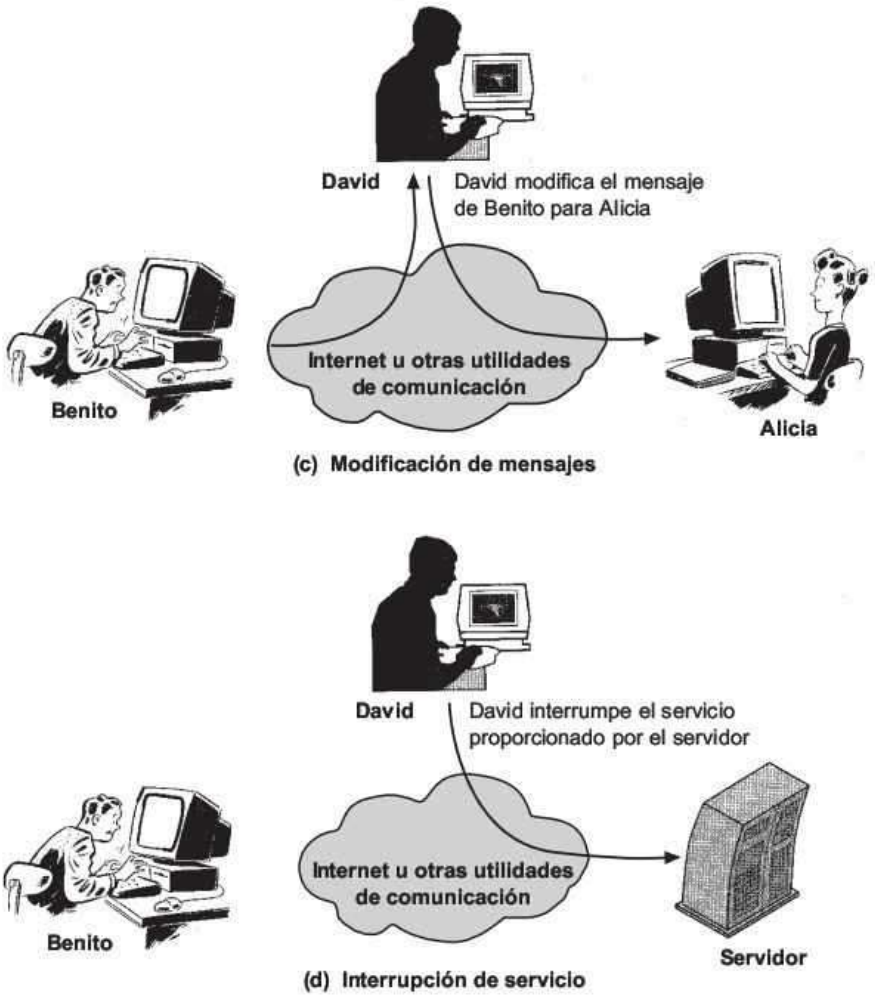


Figura 1.2 Ataques activos *(continuación)*

ATAQUES ACTIVOS

Los ataques activos implican alguna modificación del flujo de datos o la creación de un flujo falso y se pueden dividir en cuatro categorías: suplantación de identidad, repetición, modificación de mensajes e interrupción de servicio.

Una **suplantación** se produce cuando una entidad finge ser otra (Figura 1.2a). Un ataque de este tipo incluye habitualmente una de las otras formas de ataque activo. Por

ejemplo, las secuencias de autentificación pueden ser capturadas y repetidas después de que una secuencia válida de autentificación haya tenido lugar, permitiendo así, que una entidad autorizada con pocos privilegios obtenga privilegios extra haciéndose pasar por la entidad que realmente los posee.

La repetición implica la captura pasiva de una unidad de datos y su retransmisión posterior para producir un efecto no autorizado (Figura 1.2b).

La **modificación de mensajes** significa que una parte de un mensaje original es alterada, o que los mensajes se han retrasado o reordenado, para producir un efecto no autorizado (Figura 1.2c). Por ejemplo, el mensaje «Permitir a Carlos Pérez que lea las cuentas de archivos confidenciales» se modifica para convertirlo en «Permitir a Marcos Fernández que lea las cuentas de archivos confidenciales».

La **interrupción de servicio** impide el uso o la gestión normal de las utilidades de comunicación (Figura 1.2d). Este ataque podría tener un objetivo específico; por ejemplo, una entidad podría suprimir todos los mensajes dirigidos a un destino en particular (por ejemplo, el servicio de auditoría de la seguridad). Otra forma de este tipo de ataque es la interrupción de una red completa, ya sea inhabilitándola o sobrecargándola con mensajes para reducir su rendimiento.

Los ataques activos presentan las características opuestas a los pasivos. Aunque los ataques pasivos son difíciles de detectar, existen medidas para prevenir su éxito. Sin embargo, es bastante difícil prevenir por completo los ataques activos, debido a que se requeriría la protección física de todas las herramientas de comunicación y las rutas en todo momento. Por el contrario, el objetivo es el de detectarlos y recuperarse de cualquier irrupción o retraso que originen. Como la detección tiene un efecto disuasivo, también podría contribuir a la prevención.

1.3 SERVICIOS DE SEGURIDAD

La recomendación X.800 define un servicio de seguridad como un servicio proporcionado por una capa de protocolo de sistemas abiertos de comunicación, que garantiza la seguridad adecuada de los sistemas o de las transferencias de datos. Quizás es más clara la definición recogida en RFC 2828: un servicio de procesamiento o de comunicación proporcionado por un sistema para dar un tipo especial de protección a los recursos del sistema; los servicios de seguridad implementan políticas de seguridad y son implementados, a su vez, por mecanismos de seguridad.

En X.800 estos servicios quedan divididos en cinco categorías y 14 servicios específicos (Tabla 1.2). Observemos a continuación cada una de las categorías[3].

[3] No existe un acuerdo universal sobre la gran cantidad de términos que se emplean en la literatura sobre seguridad. Por ejemplo, el término *integridad* se usa a veces para referirse a todos los aspectos de la seguridad de la información. El término *autentificación* se usa con frecuencia para hacer alusión tanto a la verificación de la identidad como a las diferentes funciones que aparecen referidas a integridad en este Capítulo. Nuestro uso aquí está de acuerdo con las normas X.800 y RFC 2828.

Tabla 1.2 Servicios de seguridad (X.800)

AUTENTIFICACIÓN

La seguridad de que la entidad que se comunica es quien dice ser.

Autentificación de las entidades origen/destino

Empleada conjuntamente con una conexión lógica para aportar confianza sobre la identidad de las entidades conectadas.

Autentificación del origen de los datos

En transferencias no orientadas a la conexión, garantiza que la fuente de los datos recibidos es la que dice ser.

CONTROL DE ACCESO

La prevención del uso no autorizado de una fuente (este servicio controla quién puede tener acceso a una fuente, en qué condiciones se puede producir el acceso y qué tienen permitido los que acceden a la fuente).

CONFIDENCIALIDAD DE LOS DATOS

La protección de los datos contra la revelación no autorizada.

Confidencialidad de la conexión

La protección de los datos de todos los usuarios en una conexión.

Confidencialidad no orientada a la conexión

La protección de los datos de todos los usuarios en un único bloque de datos.

Confidencialidad de campos seleccionados

La confidencialidad de campos seleccionados en los datos del usuario en una conexión o en un único bloque de datos.

Confidencialidad del flujo de tráfico

La protección de la información que podría extraerse a partir de la observación del flujo del tráfico.

INTEGRIDAD DE LOS DATOS

La seguridad de que los datos recibidos son exactamente como los envió una entidad autorizada (no contienen modificación, inserción, omisión, ni repetición).

Integridad de la conexión con recuperación

Proporciona la integridad de los datos de todos los usuarios en una conexión y detecta cualquier modificación, inserción, omisión o repetición de cualquier dato de una secuencia completa de datos, con intento de recuperación.

Integridad de la conexión sin recuperación

Igual que el anterior, pero proporciona sólo detección sin recuperación.

Integridad de la conexión de campos seleccionados

Proporciona la integridad de los campos seleccionados en los datos del usuario del bloque de datos transferido por una conexión y determina si los campos seleccionados han sido modificados, insertados, suprimidos o repetidos.

Integridad no orientada a la conexión

Proporciona integridad de un bloque de datos sin conexión y puede detectar la alteración de datos. Además, puede proporcionar una forma limitada de detección de repetición.

Integridad no orientada a la conexión de campos seleccionados

Proporciona la integridad de los campos seleccionados en un bloque de datos sin conexión; determina si los campos seleccionados han sido modificados.

NO REPUDIO

Proporciona protección contra la interrupción, por parte de una de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación.

No repudio, origen

Prueba que el mensaje fue enviado por la parte especificada.

No repudio, destino

Prueba que el mensaje fue recibido por la parte especificada.

AUTENTIFICACIÓN

El servicio de autentificación se encarga de garantizar la autenticidad de la comunicación. En el caso de un único mensaje como, por ejemplo, una señal de aviso o de alarma, la función del servicio de autentificación es asegurar al receptor que el mensaje pertenece a la fuente de la que dice proceder. En el caso de una interacción continuada como la conexión de un terminal a un *host,* intervienen dos aspectos. En primer lugar, en el inicio de la conexión, el servicio asegura que las dos entidades son auténticas; es decir, cada entidad es la que dice ser. En segundo lugar, el servicio debe asegurar que la conexión no está intervenida de forma que una tercera persona pueda suplantar a una de las dos partes auténticas con la finalidad de realizar una transmisión o una recepción no autorizada.

En el estándar X.800 se definen dos tipos particulares de autentificación:

- **Autentificación de entidades origen/destino:** proporciona la confirmación de la identidad de una entidad de una asociación. Se proporciona en el establecimiento de una conexión o a veces durante la fase de transmisión de datos de dicha conexión. Intenta asegurar que una entidad no está realizando una suplantación o una repetición no autorizada de una conexión anterior.
- **Autentificación del origen de los datos:** corrobora la fuente de una unidad de datos. No aporta protección contra la repetición o la alteración de unidades de datos. Este tipo de servicio admite aplicaciones como el correo electrónico, donde no hay interacciones previas entre las entidades que se comunican.

CONTROL DE ACCESO

En el contexto de la seguridad de redes, el control de acceso es la capacidad de limitar y controlar el acceso a sistemas *host* y aplicaciones por medio de enlaces de comunicaciones. Para conseguirlo, cualquier entidad que intente acceder debe antes ser identificada o autentificada, de forma que los derechos de acceso puedan adaptarse de manera individual.

CONFIDENCIALIDAD DE LOS DATOS

La confidencialidad es la protección de los datos transmitidos por medio de ataques pasivos. En función del contenido de una transmisión de datos, existen diferentes niveles de protección. El servicio más amplio protege los datos de los usuarios que se han transmitido por conexión TCP. Se pueden distinguir formas más específicas de este servicio, incluyendo la protección de un solo mensaje o incluso de determinados campos de un mensaje. Estos refinamientos son menos útiles que el enfoque amplio y su implementación puede incluso ser más compleja y costosa.

El otro aspecto de la confidencialidad es la protección del flujo del tráfico frente al análisis del tráfico. Para ello el atacante no debería poder ver la fuente, el destino, la frecuencia, la longitud ni otras características del tráfico en una comunicación.

INTEGRIDAD DE LOS DATOS

Al igual que ocurre con la confidencialidad, la integridad se puede aplicar a una serie de mensajes, a un solo mensaje o a campos seleccionados de un mensaje. Nuevamente, el enfoque más útil y claro es la protección del flujo completo.

Un servicio de integridad orientado a la conexión que funcione sobre un flujo de mensajes garantiza que los mensajes se reciben tal y como son enviados, sin duplicación, inserción, modificación, reordenación ni repeticiones. La destrucción de datos también queda cubierta con este servicio. Así, el servicio de integridad orientado a la conexión trata tanto la modificación del flujo de mensajes como la interrupción del servicio. Por otra parte, un servicio de integridad sin conexión, que trata únicamente mensajes individuales sin tener en cuenta contextos mayores, sólo proporciona, generalmente, protección contra la modificación del mensaje.

Podemos distinguir entre el servicio con y sin recuperación. Debido a que el servicio de integridad tiene que ver con ataques activos, nos interesa más la detección que la prevención. Si se detecta una violación de la integridad, el servicio podría simplemente informar de esta violación, y será necesaria la intervención humana o de algún otro *software* para restablecerse de la violación. Por otra parte, existen mecanismos para la recuperación de la pérdida de integridad de los datos, como estudiaremos más tarde. La incorporación de mecanismos de recuperación automatizada se presenta, en general, como la alternativa más atrayente.

NO REPUDIO

El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. Así, cuando se envía un mensaje, el receptor puede comprobar que, efectivamente, el supuesto emisor envió el mensaje. De forma similar, cuando se recibe un mensaje, el emisor puede verificar que, de hecho, el supuesto receptor recibió el mensaje.

SERVICIO DE DISPONIBILIDAD

Tanto X.800 como RFC 2828 definen la disponibilidad como la propiedad que tiene un sistema o recurso de un sistema de estar accesible y utilizable a petición de una entidad autorizada, según las especificaciones de rendimiento para el sistema (un sistema está disponible si proporciona servicios de acuerdo con el diseño del sistema en el momento en que los usuarios lo soliciten). Una variedad de ataques puede dar como resultado la pérdida o reducción de la disponibilidad. Algunos de estos ataques son susceptibles a contramedidas automatizadas, como la autentificación o el cifrado, mientras que otras requieren algún tipo de acción física para prevenir o recuperarse de la pérdida de disponibilidad de elementos de un sistema distribuido.

La norma X.800 trata la disponibilidad como una propiedad asociada a diferentes servicios de seguridad. Sin embargo, tiene sentido solicitar un servicio concreto de disponibilidad. Un servicio de disponibilidad es aquel que protege un sistema para asegurar su disponibilidad y trata los problemas de seguridad que surgen a raíz de ataques de interrupción de servicio. Depende de la gestión y control adecuados de los recursos del sistema y, por lo tanto, del servicio de control de acceso y otros servicios de seguridad.

La Tabla 1.3 muestra la relación existente entre los servicios de seguridad y los ataques.

Tabla 1.3 Relación entre servicios de seguridad y ataques

	Ataque					
Servicio	**Obtención del contenido del mensaje**	**Análisis de tráfico**	**Suplantación**	**Repetición**	**Modificación de mensajes**	**Interrupción de servicio**
Autentificación de las entidades origen/destino			Y			
Autentificación del origen de los datos			Y			
Control de acceso			Y			
Confidencialidad	Y					
Confidencialidad del flujo de tráfico		Y				
Integridad de los datos				Y	Y	
No repudio						
Disponibilidad						Y

1.4 MECANISMOS DE SEGURIDAD

La Tabla 1.4 presenta los mecanismos de seguridad definidos en X.800. Como se puede observar, los mecanismos se dividen en aquellos que se implementan en una capa específica de un protocolo y aquellos que no son específicos de ninguna capa de protocolo o servicio de seguridad en particular. Estos mecanismos se tratarán en las secciones correspondientes de este libro y por ello no se elaboran ahora, excepto para adelantar la definición de cifrado. X.800 distingue entre mecanismos de cifrado reversible y mecanismos de cifrado irreversible. El primero es un algoritmo de cifrado que permite cifrar los datos y, posteriormente, descifrarlos. Por otro lado, los mecanismos de cifrado irreversible incluyen algoritmos *hash* y códigos de autentificación de mensajes, que se emplean en firmas digitales y en aplicaciones de autentificación de mensajes.

La Tabla 1.5, basada en X.800, indica la relación que se da entre los servicios de seguridad y los mecanismos de seguridad.

Tabla 1.4 Mecanismos de seguridad (X.800)

MECANISMOS ESPECÍFICOS DE SEGURIDAD

Pueden ser incorporados en la capa de protocolo adecuada para proporcionar algunos de los servicios de seguridad OSI

Cifrado

El uso de algoritmos matemáticos para transformar datos en una forma inteligible. La transformación y la posterior recuperación de los datos depende de un algoritmo y cero o más claves de cifrado.

Firma digital

Datos añadidos a, o una transformación criptográfica de, una unidad de datos que permite al receptor verificar la fuente y la integridad de la unidad de datos y protegerla de la falsificación (por parte del receptor).

Control de acceso

Una serie de mecanismos que refuerzan los derechos de acceso a los recursos.

Integridad de los datos

Una serie de mecanismos empleados para verificar la integridad de una unidad de datos o del flujo de unidades de datos.

Intercambio de autentificación

Un mecanismo diseñado para comprobar la identidad de una entidad por medio del intercambio de información.

Relleno del tráfico

La inserción de bits en espacios en un flujo de datos para frustrar los intentos de análisis de tráfico.

Control de enrutamiento

Permite la selección de rutas físicamente seguras para determinados datos y permite los cambios de enrutamiento, especialmente cuando se sospecha de una brecha en la seguridad.

Notarización

El uso de una tercera parte confiable para asegurar determinadas propiedades de un intercambio de datos.

MECANISMOS GENERALES DE SEGURIDAD

Mecanismos que no son específicos de ninguna capa de protocolo o sistema de seguridad OSI en particular.

Funcionalidad fiable

La que se considera correcta con respecto a algunos criterios (por ejemplo, los establecidos por una política de seguridad).

Etiquetas de seguridad

La marca asociada a un recurso (que podría ser una unidad de datos) que designa los atributos de seguridad de ese recurso.

Detección de acciones

Detección de acciones relacionadas con la seguridad.

Informe para la auditoría de seguridad

Recopilación de datos para facilitar una auditoría de seguridad, que consiste en una revisión y un examen independientes de los informes y actividades del sistema.

Recuperación de la seguridad

Maneja las peticiones de los mecanismos (como funciones de gestión de acciones) y lleva a cabo acciones de recuperación.

1.5 UN MODELO DE SEGURIDAD EN REDES

La Figura 1.3 constituye un modelo que presenta, en términos generales, gran parte de los aspectos que discutiremos a continuación. Un mensaje ha de ser transmitido de una parte a otra mediante algún tipo de internet. Las dos partes, que son los interlocutores en esta transacción, deben cooperar para que el intercambio tenga lugar. Se establece un canal de información definiendo una ruta a través de la internet que vaya de la fuente al

Tabla 1.5 Relación entre servicios y mecanismos de seguridad

	Mecanismo							
Servicio	**Cifrado**	**Firma digital**	**Control de acceso**	**Integridad de los datos**	**Intercambio de autentificación**	**Relleno del tráfico**	**Control del enrutamiento**	**Notarización**
Autentificación de entidades origen/destino	Y	Y			Y			
Autentificación del origen de los datos	Y	Y						
Control de acceso			Y					
Confidencialidad	Y						Y	
Confidencialidad del flujo del tráfico	Y					Y	Y	
Integridad de los datos	Y	Y		Y				
No repudio		Y		Y				Y
Disponibilidad				Y	Y			

destino y mediante el uso cooperativo de los protocolos de comunicación (TCP/IP) por parte de los dos interlocutores.

Los aspectos de seguridad entran en juego cuando se necesita o se quiere proteger la transmisión de información de un oponente que pudiera presentar una amenaza a la confidencialidad, a la autenticidad, etc. Todas las técnicas para proporcionar seguridad tienen dos componentes:

- Una transformación relacionada con la seguridad de la información que se va a enviar. Ejemplos de ello los tenemos en el cifrado del mensaje, que lo desordena para que resulte ilegible al oponente, y la aplicación de un código basado en el contenido del mensaje, que puede usarse para verificar la identidad del emisor.
- Alguna información secreta compartida por los interlocutores y desconocida por el oponente. El ejemplo lo hallamos en una clave de cifrado usada en conjunción con la transformación para desordenar el mensaje antes de la transmisión y reordenarlo en el momento de la recepción[4].

[4] El Capítulo 3 trata una forma de cifrado, conocida como cifrado de clave pública, en la que sólo uno de los dos interlocutores necesita conocer la información secreta.

Para lograr una transmisión segura, puede ser necesaria una tercera parte confiable, que, por ejemplo, sea la responsable de distribuir la información secreta a los dos interlocutores y la guarde de cualquier oponente. También puede ser necesaria para arbitrar disputas entre los interlocutores en lo relativo a la autenticidad de la transmisión de un mensaje.

Este modelo general muestra que hay cuatro tareas básicas en el diseño de un servicio de seguridad particular:

1. Diseñar un algoritmo para llevar a cabo la transformación relacionada con la seguridad. El algoritmo debe estar diseñado de forma que un oponente no pueda frustrar su finalidad.
2. Generar la información secreta que deba ser usada con el algoritmo.
3. Desarrollar métodos para distribuir y compartir la información secreta.
4. Especificar un protocolo para los dos interlocutores que hagan uso del algoritmo de seguridad y la información secreta, para obtener un servicio concreto de seguridad.

La Segunda Parte de este libro se centra en los tipos de mecanismos y servicios de seguridad que encajan en el modelo que muestra la Figura 1.3. Sin embargo, existen otras situaciones relacionadas con la seguridad que son de interés y que no se corresponden claramente con este modelo, pero que se tienen en consideración en este libro. La Figura 1.4 ofrece un modelo general de estas situaciones, que refleja la preocupación por proteger un sistema de información del acceso no deseado. La mayoría de los lectores están familiarizados con los problemas ocasionados por la existencia de *hackers*, que tratan de penetrar sistemas a los que se puede acceder por una red. El *hacker* puede ser alguien que, sin la intención de hacer daño, obtiene satisfacción simplemente rompiendo y entrando en sistemas informáticos. El intruso también puede ser un empleado contrariado que quiere hacer daño, o un criminal que intenta explotar los sistemas computacionales para obtener beneficios financieros (obtención de números de tarjetas de crédito o realización de transferencias ilegales de dinero).

Otro tipo de acceso no deseado consiste en introducir en un sistema computacional *software* que explote debilidades en el sistema y que pueda afectar a programas de aplicaciones, como editores y compiladores. Los programas pueden presentar dos tipos de amenazas:

- **Amenazas al acceso a la información:** captura o alteración de datos por parte de usuarios que no deberían tener acceso a dichos datos.
- **Amenazas al servicio:** explotación de fallos del servicio en los computadores para impedir el uso por parte de los usuarios legítimos.

Los virus y gusanos son dos ejemplos de ataques mediante *software*. Tales ataques pueden introducirse en un sistema por medio de un disco que contenga el programa no deseado oculto en *software* útil. También pueden ser introducidos en un sistema a través de una red; este último mecanismo es de más interés en la seguridad de redes.

Los mecanismos de seguridad necesarios para enfrentarse a accesos no deseados se dividen en dos grandes categorías (véase la Figura 1.4). La primera categoría puede denominarse función de vigilancia. Incluye los procedimientos de conexión mediante clave, diseñados para negar acceso a usuarios no autorizados, y los *software* de ocultación, diseñados para detectar y rechazar gusanos, virus y ataques similares. Una vez que

un usuario o *software* no deseado accede, la segunda línea de la defensa consiste en una serie de controles internos que monitorizan la actividad y analizan la información almacenada con el fin de detectar la presencia de intrusos. Estos aspectos se tratan más exhaustivamente en la Tercera Parte del libro.

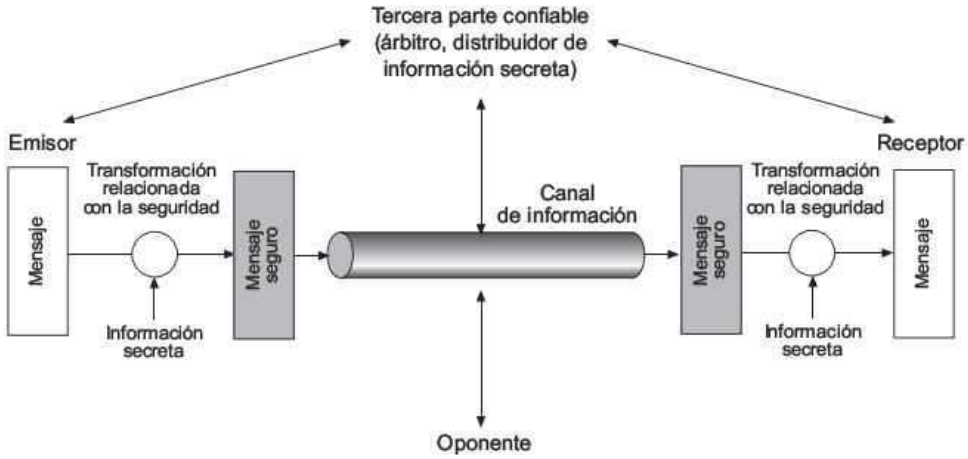


Figura 1.3 Modelo para la seguridad de redes

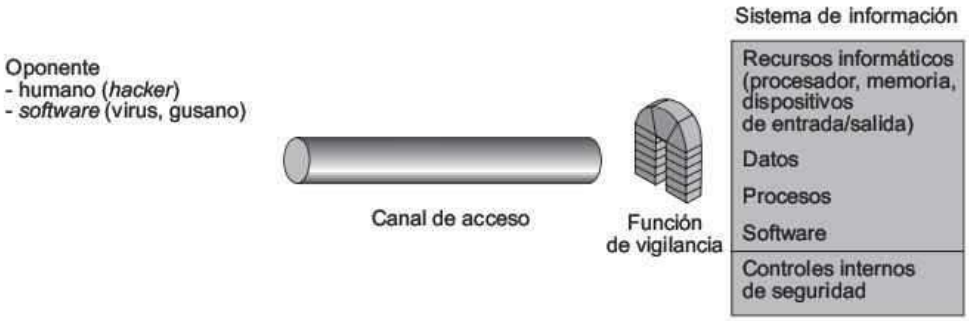


Figura 1.4 Modelo para la seguridad en el acceso a redes

1.6 ESTÁNDARES DE INTERNET Y LA SOCIEDAD INTERNET

Muchos protocolos que conforman la *suite* de protocolos TCP/IP han sido estandarizados o están en proceso de estandarización. Por acuerdo universal, una organización conocida como la Sociedad Internet es responsable del desarrollo y la publicación de los estándares. La Sociedad Internet es una organización de miembros profesionales que

controla una serie de comisiones y grupos de trabajo implicados en el desarrollo y la estandarización de Internet.

Esta sección ofrece una breve descripción de la forma en que se desarrollan los estándares para la *suite* de protocolos TCP/IP.

Tabla 1.6 Áreas de la IETF

Área IETF	Tema	Grupos de trabajo (ejemplos)
General	Proceso y procedimientos de IETF.	Políticas de trabajo. Proceso para la organización de los estándares de Internet.
Aplicaciones	Aplicaciones de Internet.	Protocolos web (HTTP). Integración EDI-Internet. LDAP.
Internet	Infraestructura de Internet.	IPv6. Extensiones PPP.
Operaciones y gestión	Estándares y definiciones para las operaciones de las redes.	SNMPv3. Monitorización remota de redes de comunicación.
Enrutamiento	Protocolos y administración para el enrutamiento de la información.	Enrutamiento Multicast. OSPF. Enrutamiento QoS.
Seguridad	Protocolos y tecnologías de seguridad.	Kerberos. IPSec. X.509. S/MIME. TLS.
Transporte	Protocolos de la capa de transporte.	Servicios diferenciados. Telefonía IP. NFS. RSVP.
Servicios de usuarios	Métodos para mejorar la calidad de la información disponible a los usuarios de Internet.	Uso responsable de Internet. Servicios de usuarios. Documentos FYI.

LAS ORGANIZACIONES DE INTERNET Y LA PUBLICACIÓN DE LOS RFC

La Sociedad Internet es el comité coordinador para el diseño, la ingeniería y la gestión de Internet. Las áreas que cubre incluyen el funcionamiento de Internet y la estandari-

zación de protocolos que se usan en sistemas terminales en Internet para operar entre sí. Existen tres organizaciones en el ámbito de la Sociedad Internet que son responsables del trabajo real del desarrollo y la publicación de los estándares:

- ***Internet Architecture Board* (IAB):** es responsable de definir la arquitectura general de Internet, proporcionando orientaciones a la IETF.
- ***Internet Engineering Task Force* (IETF):** se encarga del desarrollo y la ingeniería de protocolos en Internet.
- ***Internet Engineering Steering Group* (IESG):** responsable de la gestión técnica de las actividades de la IETF y del proceso de estándares de Internet.

Los grupos de trabajo de IETF llevan a cabo el desarrollo real de los nuevos estándares y protocolos para Internet. Ser miembro de un grupo de trabajo es una acción voluntaria y cualquier parte interesada puede participar. Durante el desarrollo de una especificación, un grupo de trabajo realizará un borrador del documento disponible como Borrador de Internet, que se coloca en el directorio en línea «Borradores de Internet» de la IETF. El documento puede permanecer como un Borrador de Internet durante seis meses, y las partes interesadas pueden revisarlo y hacer observaciones sobre él. Durante ese período de tiempo, el IESG puede aprobar la publicación del borrador como RFC (*Request for Comment*). Si el borrador no ha progresado hasta llegar al estado de RFC durante esos seis meses, se retira del directorio. El grupo de trabajo puede, a continuación, publicar una versión revisada del borrador.

La IETF es responsable de la publicación de los RFC con la aprobación del IESG. Los RFC son las notas de trabajo de la comunidad de investigación y desarrollo de Internet. Estos documentos pueden versar sobre cualquier asunto relacionado con las comunicaciones computacionales y puede constituir cualquier tipo de documento, desde un informe de una reunión a las especificaciones de un estándar.

El trabajo de la IETF se divide en ocho grandes áreas. La Tabla 1.6 refleja estas áreas y sus correspondientes objetivos.

EL PROCESO DE ESTANDARIZACIÓN

El IESG toma la decisión por la cual los RFC se convierten en estándares de Internet, con la recomendación de la IETF. Para llegar a ser un estándar, una especificación debe cumplir con los siguientes requisitos:

- Ser estable y comprensible.
- Ser técnicamente competente.
- Tener implementaciones múltiples, independientes e interoperativas con una experiencia operativa sustancial.
- Tener apoyo público significativo.
- Ser reconocidamente útil en algunas o en todas las partes de Internet.

La diferencia clave entre estos criterios y los que se usan para los estándares internacionales de la ITU se halla en la importancia que se otorga aquí a la experiencia operativa.

La parte izquierda de la Figura 1.5 presenta los diferentes pasos (*standards track*), que sigue una especificación hasta convertirse en estándar; este proceso está definido en la norma RFC 2026. A medida que se avanza por dichos pasos aumentan el escrutinio y las pruebas. En cada paso, la IETF debe solicitar recomendación para el avance del protocolo, y el IESG debe ratificarlo. El proceso comienza cuando el IESG aprueba la publicación de un borrador de Internet como RFC con el estatus de Estándar Propuesto.

Los recuadros blancos de la Figura 1.5 representan estados temporales, que deberían estar ocupados durante el tiempo mínimo. Sin embargo, un documento debe permanecer como Estándar Propuesto durante al menos seis meses, y un Estándar de Borrador, durante un mínimo de cuatro meses para permitir su revisión y discusión. Los recuadros grises representan los estados de larga duración que pueden estar ocupados durante años.

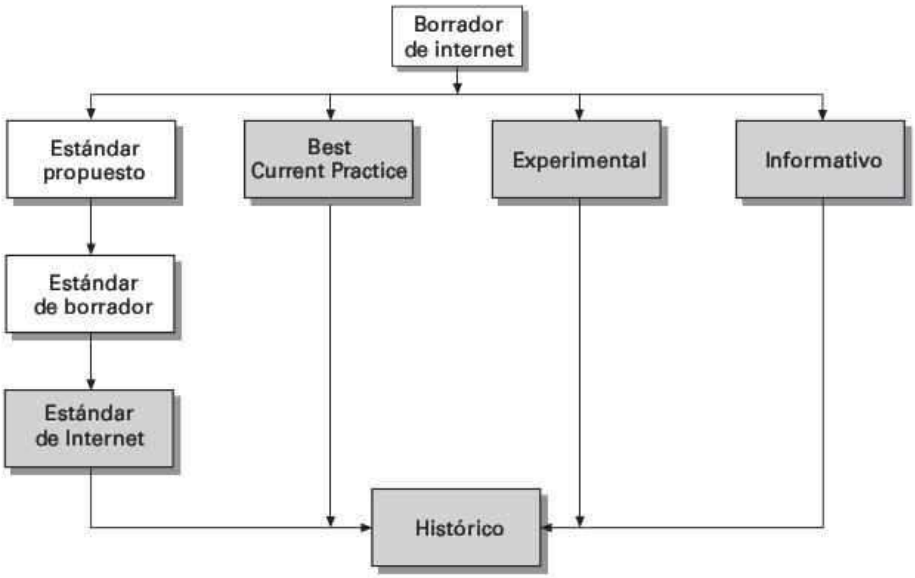


Figura 1.5 Proceso para la publicación de los RFC de Internet

Para que una especificación adquiera el estatus de Estándar de Borrador, debe haber al menos dos implementaciones independientes e interoperativas de las cuales se haya obtenido experiencia operativa adecuada.

Después de que se haya obtenido implementación significativa y experiencia operativa, la especificación puede ser elevada a Estándar de Internet. En este momento, se asigna un número STD y un número RFC a la especificación.

Finalmente, cuando un protocolo se queda obsoleto, se asigna al estado de Histórico.

CATEGORÍAS DE ESTÁNDARES DE INTERNET

Los estándares de Internet se dividen en dos categorías:

- **Especificación técnica (TS, *Technical Specification*):** define un protocolo, servicio, procedimiento, convención o formato. La mayoría de los estándares de Internet son especificaciones técnicas.

- **Informe de aplicabilidad (AS, *Applicability Statement*):** especifica cómo y en qué circunstancias una o más especificaciones técnicas pueden aplicarse para posibilitar una determinada capacidad de Internet. Un informe de aplicabilidad identifica a una o más especificaciones técnicas que son relevantes para la capacidad y puede especificar valores o rangos para determinados parámetros asociados con un TS o subgrupos funcionales de un TS relevantes para la capacidad.

OTROS TIPOS DE RFC

Hay numerosos RFC que no están destinados a convertirse en estándares de Internet. Algunos RFC estandarizan los resultados de las deliberaciones de la comunidad sobre los informes de principios o conclusiones sobre el mejor modo de realizar algunas operaciones o la función del proceso de la IETF. Estos RFC se denominan *Best Current Practice* (BCP). La aprobación de los BCP sigue básicamente el mismo proceso de aprobación para los Estándares Propuestos. A diferencia de los otros documentos, los BCP no siguen un proceso de tres etapas, sino que pasan del estatus de Borrador de Internet a BCP aprobado en un solo paso.

Un protocolo u otra especificación que no se considere preparada para la estandarización podría publicarse como un RFC Experimental. Más tarde, la especificación podría volverse a presentar. Si la especificación es, en general, estable, cumple los requisitos de diseño, se considera comprensible, ha recibido una revisión significativa por parte de la comunidad y parece gozar de suficiente interés en la misma, entonces el RFC se elevará al estatus de Estándar Propuesto.

Finalmente, se publica una Especificación Informativa para informar a la comunidad de Internet.

1.7 ESTRUCTURA DEL LIBRO

Este primer Capítulo, como vemos, sirve como introducción. El resto del libro se organiza en tres partes:

Primera Parte: proporciona un estudio conciso de los algoritmos criptográficos y los protocolos fundamentales para las aplicaciones de seguridad de redes, incluyendo el cifrado, las funciones *hash*, las firmas digitales y el intercambio de claves.

Segunda Parte: examina el uso de algoritmos criptográficos y protocolos de seguridad para proporcionar seguridad a las redes y a Internet. Los temas que abarca incluyen la autentificación de usuarios, el correo electrónico, la seguridad IP y web.

Tercera Parte: se centra en las herramientas de seguridad diseñadas para proteger un sistema informático de amenazas a la seguridad, como intrusos, virus y gusanos. Esta parte también menciona la tecnología de cortafuegos.

Muchos de los algoritmos criptográficos, protocolos y aplicaciones de seguridad en redes descritos en este libro han sido especificados como estándares. Los más importantes de ellos son los Estándares de Internet, definidos en los RFC de Internet (*Request for Comments*), y *Federal Information Processing Standards* (FIPS), publicados por el

NIST (*National Institute of Standards and Technology*). El apéndice A presenta un listado de los estándares citados en este libro.

1.8 BIBLIOGRAFÍA RECOMENDADA

[PFLE97] proporciona una buena introducción a la seguridad de computadores y de redes. Otro estudio excelente es [NICH99]. [SCHN00] es una lectura valiosa para cualquier iniciado en el campo de la seguridad en computadores y redes: trata las limitaciones de la tecnología y la criptografía en particular, a la hora de proporcionar seguridad, y la necesidad de tener en cuenta el *hardware*, la implementación de *software*, las redes y las personas implicadas en proporcionar seguridad y en atacarla.

NICH99 Nichols, R. Ed. *ICSA Guide to Cryptography.* New York: McGraw-Hill, 1999.

PFLE97 Pfleeger, C. *Security in Computing.* Upper Saddle River, NJ: Prentice Hall, 1997.

SCHN00 Schneier, B. *Secrets and Lies: Digital Security in a Networked World.* New York: Wiley, 2000.

1.9 RECURSOS WEB Y DE INTERNET

Existe una serie de recursos web y de Internet que sirven de apoyo a este libro y que pueden ayudar a seguir el ritmo de los avances en este campo.

SITIOS WEB PARA ESTE LIBRO

Se ha creado una página web especial para este libro en:

WilliamStallings.com/NetSec2e.html

El sitio incluye lo siguiente:

- **Sitios web útiles:** enlaces a otros sitios web relevantes, organizados en capítulos, que incluyen los sitios que se mencionan en esta sección y a lo largo de este libro.
- **Fe de erratas:** se mantiene y actualiza la fe de erratas de este libro. Se agradecen las indicaciones por correo electrónico sobre cualquier error que se encuentre. La fe de erratas de mis otros libros se encuentran en WilliamStallings.com.
- **Figuras:** todas las figuras de este libro en formato PDF (Adobe Acrobat).
- **Tablas:** todas las tablas de este libro en formato PDF.
- **Diapositivas:** una serie de diapositivas en Power Point, organizadas por capítulos.
- **Lista de correo de Internet:** el sitio incluye información para participar en la lista de correo de Internet del libro.

- **Cursos de seguridad de redes:** hay enlaces a páginas de cursos basados en este libro y que pueden aportar ideas a otros profesores sobre cómo estructurar el curso.

También se mantiene el sitio de recursos para estudiantes de Ciencias de la Computación en:

WilliamStallings.com/StudentSupport.html

La finalidad de este sitio es la de proporcionar documentos, información y enlaces para estudiantes y profesionales del campo de la Computación. Los enlaces y documentos están organizados en cuatro categorías:

- **Matemáticas:** incluye un curso básico de matemáticas, un libro de texto de análisis de colas, un libro de texto de sistemas de números y enlaces a numerosos sitios de matemáticas.
- **Guía *(how-to)*:** recomendaciones e indicaciones para resolver problemas, escribir informes técnicos y preparar presentaciones técnicas.
- **Recursos de investigación:** enlaces a artículos, informes técnicos y bibliografías.
- **Miscelánea:** otros documentos y enlaces útiles.

OTROS SITIOS WEB

Hay numerosos sitios web que proporcionan información relacionada con los temas de este libro. En la sección de *Bibliografía y sitios web recomendados* de capítulos posteriores, se pueden encontrar enlaces a sitios web específicos. Como las direcciones de los sitios web cambian con frecuencia, no están incluidas en el libro. Para todos los sitios web mencionados en este libro se puede encontrar el enlace adecuado en el sitio web del mismo, al que, además, se irán añadiendo otros enlaces que no se han mencionado.

Los siguientes sitios web de interés general están relacionados con la criptografía y la seguridad de redes:

- **COAST:** serie exhaustiva de enlaces relacionados con la criptografía y la seguridad de redes.
- **IETF Security Area:** material relacionado con la estandarización de la seguridad de Internet.
- **Computer and Network Security Reference Index:** un buen índice para productos comerciales, preguntas más frecuentes (FAQs), archivos de grupos de noticias, artículos y otros sitios web.
- **The Cryptography FAQ:** extensa y útil lista de preguntas más frecuentes que cubren todos los aspectos de la criptografía.
- **Tom Dunigan's Security Page:** una excelente lista de enlaces a sitios web sobre criptografía y seguridad de redes.
- **IEEE Technical Committee on Security and Privacy:** copias de sus *newsletters*, información sobre las actividades relacionadas con IEEE.
- **Computer Security Resource Center:** mantenido por el Instituto Nacional de Estándares y Tecnología (NIST); contiene una amplia información sobre amenazas a la seguridad, tecnología y estándares.

GRUPOS DE NOTICIAS DE USENET

Una serie de grupos de noticias de USENET están dedicados a algún aspecto de la seguridad de redes o la criptografía. Como con casi todos los grupos de USENET, hay un alto índice de ruido a señal, pero vale la pena comprobar si alguno cubre sus necesidades. Los más importantes son los siguientes:

- **sci.crypt.research:** es el grupo más interesante. Es un grupo moderado que trata temas de investigación; las consultas y comentarios deben guardar alguna relación con los aspectos técnicos del cifrado.
- **sci.crypt:** discusión general sobre cifrado y otros temas relacionados.
- **sci.crypt.random-numbers:** discusión sobre la aleatoriedad de la fuerza del cifrado.
- **alt.security:** discusión general sobre temas de seguridad.
- **comp.security.misc:** discusión general sobre temas de seguridad de computadores.
- **comp.security.firewalls:** discusión sobre productos y tecnología cortafuego.
- **comp.security.announce:** noticias y anuncios de CERT.
- **comp.risks:** discusión sobre riesgos ocasionados por los computadores y los usuarios.
- **comp.virus:** discusión moderada sobre virus informáticos.