IMPROVET

Seguridad en redes y seguridad de la información

Miguel Soriano

Autor: Miguel Soriano
Título: Seguridad en redes y seguridad de la información
Publicado por: České vysoké učení technické v Praze
Compilado por: Fakulta elektrotechnická
Dirección de contacto: Technická 2, Praha 6, Czech Republic
Número de teléfono: +420 2 2435 2084
Print: (only electronic form)
Número de páginas: 80
Edición: Primera edición

ISBN 978-80-01-05298-3

Revisado por: Sandra Bermejo, Jose Antonio Santos, Jordi Farré, Anna Roset

Innovative Methodology for Promising VET Areas
http://improvet.cvut.cz

Programa de acción en el ámbito del aprendizaje permanente

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea.
Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

NOTAS EXPLICATIVAS

	Definición
	Interesante
	Nota
	Ejemplo
	Resumen
+	Ventajas
–	Desventajas

ANOTACIÓN

Este módulo contiene información necesaria para la orientación básica de estudiantes en el campo de la seguridad de la información y seguridad en redes de telecomunicación.

OBJETIVOS

Este módulo proporciona información básica acerca de la seguridad de la información y la seguridad en redes de telecomunicación. Se introducen brevemente los mecanismos y herramientas para la protección de los datos que o bien están almacenados en un ordenador personal, o bien son transmitidos a través de una red. Asimismo, se indican algunas pinceladas sobre los procedimientos para mitigar los diferentes tipos de amenazas de seguridad. También incluye una breve descripción de la criptografía de clave pública, de clave simétrica y algoritmos. Por último, se comentan algunos conceptos básicos sobre la seguridad perimetral de la red incluyendo cortafuegos y sistemas de detección de intrusión, así como los protocolos habituales de seguridad en redes inalámbricas.

LITERATURA

[1] Bruce Schneier: Applied Cryptography. John Kiley & Sons, Inc., New York, 1994

[2] William Stallings: Cryptography and Network Security. Principles and Practices. Prentice Hall, New Jersey, 2003

[3] Vesna Hassler: Security fundamentals for E-Commerce. Artech House, Boston, 2001

[4] Rolf Oppliger: Internet and Intranet Security. Artech House, Boston, 2002

[5] Michael Sikorski, Andrew Honig: Practical Malware Analysis, The Hands-On Guide to Dissecting Malicious Software. No Starch Press, February 2012

[6] Michael Goodrich,Roberto Tamassia: Introduction to Computer Security, 2010

[7] John R. Vacca: Computer and Information Security Handbook (Morgan Kaufmann Series in Computer Security), 2009

[8] Jason Andress: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Elsevier, 2011

Indice

1 Introducción

1.1 Introducción

El concepto de seguridad de la información no se limita a eliminar virus, evitar que hackers puedan acceder a la red y suprimir el spam en el correo electrónico. La seguridad de la información también abarca los procedimientos que deben seguir los empleados y la dirección de una compañía para garantizar la protección de los datos confidenciales y de los sistemas de información frente a las amenazas actuales. Los términos seguridad de la información, seguridad informática y seguridad en la red a menudo se utilizan indistintamente. Estos conceptos están muy relacionados y comparten los objetivos comunes de la protección de la confidencialidad, integridad y disponibilidad de la información; sin embargo, hay algunas diferencias sutiles entre ellos.

El concepto de seguridad de la información significa proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados.

La seguridad informática es el nombre genérico para el conjunto de herramientas diseñadas con el fin de proteger los datos almacenados en un equipo y evitar ataques de piratas informáticos.

Seguridad en la red es el nombre genérico para el conjunto de herramientas diseñadas para proteger los datos durante su transmisión a través de una red de telecomunicación.

Asimismo, es muy habitual el término de seguridad en Internet. La seguridad en Internet abarca el concepto de seguridad perimetral, nombre genérico para el conjunto de herramientas diseñadas para proteger los recursos de una red privada frente a usuarios de otras redes

Las diferencias entre seguridad de la información, seguridad informática y seguridad en la red radican principalmente en la aproximación al tema, metodologías utilizadas y el ámbito en que se centra. La seguridad de la información tiene que ver con la confidencialidad, integridad y disponibilidad de los datos, independientemente de su formato. La seguridad informática se orienta a garantizar la disponibilidad y el correcto funcionamiento de un sistema informático. La seguridad en la red se centra en la protección de los datos durante su transmisión.

1.2 Causas de la inseguridad

La inseguridad de los sistemas informáticos y de las redes va más allá de los virus informáticos conocidos. La introducción de mecanismos de protección es una prioridad para cualquier empresa. Los atacantes a una red de telecomunicación no necesitan estar en contacto físico con la víctima; los datos pueden ser fácilmente copiados, transmitidos, modificados o destruidos cuando son transmitidos por la red. Como resultado, si no se dispone de los mecanismos de protección adecuados resulta difícil identificar al atacante: no hay huellas y el marco legal no está suficientemente actualizado para tratar este tipo de delitos.

La naturaleza en tiempo real de Internet añade una nueva dimensión a la delincuencia: es instantáneo.

Aunque existen muchas causas para los problemas de seguridad, por lo menos podemos mencionar tres tipos de deficiencias fundamentales que dan lugar a dichos problemas:

- Deficiencias tecnológicas
- Deficiencias de la política de seguridad
- Deficiencias de configuración

Obviamente, probablemente podríamos añadir las deficiencias humanas y algunas otras, pero el propósito de este documento es concentrarnos en aquellas cuestiones que, una vez reconocidas, se pueden controlar, vigilar y mejorar dentro de una estrategia de seguridad.

Deficiencias tecnológicas

Cada tecnología tiene algunas deficiencias inherentes conocidas o desconocidas, o vulnerabilidades que pueden ser explotadas por un atacante suficientemente motivado. Algunas deficiencias son ampliamente publicitadas en los medios de comunicación porque están asociadas con un producto bien conocido. Esto no significa que otros desarrollos o sistemas sean seguros. El hecho de que a nadie le importe lo suficiente un sistema como para hackearlo no significa necesariamente que sea seguro.

Entre otras, podemos mencionar las siguientes deficiencias:

- Los protocolos de Internet no fueron diseñados pensando en la seguridad de las comunicaciones. Actualmente se emplean servicios de seguridad y las mejores prácticas posibles para reducir los riesgos.
- Sistemas Operativos. Independientemente del fabricante o si se trata de un producto propietario o un desarrollo abierto, todos los *sistemas operativos*

(**SO**) tienen vulnerabilidades que deben ser abordadas mediante parches, actualizaciones …

- Debilidades de los accesorios y equipos de comunicación con la red. Tanto los accesorios que permiten la comunicación de un dispositivo con la red, como los equipos de red propiamente dichos (routers, …) pueden tener vulnerabilidades, a menudo llamadas "agujeros" que pueden ser aprovechas por atacantes maliciosos. Siempre que sea posible se deben aplicar parches y actualizaciones para eliminar o mitigar los problemas conocidos.

Deficiencias de la política de seguridad

Una deficiencia de la política de seguridad es una frase comodín para indicar que una política de seguridad de la empresa, (o tal vez, la falta de política), genera amenazas de seguridad en la red de forma inconsciente. Los siguientes ejemplos son algunas situaciones que pueden afectar negativamente al sistema informático de un negocio o empresa:

- Inexistencia de un documento escrito donde conste la política de seguridad. Es necesario disponer de un plan documentado y adoptado en el que consten las normativas que se deben cumplir.

- Ausencia de un plan de contingencia para recuperación en caso de desastres. Si no se dispone de dicho plan, en caso que haya un ataque a la red o una catástrofe -un incendio, una inundación o terremoto – el personal disponible improvisará las decisiones a tomar para minimizar las consecuencias. Incluso el personal mejor capacitado y con más experiencia puede tomar decisiones insensatas cuando se enfrentan a un evento catastrófico inesperado.

- Inexistencia de criterios para la modificación o incorporación de hardware o software. Ya sea motivado por el aumento de la productividad o por placer, cualquier incorporación o actualización de software o hardware puede dar lugar a nuevas vulnerabilidades de seguridad. Por ejemplo, añadir un punto de acceso inalámbrico no autorizado a una red puede suponer añadir una puerta trasera virtual a la red y a los recursos de la empresa. Del mismo modo, un protector de pantalla no autorizado puede recopilar el nombre de usuario, contraseñas, y otra información de interés para un atacante.

- Ausencia de supervisión de seguridad**.** Incluso cuando se despliega una red segura, una falta de supervisión de registros facilitan la proliferación de nuevas vulnerabilidades o un uso no autorizado. El peor caso sería no ser consciente que ha habido un ataque con importantes consecuencias.

- Políticas de empleo**.** Una rotación de personal con alta frecuencia, falta de oportunidades de los trabajadores o emplear a personas con falta de formación en cargos de responsabilidad pueden impactar de forma negativa en la seguridad de la red.

- Políticas internas**.** Una política de seguridad laxa puede dar lugar a un ambiente relativamente cómodo para un atacante. Es el síndrome de "aquí

todos somos como una familia ". Desafortunadamente, incluso en algunas de las mejores familias hay personas fraudulentas.

Deficiencias de configuración

Muchos dispositivos de red tienen una configuración por defecto que facilita la instalación o intenta conseguir las máximas prestaciones en detrimento de aspectos de seguridad. Una instalación sin la debida atención a la corrección de estas opciones puede acarrear serios problemas potenciales. Algunos problemas comunes de configuración son las siguientes:

- Ineficacia de las listas de control de acceso al no bloquear solicitudes no autorizadas.
- Contraseñas o passwords por defecto, no renovadas en mucho tiempo, o incluso, ausencia de dichas contraseñas.
- Puertos o servicios innecesarios activos.
- Intercambio de Identificadores de usuario (User IDs) y contraseñas sin cifrar.
- Acceso remoto a través de Internet no debidamente protegido

Actualmente resulta fácil identificar las vulnerabilidades más comunes y conseguir la solución adecuada para mitigar el problema.

1.3 Clasificación de los ataques

Los ataques a las redes pueden ser definidos como diferentes tipos de actividades sistemáticas dirigidas a disminuir o corromper su seguridad. Desde este punto de vista, un ataque puede ser definido como una amenaza sistemática generada por una entidad de una manera artificial, deliberada e inteligente.

Las redes de ordenadores pueden ser vulnerables a muchas amenazas utilizando distintas formas de ataque, entre ellas:

- Ingeniería social, alguien trata de acceder usando medios sociales (haciéndose pasar por un usuario legítimo o el administrador del sistema, engañando a la gente para que le revelen secretos o claves, etc.). Esta vía de ataque suele dar muchos resultados a los atacantes.

- Ataques de denegación de servicio, incluyendo todos los tipos de ataques destinados a saturar a un ordenador o a una red, de tal manera que los usuarios legítimos no puede utilizarla.

- Ataques a determinados protocolos, aprovechando debilidades conocidas.

- Ataques a servidores, que aprovechan las vulnerabilidades de ciertos sistemas operativos de los ordenadores o vulnerabilidades en la configuración y administración del sistema.

- Adivinar contraseñas; las contraseñas son secuencias de símbolos, generalmente asociadas a un nombre de usuario, que proporcionan un mecanismo para la identificación y la autenticación de un usuario en particular. En casi todos los servicios son los propios usuarios quienes eligen sus contraseñas, y con frecuencia eligen secuencias que no pueden ser consideradas seguras (por ejemplo, nombre de la pareja , nombre de hijo/hija, fechas de nacimiento, …) Como regla general, las contraseñas que son fáciles de recordar son también fáciles de adivinar.

- Espionaje de todo tipo, incluyendo la captura de mensajes de correo electrónico, archivos, contraseñas y otra información a través de una conexión de red que permite capturar todos los mensajes de un usuario.

Los ataques de seguridad pueden clasificarse en:

- Ataques pasivos.

- Ataques activos.

1.4 Ataques pasivos

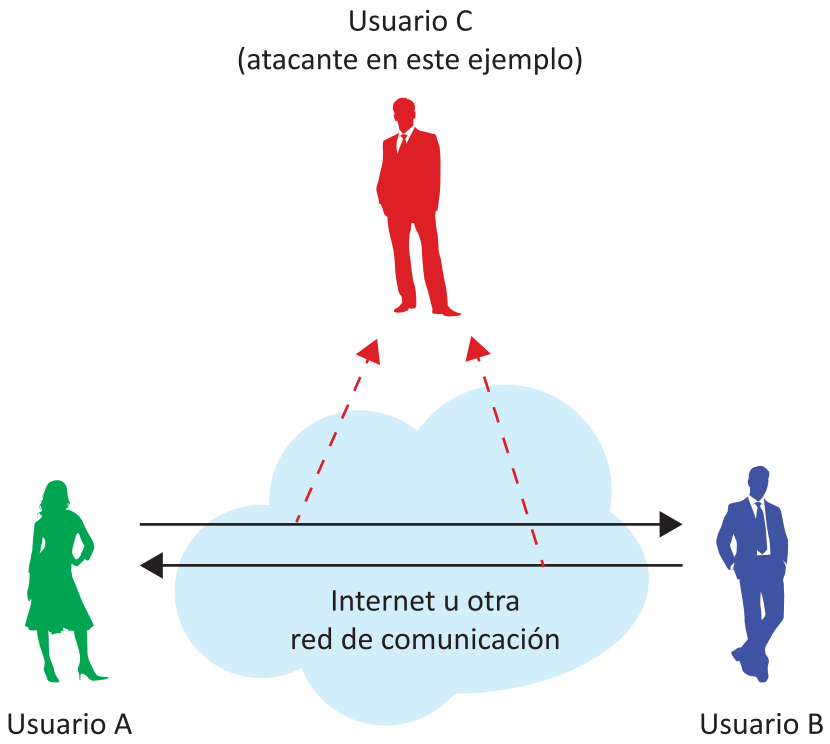
Un ataque pasivo es aquél en que el atacante monitoriza el canal de comunicación sin modificar ni añadir datos. Un atacante pasivo sólo pone en peligro la confidencialidad de los datos. El objetivo del atacante es obtener la información que se está transmitiendo.

Los ataques pasivos están relacionados con el contenido del mensaje y con el análisis de tráfico:

- Espionaje**.** En general, la mayoría de la información que se transmite utilizando una red de comunicaciones se envía de forma no segura (sin cifrar) permitiendo a un atacante "escuchar" o interpretar (leer) los datos intercambiados. Uno de los mayores problemas a los que se enfrenta un administrador de una red deriva de la capacidad de un atacante para monitorizarla. Sin servicios de cifrado (basados en el uso de técnicas criptográficas), los datos pueden ser leídos por otras personas a medida que circulan por la red.

- Análisis de tráfico. Se refiere al proceso de interceptar y examinar los mensajes con el fin de deducir información de patrones en la comunicación. Se puede realizar incluso cuando los mensajes están cifrados. En general, cuanto mayor es el número de mensajes observados, interceptados y almacenados, más se puede inferir del tráfico. El análisis de tráfico, entre otras cosas, permite a un atacante verificar que dos entidades están manteniendo una comunicación en un determinado momento.

La figura 1 muestra un modelo de ataque pasivo



Modelo de ataque pasivo

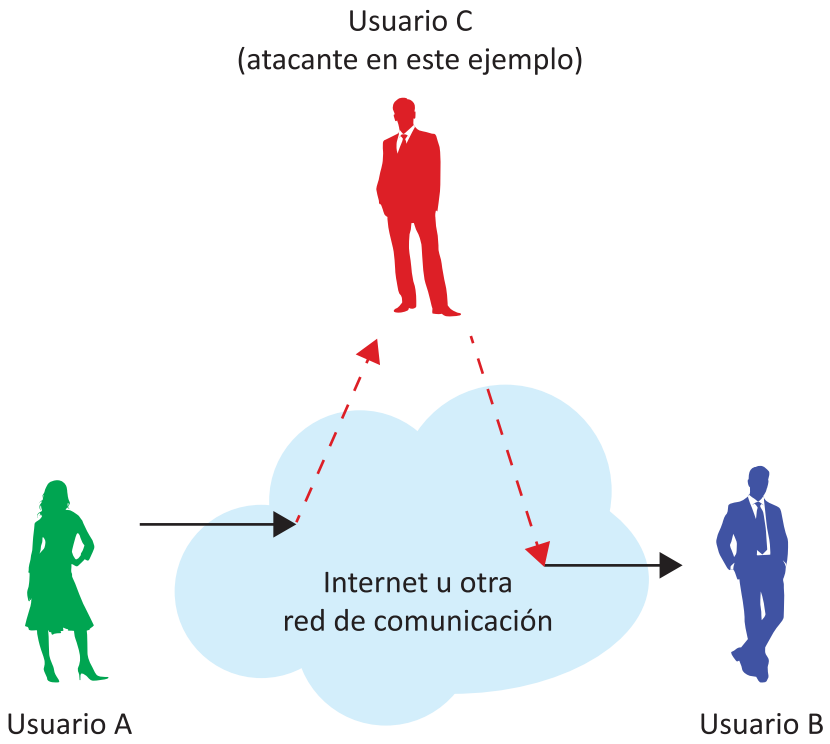
1.5 Ataques activos

Un ataque activo intenta alterar los recursos del sistema o afectar a su funcionamiento. En este tipo de ataque el adversario intenta borrar, añadir, o modificar los datos transmitidos. Un atacante activo amenaza la integridad de datos y autenticación, así como la confidencialidad.

Los ataques activos engloban alguna modificación del flujo de datos o la creación de datos falsos. Puede dividirse en seis categorías:

- **Suplantación de identidad.** Es un tipo de ataque en el que el atacante suplanta la identidad de otro usuario.
- **Repetición.** En este tipo de ataque, una transmisión de datos válida es repetida o retardada de forma maliciosa. Este ataque lo puede provocar el mismo emisor de datos originales o bien un atacante que los intercepta y posteriormente los retransmite, posiblemente como parte de un ataque de suplantación de identidad.
- **Modificación de mensajes**. El atacante elimina un mensaje que atraviesa la red, lo altera, y lo reinserta.
- *Hombre en el medio* (*Man in the Middle*, **MitM**). En este tipo de ataques, un atacante intercepta las comunicaciones entre dos entidades, por ejemplo entre un usuario y un sitio web. El atacante puede utilizar la información que consigue para luego suplantar la identidad del usuario o realizar cualquier otro tipo de fraude.
- *Denegación de Servicio* (*Denial of Service* **DoS**) y *Denegación de Servicio Distribuida* (*Distributed Denial of Service*, **DDoS**). Una **denegación de servicio** (DoS) es una situación en la que un usuario u organización se ve privado de los servicios o recursos que normalmente debería tener. En denegación de servicio distribuida, un gran número de sistemas comprometidos (a veces llamado botnet) atacan a un solo objetivo.
- *Amenazas Avanzadas Persistentes* (*Advanced Persistent Threat*, **APT**). Es un ataque a la red en el que un atacante consigue un acceso no autorizado a la red y permanece allí sin ser detectado durante un largo período de tiempo. La principal intención de un ataque APT es robar datos más que causar daños a la red u organización. Algunas organizaciones que pueden ser objetivo de ataques APT son sectores con alto valor informativo, como la defensa nacional, la industria financiera.

La figura 2 muestra un ejemplo de un ataque activo (en concreto, de un ataque de modificación)



Ataque activo de modificación

1.6 Atacantes: objetivos y comportamiento

Un atacante o intruso es un individuo que obtiene, o trata de obtener, permisos o acceso no autorizado al sistema de información.

Existen muchos enfoques sobre la forma de clasificar a los atacantes. Los criterios utilizados habitualmente se pueden dividir en los siguientes tres grupos:

- La ubicación del atacante respecto al sistema atacado.
- Nivel de conocimiento del atacante
- Objetivo – por qué se ha realizado el ataque

Desde el punto de vista de la ubicación del atacante, existen dos tipos diferentes de atacantes:

- Atacante interno
- Atacante externo o intruso

Un **atacante interno** es, en general, una persona que tiene acceso a la red informática interna, y por lo tanto es un usuario legítimo, pero intenta obtener acceso a datos, recursos y servicios del sistema a los que él no debería acceder o bien hacer mal uso de cualquier dato al que esté autorizado.

Un **intruso o atacante externo** es generalmente una persona que no está autorizada a acceder a la red informática interna y desea entrar aprovechando vulnerabilidades del sistema.

Dependiendo del nivel de conocimiento del atacante, la clasificación es:

- Aficionados.
- Profesionales.

Los aficionados llevan a cabo ataques menos peligrosos que los profesionales. Esos ataques están en consonancia con el nivel de formación e instrumentación de los atacantes.

El grupo de profesionales por lo general está constituido por excelentes especialistas en informática o telecomunicaciones, altamente capacitados y cualificados y con acceso a recursos especializados. En la práctica, esto significa que son capaces de generar ataques muy peligrosos con graves consecuencias para los sistemas informáticos y redes.

Un tema muy discutido cuando se trata de la clasificación de atacantes es la división en las dos categorías siguientes

- Hackers,

- Crackers.

Un **Hacker** es una persona con excelentes habilidades en informática o telecomunicaciones, muchas veces con experiencia en proyectos importantes de software y cuyo conocimiento es muy útil para encontrar posibles vulnerabilidades y agujeros de seguridad en los sistemas. La actividad del hacker es útil y provechosa. Incluso hay códigos éticos del comportamiento que debe tener un hacker.

Un **Cracker** es una persona que tiene la capacidad de superar las protecciones de un sistema informáticos y que utiliza sus conocimientos de una manera poco ética. Sin embargo, hay más definiciones de este grupo de atacantes que hacen hincapié en el diferente alcance de sus actividades.

Existen también otros grupos de atacantes, posiblemente el más numeroso sea el de **scriptkiddies**. Se trata de usuarios con conocimientos informáticos bastante limitados. Sus ataques se limitan a ejecutar partes de código que han encontrado en algunas páginas web destinados a aprovecharse de una vulnerabilidad de un sistema. Dichos atacantes no conocen qué acción va a realizar la ejecución de este software, aunque sus efectos suelen tener consecuencias graves.

1.7 ¿Cómo podemos protegernos?

En esta sección se recomiendan las siguientes prácticas para usuarios domésticos

Use contraseñas robustas

A menudo, la única protección utilizada son las contraseñas. Un identificador de usuario (User ID) es sólo un nombre y requiere una contraseña asociada para poder tener la certeza que se trata de dicho usuario. Por lo tanto, las contraseñas son nuestras claves y debemos protegerlas. Los cortafuegos y sistemas de detección de intrusos no sirven para nada si nuestras contraseñas están comprometidas.

Una contraseña segura es la que no se puede encontrar en cualquier diccionario – castellano, catalán, inglés, alemán, … Eso significa que una contraseña que no debe ser fácil de adivinar. En general, las contraseñas más largas son más difíciles de adivinar o descifrar que las contraseñas cortas son.

A continuación se presenta una lista que se puede utilizar para establecer contraseñas seguras:

- **Usar una combinación de letras sin sentido:** Las mejores contraseñas aparentan ser un puro disparate bajo el punto de vista sintáctico. Por ejemplo, si tomamos la frase: "No esperes que me comporte perfectamente y dibuje esa sonrisa radiante" y utilizamos sólo la primera letra de cada palabra, nuestra contraseña sería *neqmcpydesr*.

- **Incluir una mezcla de caracteres mayúscula, minúscula y numéricos:** La contraseña debería incluir alguna letra mayúscula en algún lugar que no fuese el inicio y también algún número.

- **Las contraseñas largas son mejores**: La contraseña debería tener al menos 8 caracteres de longitud.

- **Las contraseñas deben cambiarse periódicamente**: Incluso las mejores contraseñas deben cambiarse periódicamente (cada 60 días aproximadamente) para evitar que sean utilizadas mucho tiempo si alguien las descubre. Muchos sistemas operativos permiten configurar esta regla para cada usuario. Aunque bajo el punto de vista de usuario esta regla no es práctica, bajo un punto de vista de seguridad resulta muy conveniente.

- **Generar nuevas contraseñas en lugar de reutilizar las mismos una y otra vez**: Una contraseña no debería ser utilizada de nuevo por un usuario en un periodo de tiempo inferior a un año.

- **No utilizar un conjunto de caracteres consecutivos en el teclado:** Debe evitarse el uso de contraseñas como *qwerty, 12345678,* o *asdfghj*. Aunque aparentemente son texto sin sentido, estas secuencias siguen patrones vinculados a la posición de las teclas en el teclado y se pueden romper fácilmente.

- **Tratar las contraseñas de forma totalmente secreta Las contraseñas no se comparten y tienen que estar protegidas.** Muchos usuarios escriben sus contraseñas en notas adhesivas pegadas a sus ordenadores o las ponen debajo de sus teclados. ¡Eso no sirve para nada!

Para un atacante las contraseñas de administrador son las llaves del reino. Los administradores del sistema con privilegios de root - es decir, sin restricciones de acceso y la capacidad de hacer cualquier tipo de cambios - deben tener contraseñas muy difíciles de adivinar y deben seguir las normas más estrictas respecto al cambio y reutilización. Se recomienda que un administrador cambie TODAS las contraseñas de usuario si sospecha que se ha comprometido su clave.

Del mismo modo, si un usuario general sospecha que la contraseña ha sido robada o comprometida, debe cambiarla inmediatamente.

Usar siempre protección antivirus

El software antivirus no es siempre efectivo 100%, pero es mejor que no tener ninguna protección en absoluto. Es muy posible que un usuario que no haya instalado un antivirus en su ordenador piense que no tiene ningún virus aunque probablemente su equipo esté infectado.

El software antivirus consta de dos partes: el *motor de análisis* y los *archivos de firma*. Es necesario actualizar periódicamente tanto el motor de análisis como los archivos de firmas, sino el software antivirus pierde su capacidad. El software antivirus generalmente contiene un comando de actualización, o bien se puede consultar si hay actualizaciones pendientes en el sitio Web del fabricante.

El motor de análisis le indica al software cómo y dónde realizar la búsqueda, y los archivos de firma son esencialmente una base de datos de virus conocidos y sus acciones. El motor de análisis compara los archivos que contiene el ordenador con los virus conocidos que hay en los archivos de firma. El archivo de firma contiene los patrones de virus conocidos. El software antivirus puede equivocarse indicando falsos positivos (ficheros correctos que son considerados como virus).

Cuando se encuentran nuevos virus, los vendedores de software antivirus actualizan sus archivos de firmas para incluir estos nuevos virus. En ocasiones, también el motor de análisis requiere una actualización. Si se actualiza una parte del programa y la otra queda obsoleta, el software no funcionará correctamente.

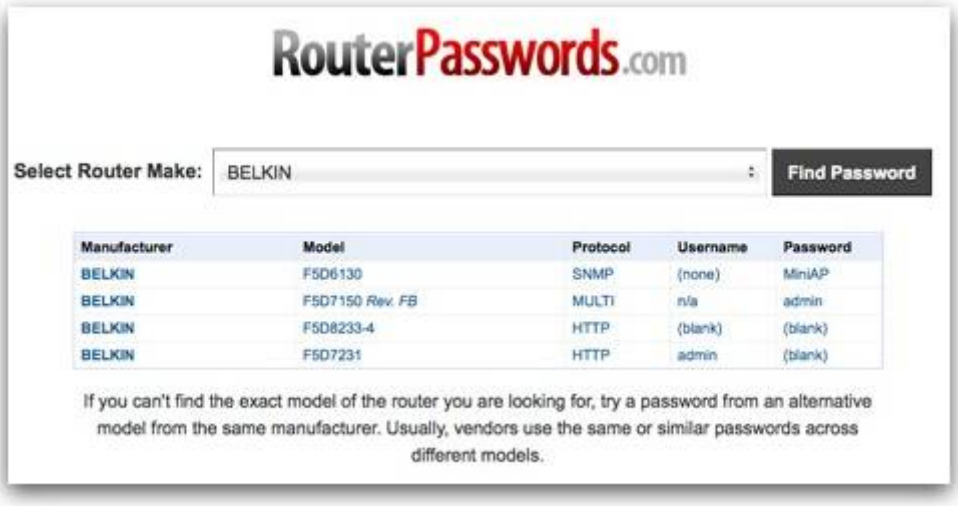
Con el fin de lograr la máxima protección, es necesario instalar el software antivirus tanto en equipos individuales, como en todos los servidores de la red. Esa es la única manera de detectar virus en todos los puntos de entrada. Todos los medios extraíbles, como unidades de memoria USB, CD, ... deben ser analizados antes de utilizarse en un sistema. Si el software antivirus está instalado en los cortafuegos se podrán detectar los virus que vienen de las conexiones externas, en particular de Internet.

Cambiar las configuraciones predeterminadas

Uno de los errores más habituales es instalar un sistema dejando la configuración por defecto. Las configuraciones predeterminadas a menudo tienen cuentas de administrador predeterminadas y contraseñas que conocen todos los piratas informáticos. Esto es aplicable a routers, hubs, switches, sistemas operativos, sistemas de correo electrónico, bases de datos, servidores web…

Además de tener contraseñas conocidas en los equipos, las configuraciones predeterminadas pueden contener múltiples vulnerabilidades de seguridad y deben ser parcheadas. Antes de poner cualquier ordenador en la red, se deberían cambiar los nombres de cuenta y contraseñas por defecto y aplicar todos los parches de seguridad. Aunque esas tareas impliquen consumir más tiempo en la instalación, ahorrará muchos dolores de cabeza posteriores.

La figura 3 muestra un ejemplo de passwords por defecto en algunos routers.



Ejemplo de passwords por defecto en routers

Usar un cortafuego (firewall)

Es muy recomendable usar algún tipo de producto de firewall. Los posibles atacantes exploran constantemente los sistemas que utilizan la mayoría de usuarios en busca de vulnerabilidades conocidas. Los firewalls de red (ya sean basados en software o hardware) pueden proporcionar cierto grado de protección contra estos ataques. Sin embargo, ningún firewall puede detectar o detener todos los ataques, por lo que no es de gran ayuda instalar un firewall si luego ignoramos todas las medidas de seguridad.

No abrir ficheros adjuntos desconocidos en correos electrónicos

Antes de abrir los archivos adjuntos de correo electrónico, debemos estar seguros de conocer el origen de los datos. No es suficiente que el correo haya sido enviado

desde una dirección reconocida. El virus Melissa se extendió precisamente porque se originó a partir de una dirección familiar. El código malicioso puede ser distribuido en programas divertidos o tentadores.

Al abrir un archivo adjunto, es importante tener en cuenta el siguiente procedimiento:

1. tener el antivirus esté actualizado
2. guardar el archivo en el disco duro
3. escanear el archivo con un software antivirus
4. abrir el archivo

Para una protección adicional, se puede desconectar el ordenador de la red antes de abrir el archivo.

Debemos tener en cuenta que seguir estos pasos reduce, pero no elimina totalmente la posibilidad de que cualquier código malicioso que haya en el fichero adjunto se extienda desde un ordenador a otros.

No ejecutar programas de origen desconocido

Nunca se debe ejecutar un programa a menos que sepa lo ha desarrollado una persona o empresa de confianza. Además, no se deben enviar programas de origen desconocido a amigos o compañeros de trabajo simplemente porque son divertidos - pueden contener lo que se denomina un caballo de Troya.

Mantener actualizadas todas las aplicaciones, incluyendo el sistema operativo

Los vendedores de software suelen entregar parches cuando se descubre que un programa tiene una vulnerabilidad. La mayoría de los productos disponen de un método para obtener actualizaciones y parches.

Algunas aplicaciones comprueban automáticamente si hay actualizaciones disponibles. Si no es así, es necesario comprobar periódicamente si hay actualizaciones pendientes de instalar.

Apagar el ordenador o desconéctelo de la red cuando no lo use

Es recomendable tener el ordenador apagado o desconectado de la red cuando no está siendo utilizado. En esas condiciones, un atacante no puede atacar a un equipo.

Hacer copias de seguridad de los datos críticos y crear un disco de arranque

Es conveniente guardar una copia de los archivos críticos en un medio extraíble, y almacenar los discos de copia de seguridad en algún lugar lejos del ordenador. Además, es muy útil crear un disco de arranque para permitir la recuperación de un equipo si hubiese problemas.

1.8 Resumen

En este capítulo se han introducido algunos conceptos fundamentales: seguridad de la información, seguridad informática y seguridad de la red, así como las diferencias entre ellos. En segundo lugar, se han presentado algunas de las causas de la inseguridad de la información y se han clasificado los ataques a la seguridad y los tipos de atacantes siguiendo diferentes criterios. Por último, se ha incluido un apartado donde se recomiendan buenas prácticas para los usuarios domésticos con el fin de mejorar su protección.

2 Software malicioso y antivirus

2.1 Concepto of software malicioso (malware)

Software malicioso (**malware**) es un término genérico que hace referencia a cualquier software dañino instalado en un sistema, diseñado para ejecutar instrucciones no deseadas en un ordenador, sin el consentimiento del usuario.

La ejecución de malware puede degradar la velocidad de las tareas que un usuario desea realizar en su ordenador y también puede obtener información crítica u obtener acceso no autorizado a un sistema informático. Malware no es lo mismo que software defectuoso, este último es software que tiene un propósito legítimo, pero contiene errores que no fueron detectados antes de su despliegue.

De hecho, los virus informáticos son en realidad un subconjunto de la familia de malware, donde también se incluyen los gusanos, troyanos, adware, spyware, rootkits, etc...

Hoy en día, la mayoría de los programas maliciosos se distribuyen a través de Internet. Uno de los métodos más comunes que se conoce como "drive-by download". El archivo malicioso se descarga a través de la web o por correo electrónico como fichero adjunto, y se ejecuta. En muchos casos, se engaña al usuario haciéndole creer que un determinado programa le puede resultar muy útil. En otros casos, el usuario no es consciente de estar infectado y visita una página Web que se aprovecha de las vulnerabilidades de su navegador web para descargar y ejecutar el malware. Prácticamente cualquier protocolo de Internet puede ser utilizado para distribuir malware, por ejemplo, la mensajería instantánea o P2P. Por otra parte, es importante recordar que los dispositivos de almacenamiento físicos pueden propagar el malware, es muy común la distribución a través de los pen drives USB.

2.2 Software antivirus

El software antivirus o anti-virus se usa para prevenir, detectar y eliminar el malware, incluyendo pero sin limitarse a los virus informáticos, gusanos, troyanos, spyware y adware. Para ser eficaz, el software antivirus debe ser actualizado periódicamente - de lo contrario no será capaz de ofrecer protección contra nuevos virus.

El término utilizado para la limpieza de un ordenador es la erradicación de virus. Hay varios métodos de erradicación:

- Eliminar el código que se corresponde con el virus del archivo infectado;
- Eliminar el archivo infectado;
- Poner en cuarentena el archivo infectado, lo que implica su traslado a un lugar donde no se puede ejecutar.

Se suelen emplear distintas estrategias:

Detección basada en firmas consiste en la búsqueda de patrones conocidos en un código ejecutable. Los virus se reproducen infectando las "aplicaciones host" lo que significa que se copia una porción de código ejecutable en un programa existente. Los virus están programados para no infectar el mismo archivo varias veces con el fin de tener la certeza que funcionan según lo previsto. Para ello, se incluyen una serie de bytes en la aplicación para comprobar si ya ha sido infectada, esto se denomina firma de virus. Dicha firma es única para cada virus. Los programas antivirus intentan detectar la presencia de esta firma para decidir si el archivo está infectado o no. Este método se denomina detección basada en firmas y es el método más antiguo utilizado por el software antivirus. Sin embargo, este método no puede detectar virus cuyas firmas no han sido archivadas por los editores del software antivirus. Además, los programadores de virus a menudo utilizan técnicas de camuflaje para dificultar la detección de las firmas.

Un tipo de enfoque heurístico son las firmas genéricas que pueden identificar virus nuevos o variantes de los virus existentes a partir del conocimiento de código malicioso conocido o ligeras variaciones de dicho código. El método heurístico analiza el comportamiento de las aplicaciones con el objetivo de detectar actividad similar a la de un virus conocido. Por lo tanto, este tipo de programa antivirus puede detectar virus, aun cuando la base de datos antivirus no haya sido actualizado. Sin embargo, en estos esquemas podemos encontrarnos con falsas alarmas, es decir, que el antivirus identifique a un software totalmente correcto como malicioso.

Independientemente de las prestaciones que ofrezca un software antivirus, a veces puede tener inconvenientes. El software antivirus puede empeorar el rendimiento de un ordenador. Los usuarios inexpertos pueden tener problemas para entender las indicaciones y decisiones que el software antivirus les presenta. Una decisión incorrecta puede dar lugar a una brecha de seguridad.

2.3 Clasificación de malware

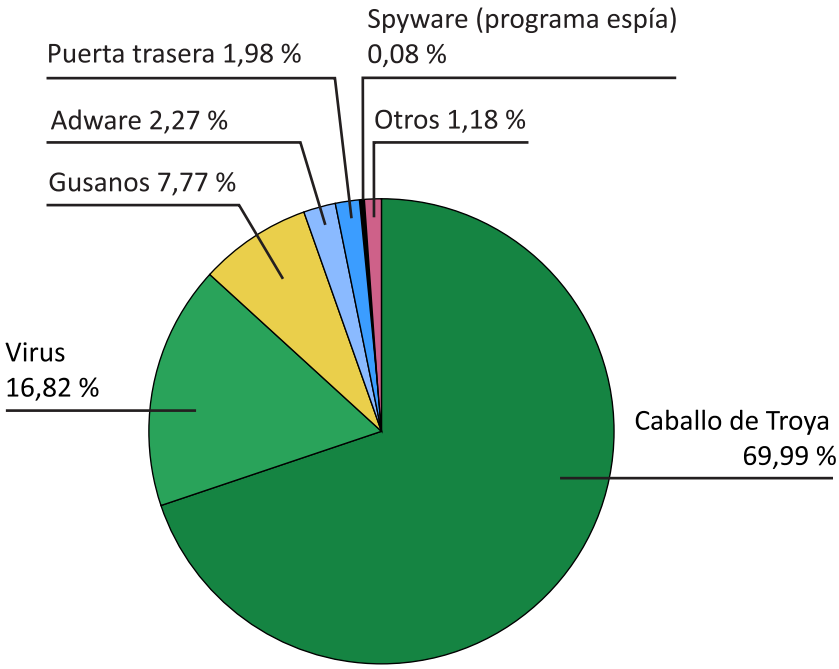
El malware puede ser clasificado de diferentes maneras de acuerdo a diferentes criterios: mecanismos de distribución, métodos de instalación del sistema, la forma en que son controlados remotamente, etc.

Actualmente los ejemplares de malware suelen tener muchas características, por lo que normalmente se clasifican de acuerdo a su función principal. Por ejemplo, podría haber un caballo de Troya con capacidades de rootkit y que puede permanecer oculto tanto a soluciones de seguridad como a usuarios expertos. También podría estar instalado en un equipo que forme parte de una red de ordenadores infectados y controlados a distancia. Al mismo tiempo, podría hacer que aparezcan anuncios y capture las pulsaciones de teclado, por lo que también sería parte de las familias de programas publicitarios y keylogger. Es decir, sería un caballo de Troya-rootkit-bot-adware-keylogger ... Todo en uno! De hecho, este ejemplo es bastante común

Una primera clasificación de programas maliciosos se basa en la necesidad de un archivo de host para propagarse. Los siguientes cuatro tipos de software malicioso se corresponden a malware que requieren dicho archivo:

- Puertas trampa (Trap doors),
- Bombas lógicas (Logic bombs),
- Caballos de Troya o troyanos,
- Virus.

La figura 4 muestra la distribución de malware por categorías (fuente: Panda Security)



Distribución de malware por categorías.
16 de marzo de 2011

Fuente: Panda Security

Distribución de malware por categorías

Hay dos tipos de software malicioso que no necesitan un archivo de host para su propagación. Son:

- Gusanos (Worms),
- Zombies.

Las puertas trampa son como entradas ocultas en el programa que permiten conseguir el acceso al sistema, evitando los mecanismos de seguridad. Estos mecanismos son utilizados por los programadores durante la depuración de programas para evitar el uso de mecanismos de autenticación y obtener así privilegios especiales. El software malicioso busca estas trampas para evitar los mecanismos de seguridad. Las consecuencias en el sistema informático suelen ser graves.

Las bombas lógicas constituyen la clase de software malicioso más antigua. Es un software integrado en un programa legítimo que se activa cuando se dan algunas condiciones. Un ejemplo de estas condiciones puede ser la presencia o ausencia de un archivo específico en días preestablecidos, semana o fecha de inicio de una aplicación determinada… Una bomba lógica puede causar pérdida o daños en el sistema de información, por ejemplo, puede borrar algunos archivos, dejar de ejecutar aplicaciones y así sucesivamente ...

Los troyanos son programas o comandos, que realizan procedimientos o procesos útiles, y al mismo tiempo realizan actividades maliciosas en segundo plano como

borrado de datos. Un caso particular es el spyware, un software que captura las contraseñas introducidas a través del teclado, recopila la información sobre las páginas web visitadas, el tipo de software que está utilizando en el equipo, … y toda esa información recopilada se envía a través de Internet.

Los virus son programas capaces de conectarse a otro programa o archivo y pueden ejecutar acciones no autorizadas. Para su propagación es necesario que el archivo host pueda ser modificado por el virus. Los virus pueden atacar a otros archivos, propagarse y corromper sistemas de información.

Un gusano puede propagarse de un sistema informático a otro si los dos sistemas están interconectados por la red. La propagación del gusano se realiza por ejemplo mediante el uso de correo electrónico.

Un zombi es un software malicioso que se propaga a través de la red. Después de penetrar con éxito en un sistema informático, el ordenador infectado puede ser controlado y administrado remotamente. Cuando varios ordenadores están infectados por el mismo tipo de software malicioso y controlados por un ordenador remoto, se denomina botnet. Este ordenador remoto puede forzar a los ordenadores infectados a ejecutar las mismas órdenes, dando lugar a los ataques de denegación de servicio distribuido **DDoS** *(Distributed Denial of Service)*.

2.4 Ciclo de vida de un virus

El ciclo de vida de un virus consta de cuatro fases:

- Fase latente,
- Fase de propagación,
- Fase de activación,
- Fase de ejecución

En la fase latente, el virus permanece inactivo, por lo que no realiza ninguna actividad. Es necesario tener en cuenta que no todos los virus tienen esta fase en su ciclo de vida.
En la fase de propagación el virus incrusta una copia idéntica en otro programa o en un sector del disco. Así pues, cada programa infectado incluye clones de virus capaces de propagarse.
En la fase de activación el virus inicia su estado activo. Esta fase tiene su inicio cuando se cumplen ciertas condiciones o estados del programa infectado.

En la fase de ejecución el virus realiza la actividad para la que se programó durante su creación. Por lo general, son actividades destructivas y pueden causar pérdidas de información en el sistema informático infectado.

2.5 Resumen

En este capítulo se ha introducido el concepto de software malicioso o malware, y se ha clasificado dicho software atendiendo a diversos criterios: propagación, método de instalación, características principales, … Además, se han presentado las fases en el ciclo de vida de un virus. Finalmente, se describen diversas técnicas para limpiar un ordenador infectado. Dado que esas técnicas exigen la detección del malware, se han presentado las distintas estrategias que se utilizan habitualmente

3 Servicios de seguridad y mecanismos de seguridad

3.1 Servicios de seguridad

Un servicio de seguridad es un servicio que garantiza que los sistemas de información o las transferencias de datos puedan tener la seguridad adecuada. Los servicios de seguridad se implementan mediante mecanismos de seguridad y de acuerdo a las políticas de seguridad.

Durante más de veinte años, los pilares básicos de la seguridad de la información han sido la *confidencialidad, integridad y disponibilidad* (conocida como la tríada CIA, del inglés confidentiality, integrity and availability).

Posteriormente se fueron añadiendo otros servicios nuevos; la **autenticación, control acceso, no repudio y privacidad**. Sin embargo, no existe todavía una clasificación de los servicios de seguridad totalmente aceptada entre los profesionales de esta materia.

3.2 Confidencialidad

La confidencialidad hace referencia a la protección de la información frente a su divulgación a entidades o individuos no autorizados (organizaciones, personas, máquinas, procesos). Nadie debe poder leer los datos a excepción de las entidades específicas previstas.

La confidencialidad es un requisito:

- Cuando se almacenan los datos en un medio (tal como un disco duro de ordenador) al que puede acceder una persona no autorizada.
- Cuando los datos se copian en un dispositivo que puede acabar en manos de una persona no autorizada.
- Cuando los datos se transmiten a través de redes desprotegidas.

Dada la sofisticación y la capacidad actual de los posibles atacantes, se deben emplear **técnicas criptográficas** para cifrar cualquier dato que se considere crítico, garantizando así su confidencialidad. Al igual que ocurre con la integridad de datos, si hay un intercambio de información crítica entre diversas entidades es necesario que haya un acuerdo previo de los algoritmos y claves a utilizar.

3.3 Integridad de datos

La integridad de datos es la protección de los datos frente a la modificación, supresión, duplicación o reordenación realizada por entidades no autorizadas (organizaciones, personas, máquinas, procesos). Más concretamente, la integridad se refiere a la fiabilidad de los recursos de información. Una violación de la integridad se debe siempre a un ataque activo.

La integridad de datos es la garantía de la no alteración: se garantiza la detección de cualquier alteración de los datos (ya sea en tránsito por la red o en almacenamiento en un disco duro, por accidente o deliberadamente). Es evidente que esta garantía es esencial en cualquier tipo de entorno empresarial o comercio electrónico, y es más que deseable en muchos otros entornos.

La integridad de un sistema de información implica garantizar que no ha habido ninguna corrupción en los datos que han sido transmitidos o almacenados en el sistema, detectando cualquier posible manipulación. Para ello, es necesario el uso de técnicas criptográficas.

3.4 Disponibilidad

Disponibilidad significa tener acceso a la información cuando se requiere. Por ejemplo, un fallo de un disco o un ataque de denegación de servicio pueden causar una violación de la disponibilidad. Cualquier retardo superior al establecido según los niveles de servicio puede ser descrito como una violación de la disponibilidad. Si un sistema de información no está disponible cuando se necesita es, como mínimo, tan malo como no disponer de dicho sistema.

La disponibilidad, de la misma forma que otros aspectos de seguridad, puede verse afectada por cuestiones puramente técnicas (por ejemplo, una parte mal funcionamiento de una computadora o dispositivo de comunicaciones), fenómenos naturales (por ejemplo, el viento o el agua), o causas humanas (accidental o deliberada).

Si bien el riesgo relativo asociado con cada una de estas categorías depende del contexto particular, la regla general es que los seres humanos constituyen el eslabón más débil. Esa es la razón por la que resulta fundamental la capacidad de cada usuario y su voluntad de utilizar un sistema de datos de forma segura.

3.5 Autenticación

El servicio de autenticación se encarga de asegurar la identidad de las entidades que participan en la comunicación. Es decir, el servicio de autenticación evita que un usuario o entidad pueda suplantar la identidad de otro.

En el caso de un único mensaje, por ejemplo una señal de alarma, la función del servicio de autenticación es garantizar al receptor la identidad del mensaje del remitente.

En el caso de una interacción, tal como la conexión de un terminal a un servidor, hay dos aspectos involucrados. En primer lugar, en el momento de inicio de conexión, el servicio de autenticación permite asegurar que las dos entidades son auténticas, es decir, que cada uno es la entidad que dice ser. En segundo lugar, el servicio debe garantizar que no hay interferencias en la conexión de tal manera que no sea posible que un tercero pueda suplantar la identidad de alguna de las dos partes legítimas durante la comunicación.

3.6 Control de acceso

El control de acceso es la protección de los servicios o recursos de información para evitar puedan ser accesibles por parte de entidades no autorizadas (organizaciones, personas, máquinas, procesos). Es decir, el control de acceso se refiere a la prevención del uso no autorizado de un recurso. Por lo tanto, este servicio controla quien y en qué condiciones puede acceder a ciertos recursos, y en caso que accedan qué permisos (lectura, modificación, ejecución, …) tienen sobre dichos recursos.

El cumplimiento de este servicio exige que cuando una entidad quiere conseguir acceso a un recurso, en primer lugar se deberá identificar. Con el fin de entender mejor este servicio es importante definir los conceptos siguientes:

- Privilegios – derechos de acceso o uso de los recursos o servicios
- Sujetos – entidades sobre las que se ejecutan los derechos de acceso
- Principal – entidades que gestiona los derechos del control de acceso
- Objeto / Objetivo – recursos y servicios a los que accede un sujeto.
- Delegación – transferencia de los privilegios de control de acceso entre principales
- Autorización – transferencia de los privilegios de control de acceso de un principal a un sujeto

Las Listas de control de acceso *(***ACLs** *Access control lists*) son el mecanismo de protección más comúnmente utilizado para ofrecer este servicio.

3.7 No-repudio (irrenunciabilidad)

Para tener comunicaciones seguras se requiere integrar un servicio encargado de generar evidencias digitales que permitan resolver posibles controversias surgidas en caso de errores de red o de mal comportamiento de alguna de las entidades que participan en el intercambio de información.

No repudio es el servicio de seguridad que utiliza estas evidencias para proporcionar protección contra la negación de una de las entidades de haber participado en la totalidad o parte de una comunicación.

No repudio es el servicio de seguridad que garantiza que el remitente de un mensaje no puede negar posteriormente haber enviado el mensaje y que el receptor no pueda negar haberlo recibido.

Esto incluye el no repudio de origen (es decir, la prueba de que el mensaje fue enviado por el emisor correspondiente) y no repudio de recepción (es decir, la prueba de que el mensaje ha sido recibido por el destinatario).

- **NRO** (*No repudio de origen*) proporciona evidencias a los receptores de que el mensaje fue enviado por el remitente
- **NRR** (*No repudio de recepción*) proporciona evidencias a los remitentes que el destinatario recibió el mensaje.

Los mecanismos de protección típicos son: notarización, registros temporales (time stamping), firmas digitales y servicios de confirmación.

3.8 Privacidad de datos

Privacidad de datos es el servicio de seguridad que permite a un individuo tener el derecho de controlar la información que se recopila sobre él, quien la utiliza, cómo y para qué la utiliza.

En una red abierta como Internet, cada vez resulta más fácil recopilar información sobre una persona, pudiendo comprometer su privacidad. Las nuevas tecnologías pueden desarrollar nuevas formas de captura de información con implicaciones negativas para la privacidad. El uso de la minería de datos y las prestaciones cada vez mejores de los motores de búsqueda permiten capturar y combinar información a partir de una amplia variedad de bases de datos.

Hay muchísima información almacenada en bases de datos en todo el mundo, de forma que una persona no tiene posibilidades o conocimientos para controlar la información que hay sobre sí misma. Dicha información puede ser vendida y/o utilizarse para fines desconocidos. El concepto de privacidad de la información es cada vez más importante.

La privacidad en Internet es un tema candente. Las problemáticas que abarca pueden clasificarse en:

- Qué información personal se puede compartir .
- Cómo se pueden intercambiar mensajes sin que nadie no autorizado los vea.
- Cómo se pueden realizar transacciones de forma totalmente anónima.

Por otra parte, la capacidad de rastrear la ubicación de dispositivos móviles da lugar a nuevos problemas como la localización de un usuario y sus preferencias.

Hay muchas formas de proteger la privacidad del usuario en Internet. Por ejemplo, tanto los e-mails como el contenido de páginas web se puede cifrar. La navegación por páginas web y otras actividades en la red pueden ser desarrolladas sin dejar huellas a través de anonimizadores llamados mix nets. Estas mix nets se pueden utilizar para impedir que los proveedores de servicios a Internet sepan qué sitios visitamos y con quién nos comunicamos.

3.9 Mecanismos de seguridad

Un mecanismo de seguridad es un proceso que implementa uno o más servicios de seguridad. Los mecanismos de seguridad dan soporte a los servicios de seguridad y ejecutan actividades específicas para la protección frente a ataques o resultados del ataque.

Los mecanismos de seguridad fundamentales son:

- Cifrado
- Firma digital
- Control de acceso
- Integridad de datos
- Intercambio de autenticación
- Relleno de tráfico
- Control de encaminamiento
- Notarización

Cifrado es un mecanismo destinado a proteger el contenido de un mensaje mediante el uso de algoritmos matemáticos que transforman los datos originales. Como resultado se obtiene una secuencia de bits indescifrables para cualquier usuario no autorizado.

Firma digital es un mecanismo que utiliza herramientas criptográficas para autentificar el origen, garantizar la integridad de los datos y ofrecer protección contra falsificaciones.

Control de acceso abarca una variedad de mecanismos que establecen la política de derechos de acceso a los recursos. Este mecanismo requiere la autenticación y posteriormente la autorización para acceder a los recursos que se desee proteger.

Integridad de datos abarca una variedad de mecanismos utilizados para asegurar la integridad de un mensaje o de un flujo de datos.

Intercambio de autenticación el objetivo de este mecanismo es asegurar la identidad de una entidad mediante un intercambio de información.

Tráfico de Relleno es un mecanismo que inserta bits en un flujo de datos para impedir que tenga éxito un ataque por análisis de tráfico.

Control de encaminamiento permite que un mensaje cuando atraviesa una red de telecomunicación siga unos determinados enlaces y permite cambios en las rutas, especialmente cuando se detecta que hay un problema de seguridad.

Notarización es un mecanismo que utiliza terceras partes de confianza para garantizar ciertas propiedades en un intercambio de datos.

Seguridad perimetral es un mecanismo que permite aceptar o bloquear datos procedentes o destinados a un ordenador concreto ubicado fuera de la red local.

3.10 Mapeo entre servicios y mecanismos de seguridad

Un servicio de seguridad a veces requiere la implantación de diversos mecanismos de seguridad. La siguiente gráfica ilustra la relación entre servicios y mecanismos de seguridad.

	Cifrado	Firma digital	Control de acceso	Integridad de datos	Intercambio autenticación	Tráfico de relleno	Control de encaminamiento	Notarización
Autenticación	√	√			√			
Control de acceso			√					
Confidencialidad	√					√	√	
Integridad de datos	√	√		√				
No repudio		√		√				√
Disponibilidad			√	√				
Privacidad	√					√	√	

Servicios y mecanismos de seguridad

3.11 Resumen

Garantizar un nivel de seguridad adecuado en las transferencias de datos requiere la integración de diferentes servicios. En este capítulo, hemos presentado los servicios de seguridad más importantes (confidencialidad, integridad, disponibilidad, autenticación, control de acceso, no repudio y privacidad) y se han introducido los mecanismos de seguridad necesarios para prestar dichos servicios. Básicamente, estos mecanismos son: cifrado, firma digital, control de acceso, integridad de datos, intercambio de autenticación, tráfico de relleno, control de encaminamiento y notarización. Finalmente, se ha establecido una conexión entre los servicios y mecanismos de seguridad.

4 Conceptos básicos de criptografía

4.1 Introducción

La criptografía es una herramienta matemática que permite ofrecer protección contra muchas amenazas. Muchas aplicaciones de seguridad están basadas en el uso de la criptografía para el cifrado y descifrado de datos.

El cifrado es la mecanismo de seguridad que permite cambiar los datos de modo que si una persona no autorizada accede a los datos cifrados, no le servirán para nada. El descifrado es la conversión de los datos cifrados a su forma original.

La criptografía permite almacenar información crítica o transmitirla a través de redes inseguras (como Internet), de modo que no puede ser leída por nadie excepto el destinatario previsto. La criptografía se ha convertido en un estándar de la industria para proporcionar seguridad de la información, privacidad, control del acceso a los recursos y las transacciones electrónicas.

Esta técnica se utiliza en las acciones cotidianas, como hacer o recibir una llamada de un teléfono móvil, pagar con una tarjeta de crédito o débito, retirar dinero de un cajero automático o iniciar una sesión en un equipo con una contraseña.

Un algoritmo criptográfico no es más que una aplicación de herramientas matemáticas usadas en el proceso de cifrado y descifrado. Un algoritmo criptográfico trabaja en combinación con una clave - una palabra, número o frase - para cifrar un documento (texto, imagen, música, video,…). El mismo documento original queda cifrado de forma distinta cuando se utilizan claves diferentes. La seguridad de los datos cifrados depende de dos cosas: la robustez del algoritmo criptográfico y el secreto de la clave.

Un algoritmo criptográfico robusto debe cumplir con los siguientes requisitos:

- No debe haber ninguna manera de encontrar el documento original a partir del documento cifrado si no se conoce la clave excepto por fuerza bruta, es decir, probando todas las claves posibles hasta que se encuentre la correcta.
- El número de claves posibles debe ser muy grande, de forma que sea imposible computacionalmente realizar un ataque de fuerza bruta con éxito en un período de tiempo razonable.

- Cualquier cosa que se realiza mediante el cifrado se debe poder deshacer durante el descifrado utilizando la clave correspondiente.
  En este documento, se presenta qué se puede conseguir mediante el uso del cifrado. A continuación se introducirán los conceptos básicos y los tipos de algoritmo criptográfico. Sin embargo, está **fuera del alcance de este documento** detallar:

  - **cómo funciona el cifrado**, principios básicos para el diseño de algoritmos criptográficos

  - **cómo puede fallar el cifrado,** como se pueden romper los algoritmos criptográficos mediante criptoanálisis.

4.2 Clasificación de los algoritmos criptográficos

Los algoritmos criptográficos se pueden clasificar en:

Algoritmos de clave simétrica o de clave secreta. En estos algoritmos, se utiliza la misma clave para el cifrado y el descifrado. El algoritmo *Advanced Encryption Standard* (**AES**) es un ejemplo de un sistema de cifrado simétrico ampliamente utilizado.

Criptografía de clave pública o criptografía de clave asimétrica es un esquema que usa un par de claves para cada usuario: una clave pública, que puede ser conocida por todo el mundo, y una clave privada que el usuario debe mantener en secreto. Aunque las dos claves de un mismo par están matemáticamente relacionadas, es computacionalmente imposible deducir la clave privada a partir de la clave pública. Se utiliza una de esas dos claves para cifrar y la otra para descifrar. Cualquier persona que tenga la clave pública de un usuario puede cifrar la información destinada a dicho usuario, pero no puede descifrarla porque ello requeriría el uso de la clave privada. Sólo el usuario que tiene dicha clave privada puede descifrar la información.

La principal ventaja de la criptografía de clave pública es que permite intercambiar mensajes de forma segura a personas que no se conocen previamente. El emisor y el receptor no tienen que compartir las claves secretas; sólo se intercambian las claves públicas y nunca se transmiten las claves privadas.

4.3 Terminología

Texto en claro es el mensaje que el emisor quiere transmitir al receptor.

Criptograma o Texto cifrado es el resultado obtenido al cifrar el texto en claro.

Cifrado es el proceso que cambia el contenido de un texto en claro ocultando el mensaje original.

Descifrado es el proceso inverso al cifrado, se trata de recuperar el mensaje original (texto en claro) a partir del criptograma.

Clave es una palabra, número o cadena de caracteres que necesita el algoritmo criptográfico para cifrar el texto en claro o para descifrar el criptograma.

Algoritmo de hash es un algoritmo que convierte una cadena de texto de longitud arbitraria en una cadena de longitud fija.

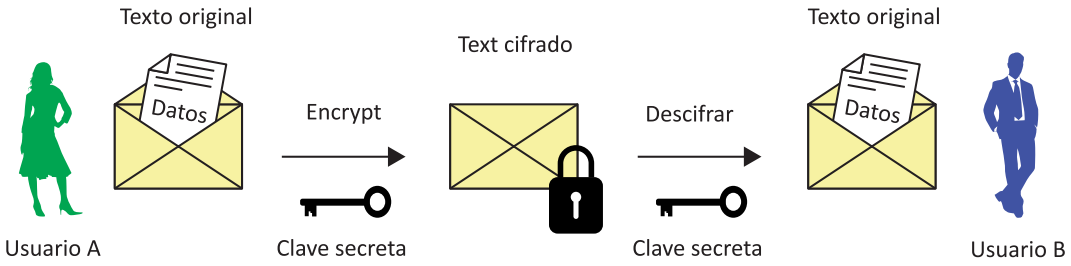
Algoritmo criptográfico una función matemática usada para el cifrado y el descifrado.

Gestión de claves - Proceso mediante el cual se genera una clave, se almacena, se protege, se transfiere, se usa y se destruye cuando es preciso.

4.4 Criptografía de clave simétrica

El proceso de cifrado y descifrado de información mediante el uso de una única clave se conoce como criptografía de clave simétrica o criptografía de clave secreta. En la criptografía de clave simétrica, las claves utilizadas para cifrar el texto en claro y para descifrar el texto cifrado suelen ser idénticas (situación habitual), o bien cuando se conoce una también se conoce la otra, ya que están vinculadas mediante una transformación muy simple. El principal problema con algoritmos de clave simétrica es que el remitente y el receptor tienen que ponerse de acuerdo en esa clave común.

El proceso de cifrar mediante criptografía de clave simétrica es el siguiente: El usuario A desea enviar un mensaje al usuario B y quiere tener la certeza que sólo el usuario B es capaz de leer el mensaje. Para proteger la transmisión, el usuario A genera una clave secreta, cifra el mensaje con esta clave, y envía el criptograma al usuario B. El usuario B necesita esa clave para poder descifrar el texto cifrado. El usuario A puede transmitir la clave secreta al usuario B mediante el uso de cualquier medio disponible, siempre que sea una transmisión segura. Cuando el usuario B reciba la clave secreta, ya podrá descifrar el criptograma para recuperar el texto en claro.



Modelo de cifrado con criptografía simétrica

Las propiedades que un algoritmo de cifrado deben cumplir son las siguientes:

- **Difusión:** cada bit del texto en claro influye en muchos bits del criptograma y cada bit del criptograma se ve afectado por muchos bits del texto en claro.
- **Confusión:** es necesario evitar las relaciones estructuradas (especialmente linealidad) entre texto plano y texto cifrado que podrían ser explotadas en los ataques conocidos.
- El criptograma debería tener apariencia aleatoria.
- **Simplicidad.** No debe ser necesario disponer de un hardware complejo para poder ejecutar el algoritmo.
- **Eficiencia:** muy rápido en hardware y software en una amplia variedad de plataformas.

Los algoritmos de clave simétrica más utilizados son:

- *Data Encryption Standard* (**DES**)
- *Advanced Encryption Standard* (**AES**)

El principal problema cuando se utiliza criptografía simétrica es que el proceso de transferencia de claves al receptor puede suponer un gran riesgo de seguridad. La transferencia de la clave secreta a través de Internet mediante un mensaje de correo electrónico es insegura. Asimismo, tampoco es seguro transmitir la clave oralmente mediante una llamada telefónica ni enviarla mediante correo convencional.

Los riesgos de seguridad derivados del uso de la criptografía simétrica se han podido solventar en gran medida mediante el uso de la criptografía de clave pública. Un ejemplo de uso de criptografía simétrica es el cifrado de datos en los discos duros. En ese caso como la misma persona cifra y descifra los datos no hay ningún problema con la distribución de claves.

4.5 Criptografía de clave pública

La criptografía de clave pública apareció para hacer resolver los problemas de seguridad que plantea la criptografía simétrica. Este método resuelve el problema de transmisión de claves que tiene la criptografía de clave secreta mediante el uso de dos **claves** en vez de una sola, utilizando una de ellas para el cifrado, y la otra para el descifrado.

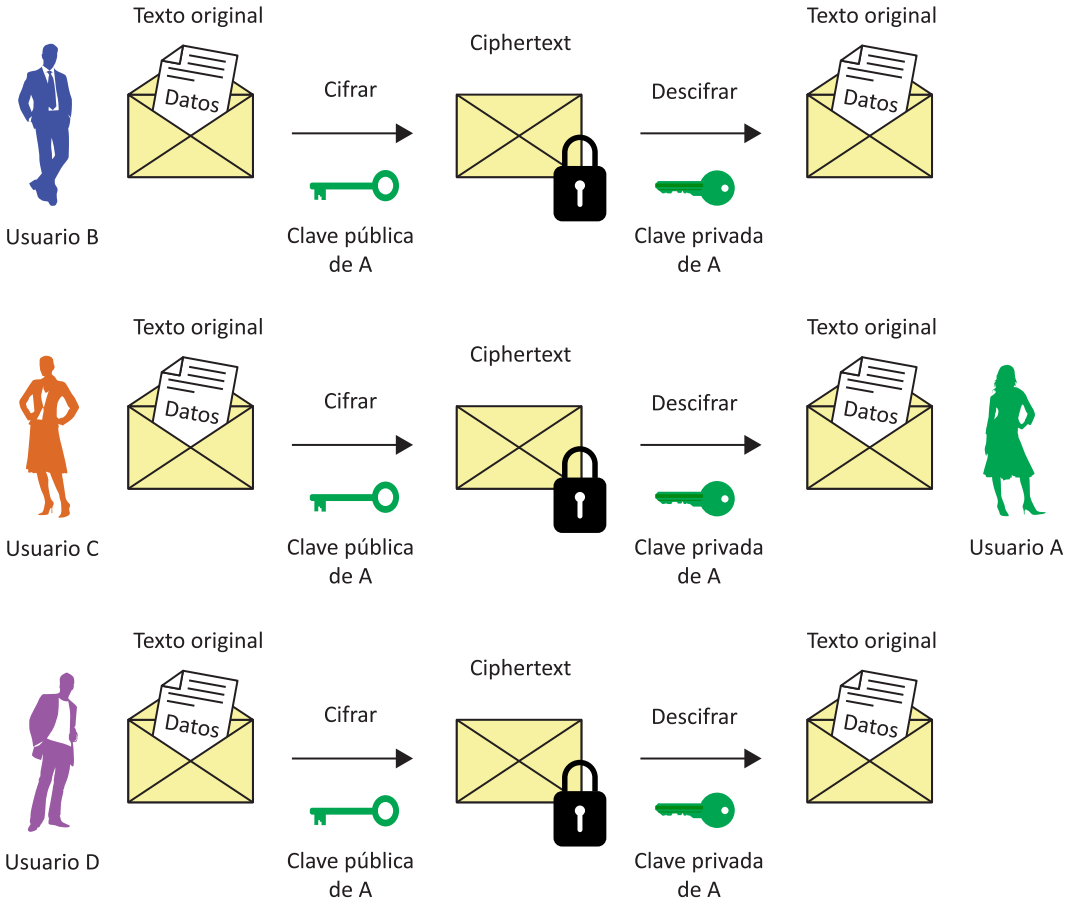
Este proceso se conoce como criptografía de clave pública o criptografía asimétrica. Las dos claves utilizadas se conocen colectivamente como el **par de claves**. En la criptografía asimétrica, una de las claves es de libre distribución. Esta clave se denomina **clave pública**. Por eso, este método de cifrado también se llama el cifrado de clave pública. La segunda clave es la **clave privada** y como indica su propio nombre no es distribuible. Es importante señalar que las claves públicas y privadas están relacionadas, pero es prácticamente imposible deducir la clave privada si se conoce la clave pública.

El más común es el algoritmo de clave pública **RSA**.

4.6 ¿Cómo se cifra con criptografía de clave pública?

Uso de cifrado de clave pública para proporcionar confidencialidad

Veamos un ejemplo: el Usuario_B quiere enviar un mensaje al Usuario_A. El Usuario_B cifra el mensaje con la clave pública del Usuario_A, y el Usuario_A descifra el mensaje utilizando su clave privada. Dado que los pares de claves son complementarias, sólo la clave privada del Usuario_A podría descifrar este mensaje. Si otra persona intercepta el texto cifrado, no será capaz de descifrarlo, ya que se necesita la clave privada de Usuario_A para el descifrado. Este método no proporciona autenticación, no se puede demostrar que el mensaje procede del Usuario_B, porque la clave pública de Usuario_A la puede conocer todo el mundo. Sin embargo, sí se ofrece confidencialidad al mensaje, ya que sólo Usuario_A puede descifrar el mensaje.



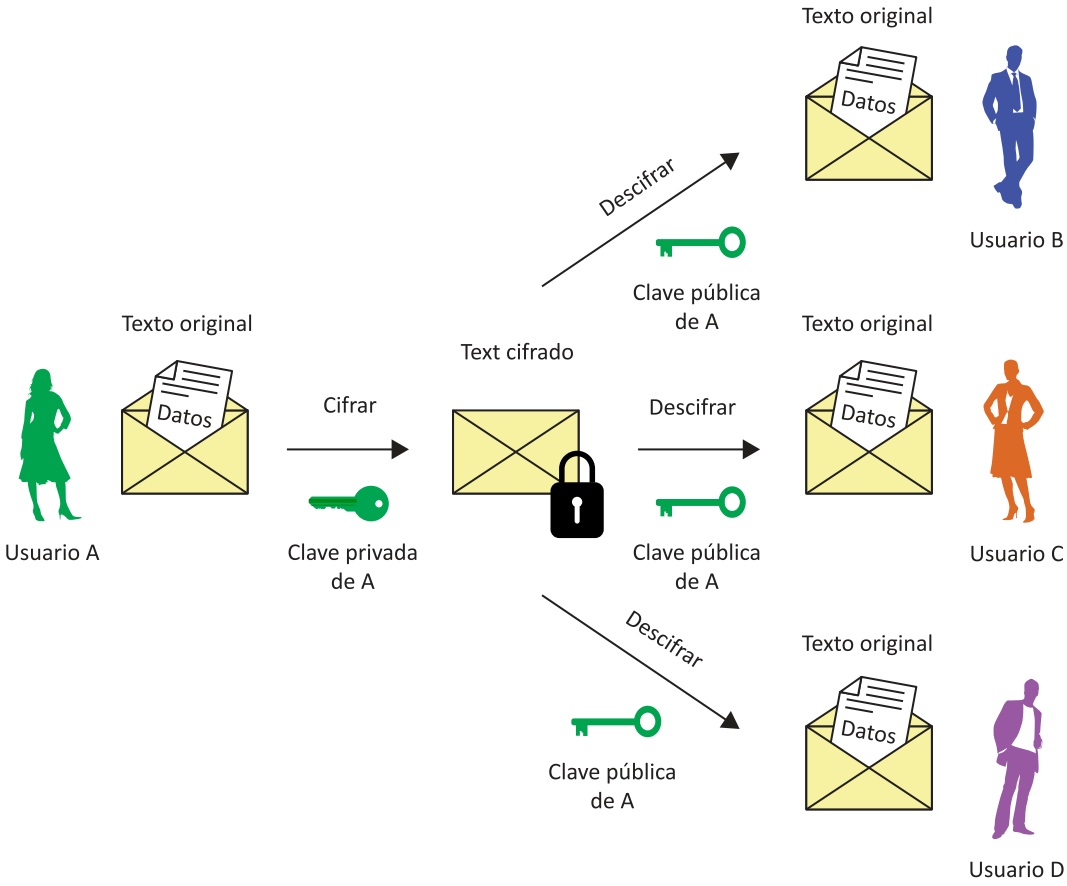
Modelo de cifrado con criptografía de clave pública (para proporcionar confidencialidad)

Este método ofrece confidencialidad ya que el criptograma enviado a un usuario sólo puede ser descifrado con la clave privada del destinatario. El cifrado se realiza mediante la clave pública de dicho destinatario, de forma que desaparece el

problema de la distribución de claves, ya que no se requiere la distribución o transmisión de ninguna clave secreta o privada.

Uso de cifrado de clave pública para proporcionar autenticación

Para proporcionar autenticación, el Usuario_A debe cifrar el mensaje con su clave privada y el Usuario_B deberá descifrar el mensaje con la clave pública del Usuario_A. Este método proporciona autenticación, ya que solo Usuario_A puede haber enviado ese mensaje, pero no proporciona confidencialidad ya la clave pública de Usuario_A es conocida por todos. Por lo tanto, cualquier persona que posea la clave pública de Usuario_A podría descifrar el mensaje



Modelo de cifrado con criptografía de clave pública (para proporcionar autenticación)

Uso de cifrado de clave pública para proporcionar autenticación y confidencialidad

Para proporcionar simultáneamente confidencialidad y autenticación, Usuario_B tendrá que cifrar el texto en claro en primer lugar con su clave privada, lo cual aportará autenticidad. Posteriormente, Usuario_B volverá a cifrar utilizando la clave pública de Usuario_A para proporcionar confidencialidad.

La desventaja del sistema es que es muy lento y complejo ya que se deben realizar dos operaciones de cifrado de clave pública y posteriormente dos operaciones de descifrado. Debe tenerse en cuenta que la longitud de estas claves es grande (1024 bits a 4096 bits).

4.7 Sistema híbrido: Combinando Criptografía Simétrica y Asimétrica

La desventaja de utilizar **cifrado de clave pública** es que es un proceso **bastante lento**, ya que se requieren longitudes de clave grandes (1024 bits a 4096 bits). Cuando se comparan ambos procesos, el **cifrado de clave simétrica** es mucho **más rápido**, y emplea longitudes de clave más pequeñas (56 bits a 256 bits). Por otro lado, como se ha mencionado anteriormente, el uso de criptografía simétrica plantea el problema de la transferencia de clave. Ambas técnicas se pueden utilizar conjuntamente para proporcionar un mejor método de cifrado. De esta manera se puede hacer uso de las ventajas combinadas y superar las desventajas.

Específicamente, el sistema híbrido utiliza un algoritmo de clave pública con el fin de compartir de forma segura la clave usada en el sistema de cifrado simétrico. El texto en claro se cifra utilizando una clave simétrica, dando lugar al criptograma. El emisor envía el criptograma al receptor junto con la clave simétrica utilizada cifrada con la clave pública del destinatario. Dado que el método de reparto es seguro, la clave simétrica se renueva cada sesión, por eso a veces a esta clave se denomina clave de sesión. Esto significa que si un atacante es capaz de conocer la clave de sesión, sólo sería capaz de leer el mensaje cifrado con esa clave.

La clave de sesión cifrada utilizando el algoritmo de clave pública, y el criptograma, se combinan automáticamente. El destinatario usa su clave privada para descifrar la clave de sesión y, a continuación utiliza la clave de sesión para descifrar el mensaje. Muchas aplicaciones utilizan este sistema.

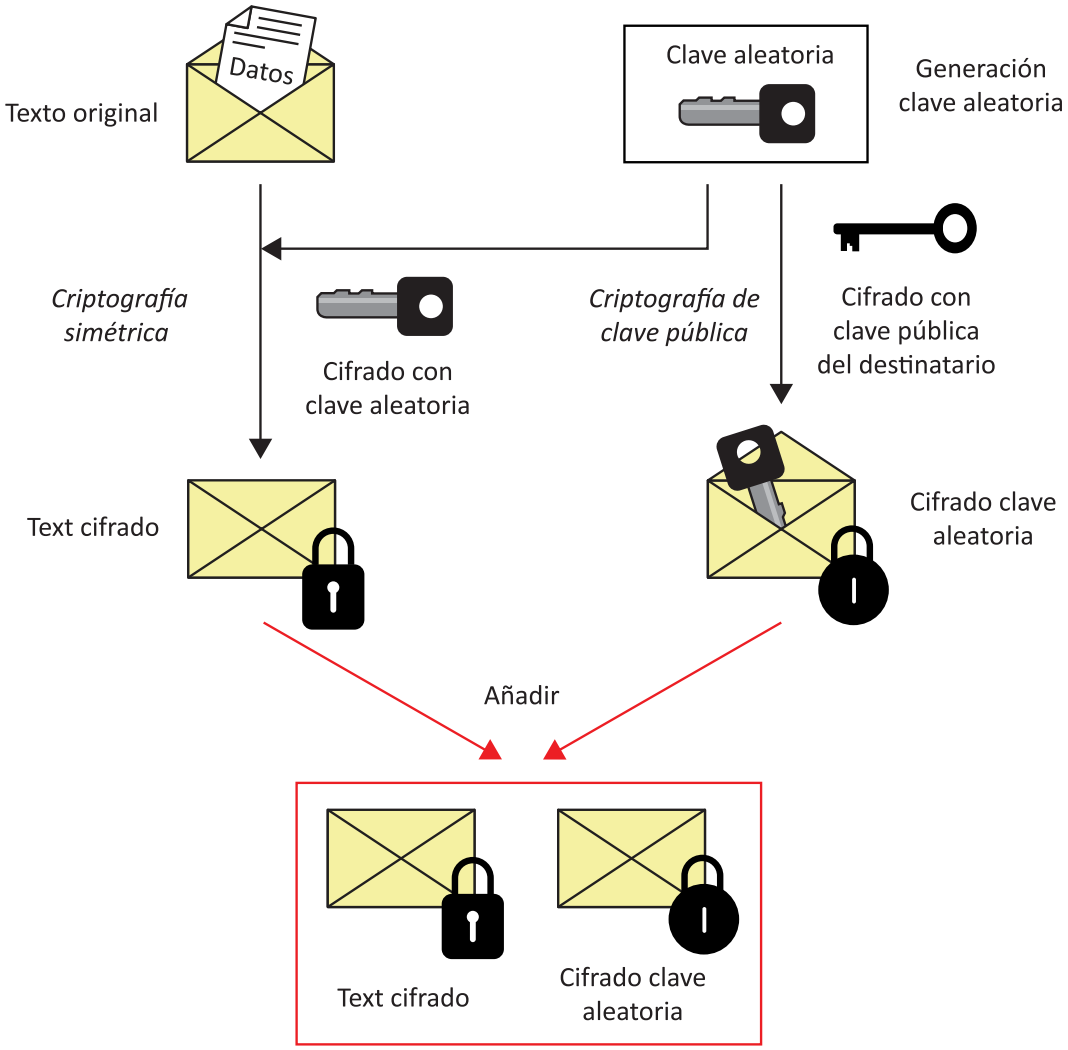
Los pasos que sigue una transacción utilizando una técnica combinada son:

1. Se genera una clave aleatoria y se cifra el mensaje con dicha clave utilizando criptografía simétrica, dando lugar al criptograma.

2. Se cifra esta clave aleatoria mediante criptografía de clave pública con la clave pública del destinatario.

3. Se envía el criptograma junto con la clave aleatoria cifrada tal como se ha mencionado en el apartado anterior.

La siguiente figura ilustra el proceso.



Modelo de cifrado híbrido (para proporcionar confidencialidad)

Esta técnica de cifrado combinado se utiliza con muchísima frecuencia. Por ejemplo, se utiliza en *Secure Shell* (**SSH**) para proteger las comunicaciones entre el cliente y el servidor y en **PGP** *(Pretty Good Privacy)* para enviar correos electrónicos. Además, es el mecanismo básico en *Transport Layer Security* (**TLS**), que es el protocolo utilizado en la Web para mantener un canal de comunicación seguro.

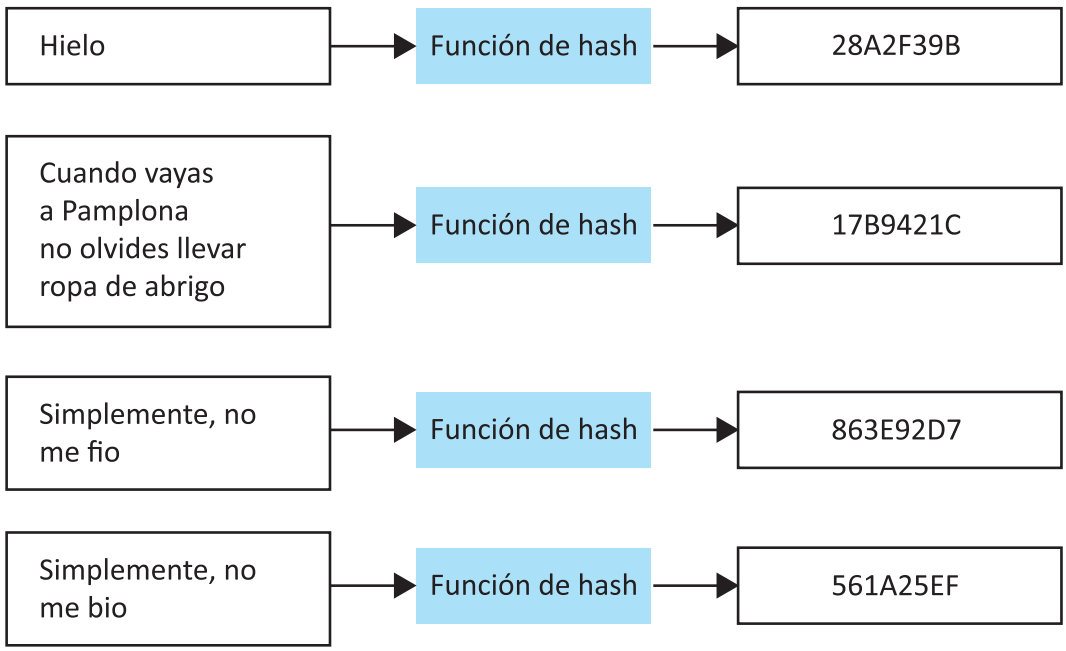
4.8 Funciones de hash

Una función de hash es una transformación que a partir de unos datos de entrada de longitud variable *m* devuelve una secuencia de caracteres de tamaño fijo, conocida como el valor hash h (es decir, $h = H(m)$). Cualquier cambio en los datos de entrada cambia el valor del hash. Las funciones hash con esta propiedad se emplean en computación; cuando se emplean en criptografía, las funciones de hash deben tener algunas propiedades adicionales.

Los requisitos básicos para una función hash criptográfica son:

- La entrada puede ser de cualquier longitud,
- La salida tiene una longitud fija,
- Es fácil calcular el valor hash para cualquier mensaje dado,
- Las funciones hash son unidireccionales, es decir, es computacionalmente imposible generar un mensaje a partir del valor de su hash,
- Es computacionalmente imposible modificar un mensaje sin que su hash también cambie.
- Libre de colisión, es decir, es computacionalmente imposible encontrar dos mensajes diferentes (x, y), tal que H(x) = H(y).

La principal aplicación de una función hash criptográfica es su uso en la firma digital. Además, un hash puede hacerse público sin revelar el contenido del documento a partir del cual se ha generado dicho hash.



Función de hash

4.9 Firma digital

Una firma digital es una firma electrónica que se puede utilizar para autenticar la identidad del remitente de un mensaje o el firmante de un documento. Asimismo, también garantiza la integridad del mensaje.

La firma digital de un remitente para un documento no puede ser generada por ningún otro usuario. La firma digital es una herramienta necesaria para el no repudio; si un usuario recibe un documento firmado por un determinado remitente, este remitente no podrá posteriormente negar que él ha enviado el documento.

Las firmas digitales se basan en las firmas manuscritas, por ello presentaremos en primer lugar las propiedades que estas últimas deben satisfacer:

- Difícil falsificación – cualquier intento de falsificación de la firma debe ser detectado fácilmente.
- La firma facilita la autenticación - la firma identifica de forma exclusiva a su autor.
- La firma es intransferible - la firma es parte de un documento y nadie puede transferir la firma de un documento a otro.
- El documento firmado es inalterable – un documento no se puede modificar después de la firma.
- La firma es innegable – el responsable de la firma no puede negar haber firmado un documento.

En la práctica, ninguna de estas características se cumplen al cien por cien en las firmas manuscritas. Las firmas digitales también deben satisfacer todos esos requisitos.

Sin embargo, aparecen nuevos problemas asociados a aspectos prácticos de la firma digital. Los documentos digitales pueden copiarse fácilmente, parte de un documento se puede transmitir a otro documento y un documento firmado se puede modificar fácilmente. Por lo tanto, se deben formular nuevos requisitos adicionales para una firma digital:

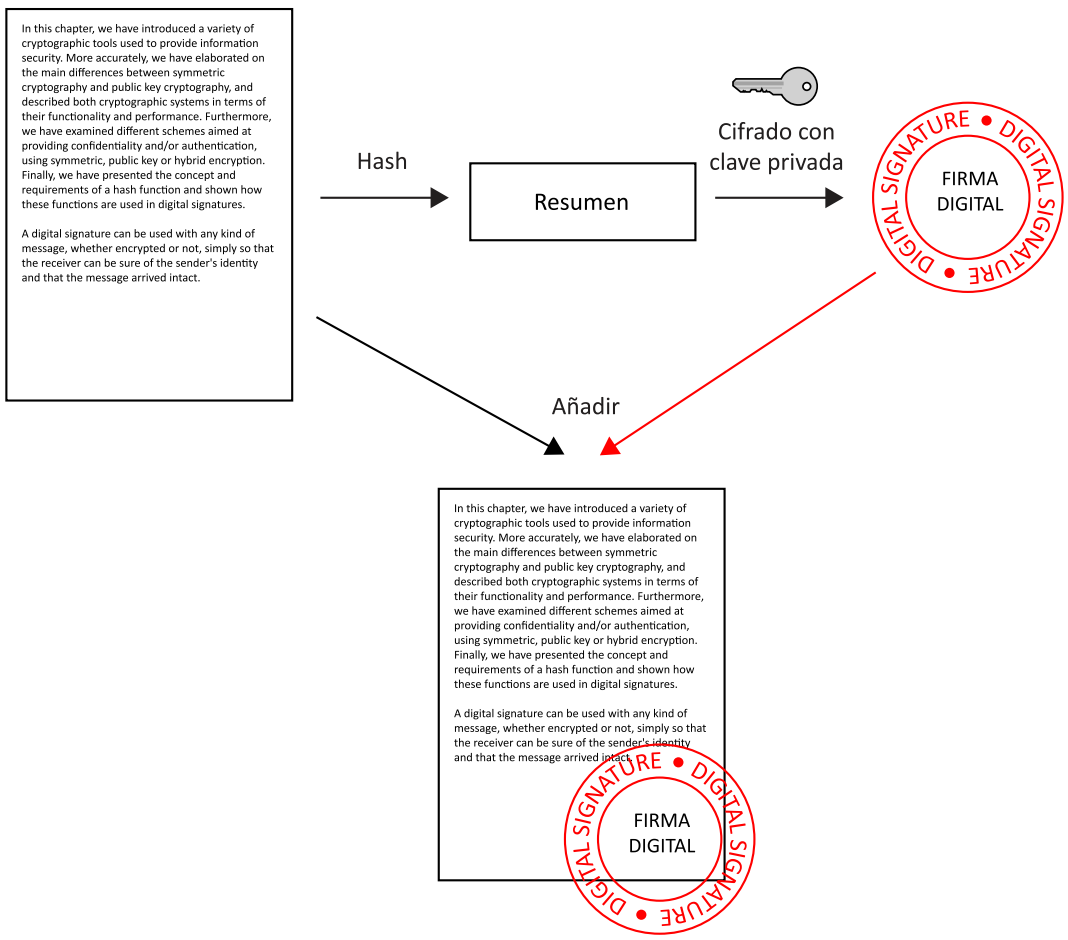
- La firma debe ser un patrón de bits que depende del mensaje firmado.
- La firma deberá utilizar información exclusiva del remitente, para impedir tanto la falsificación como la negación o repudio.
- Firmar digitalmente un documento debe ser relativamente fácil.
- La falsificación de la firma digital, ya sea elaborando un nuevo mensaje para una firma digital existente o generando una firma digital fraudulenta para un mensaje dado debe ser computacionalmente imposible.

- Almacenar una copia de un documento firmado digitalmente debe ser fácil.

Una firma digital se puede utilizar con cualquier tipo de mensaje, ya sea cifrado o no, se trata simplemente que el receptor puede estar seguro de la identidad del remitente y que el mensaje ha llegado intacto (no ha sido modificado).

Hay varios esquemas posibles para firma digital. Uno de los esquemas más aceptados se basa en las funciones hash. En este caso, si un usuario desea firmar digitalmente un documento debe seguir los siguientes pasos:

- Calcular el hash del documento que debe ser firmado.
- Usando criptografía de clave pública, se debe cifrar el hash calculado en el paso anterior con la clave privada del remitente para obtener la firma digital.
- Añadir la firma digital al documento.

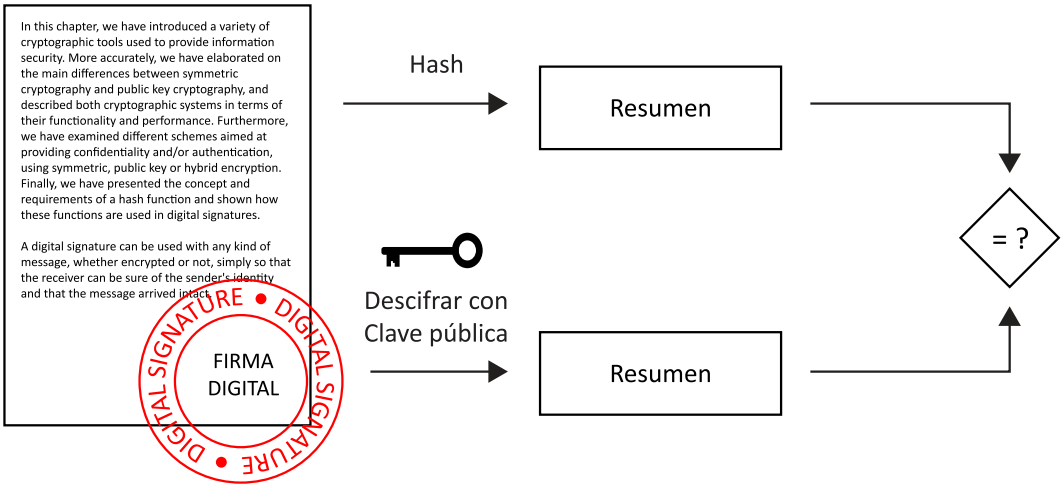


Modelo de firma digital basada en funciones de hash

El receptor puede verificar la autenticidad de esta firma digital siguiendo los siguientes pasos:

- Evaluar el hash del documento (excluyendo la parte de firma digital).

- Usando criptografía de clave pública, descifrar la firma digital con la clave pública del remitente para obtener el hash del mensaje.
- Comparar los resultados obtenidos en los dos pasos anteriores



Proceso de verificación de una firma digital basada en hash

Si los valores de hash obtenidos en los dos pasos son iguales, el destinatario sabe que los datos firmados no han sido modificados, y por tanto, la firma es correcta.

4.10 Resumen

En este capítulo, se han introducido una serie de herramientas criptográficas que se utilizan para proporcionar seguridad de la información. Más concretamente, se ha presentado la criptografía simétrica, la criptografía de clave pública así como sus principales diferencias entre ambos en cuanto a prestaciones. Además, se han mostrado distintos esquemas destinados a proporcionar confidencialidad y/o autenticación, utilizando criptografía de clave simétrica, pública o cifrado híbrido. Por último, hemos presentado el concepto y requisitos de una función de hash y se muestra como estas funciones se utilizan en firmas digitales.

5 Certificados digitales y gestión de claves

5.1 Distribución de claves públicas

Una de las principales aplicaciones de la criptografía de clave pública son las firmas digitales. Una correcta aplicación de firma digital permite al receptor de un documento firmado digitalmente tener la certeza que el mensaje fue enviado por el supuesto remitente. En muchos aspectos, la firma digital es equivalente a la firma manuscrita tradicional, pero una implantación práctica adecuada de la firma digital hace que sea más robusta y difícil de falsificar que la firma manuscrita. Para poder verificar una firma digital es necesario conocer la clave pública del remitente. Por lo tanto, es totalmente necesario un mecanismo de distribución de claves.

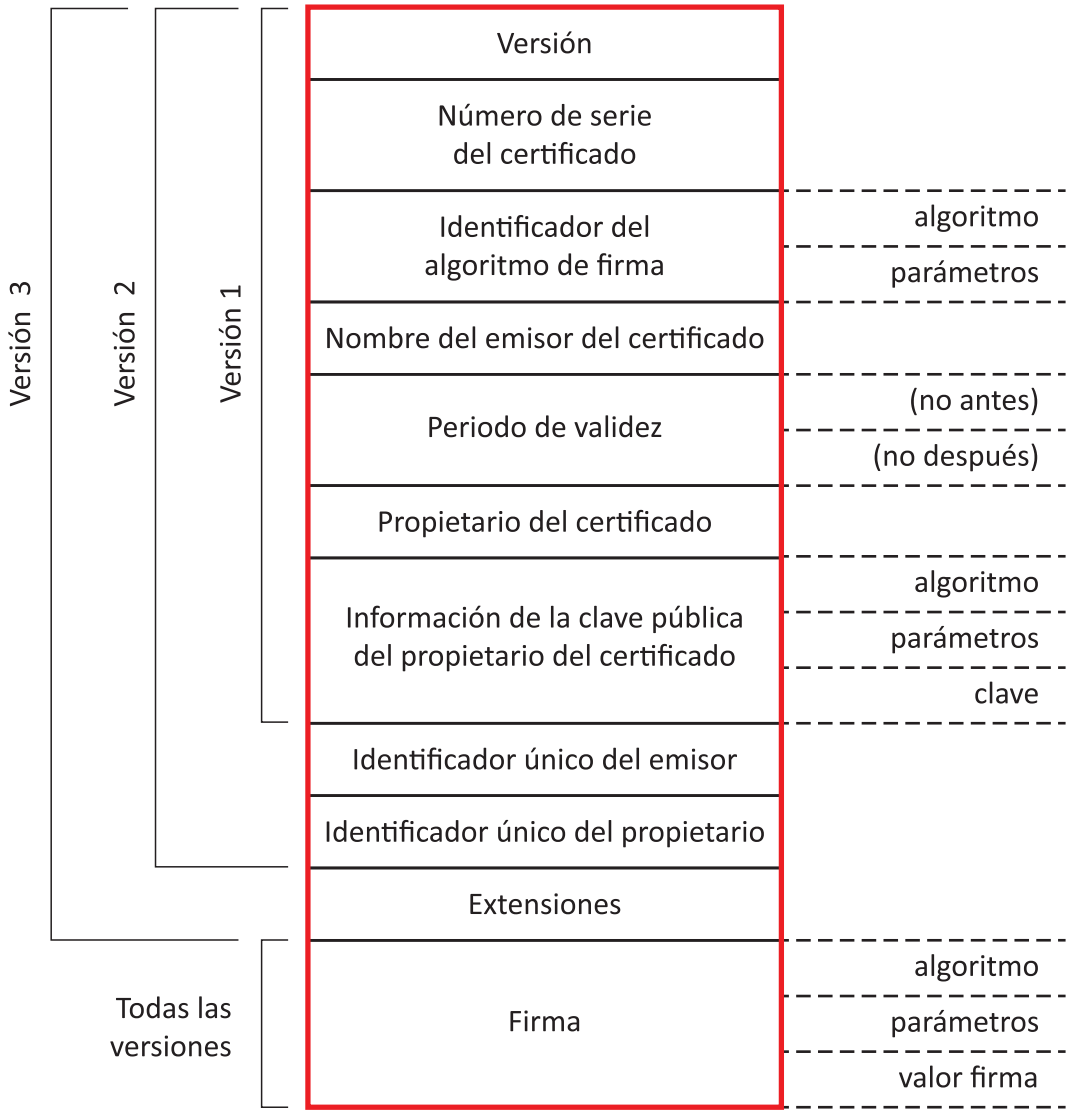
El enfoque más aceptado para la distribución de claves se basa en el uso de certificados digitales.

5.2 Concepto de certificado digital

Un certificado digital es un documento electrónico que incorpora una firma digital para **vincular una clave pública con una identidad** - el nombre de una persona o una organización.

El certificado puede ser usado para verificar que una clave pública pertenece a un individuo. Un certificado digital es una estructura de datos que contiene la clave pública de un usuario o entidad (propietario del certificado), así como los datos de identificación del titular del certificado y una marca relacionada con la validez del certificado. Esta estructura se firma con la clave privada de una entidad de confianza denominada *autoridad de certificación* (**CA**). Cada usuario es capaz de verificar la autenticidad del contenido del certificado utilizando la clave pública de la autoridad de certificación.

La siguiente figura muestra la estructura de un certificado digital:

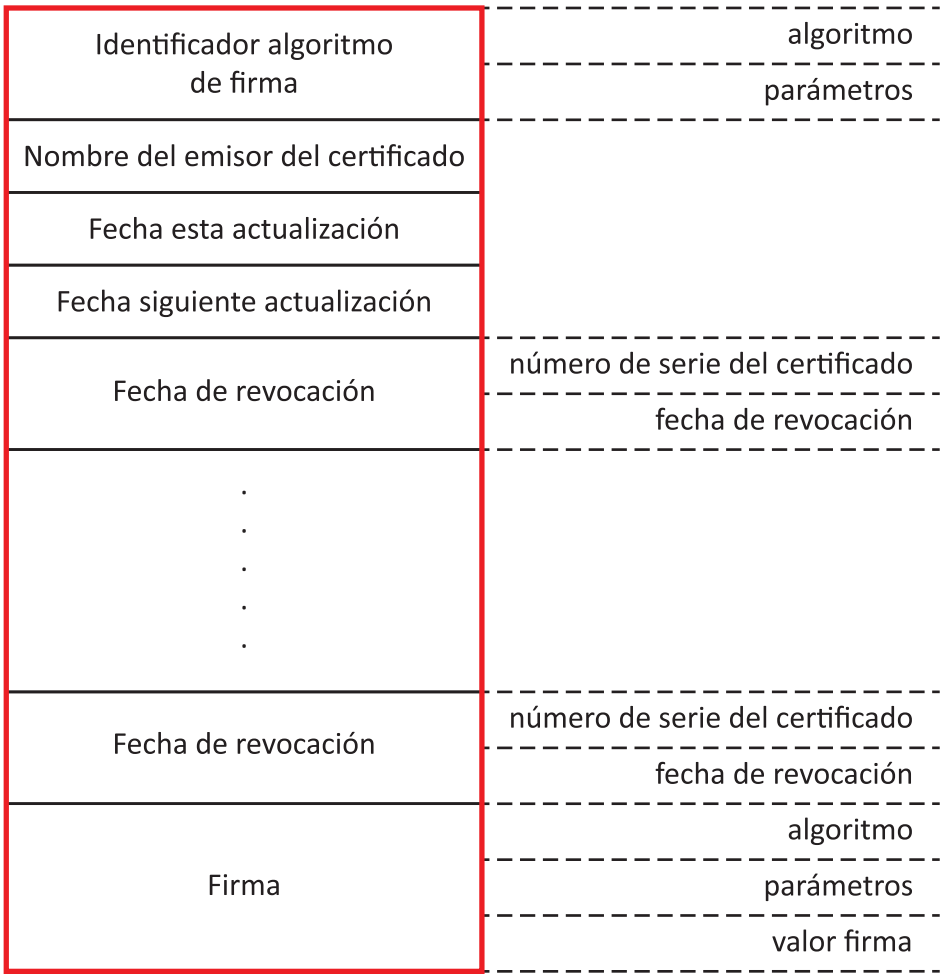


Estructura de un certificado digital

5.3 Mecanismos de revocación de certificados

Un certificado digital puede ser revocado si, por ejemplo, el usuario descubre que su clave privada ha sido perdida o robada. Los certificados también pueden ser revocados si se descubre que la autoridad de certificación (CA) ha emitido incorrectamente un certificado, sin cumplir con los requisitos de la política de seguridad. Revocar un certificado significa pedir su anulación, aunque no haya caducado; sería el proceso equivalente a anular una tarjeta de crédito porque la hemos perdido o nos la han quitado.

El mecanismo más común para verificar si un certificado ha sido revocado se basa en el uso de las *listas de certificados revocados* (**CRL**). Una CRL es una lista de los certificados (o, más específicamente, una lista de los números de serie de los certificados) que han sido revocados, y por lo tanto no se debe confiar en ellos. Las CRL siempre son emitidas por la autoridad de certificación que emitió dichos certificados. Las autoridades de certificación publican periódicamente, a menudo en un intervalo definido, la CRL actualizada. Cada CA por lo tanto necesita una CRL.



Estructura de una lista de certificados revocados (CRL)

5.4 Resumen

En este capítulo, hemos presentado el problema de distribución de claves pública y el uso de certificados digitales como el método más aceptado para resolver este problema. Además, hemos ilustrado el problema de revocación de certificados, y dado detalles de las listas de certificados revocados.

6 Seguridad en servicios de red

6.1 TLS

Transport Layer Security (**TLS**) es un protocolo estándar de Internet que proporciona seguridad de las comunicaciones a través de Internet. El objetivo principal de este protocolo es proporcionar confidencialidad e integridad de datos entre dos entidades que se comunican. Un uso importante de TLS es proteger el tráfico de la World Wide Web permitiendo transacciones seguras de comercio electrónico.

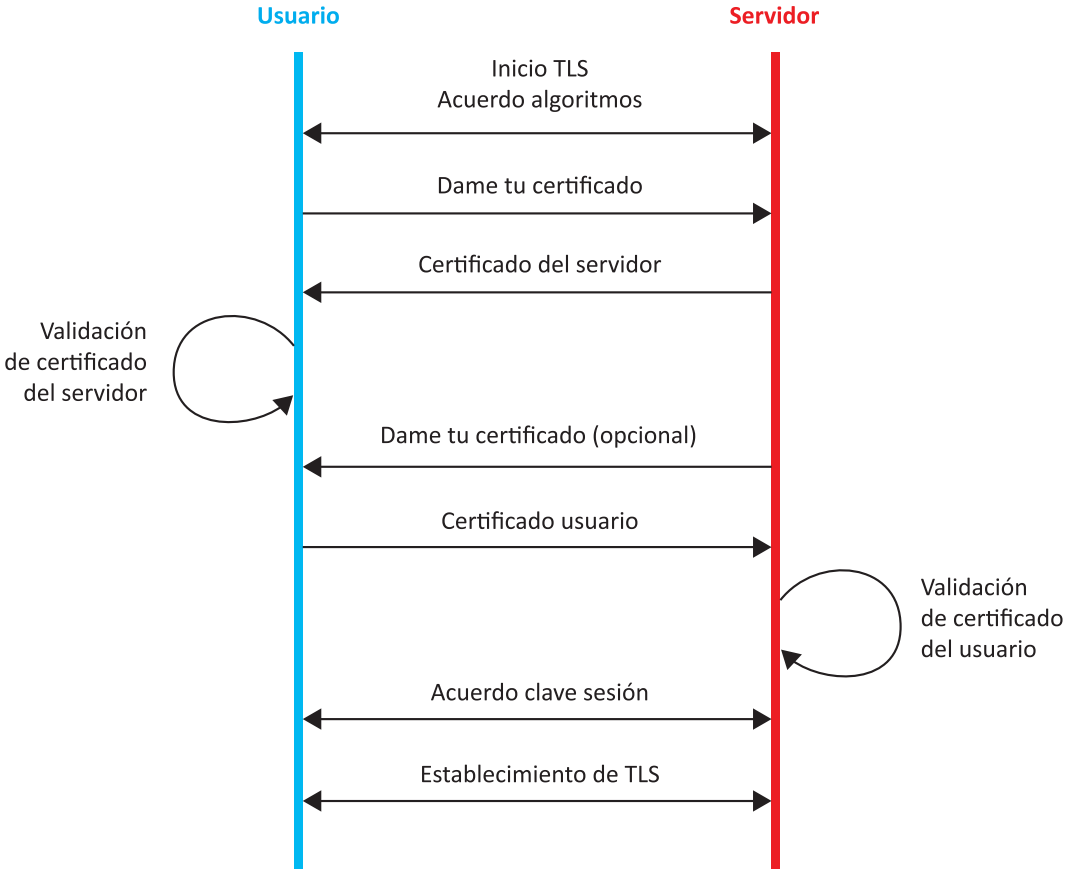
Asimismo este protocolo se utiliza para proteger otras aplicaciones como puede ser el correo electrónico.

TLS se utiliza ampliamente en aplicaciones tales como la navegación web, correo electrónico, fax por Internet, mensajería instantánea y voz sobre IP (VoIP).

TLS se basa en un protocolo anterior, *Secure Sockets Layer* (**SSL**), desarrollado por Netscape Communications. Ambos protocolos (TLS y SSL) utilizan algoritmos criptográficos y certificados de clave pública para verificar la identidad de las entidades que se comunican y para el intercambio de claves simétricas. Esta autenticación puede ser opcional, pero generalmente se requiere para al menos una de las dos entidades comunicantes.

También utilizan cifrado simétrico para ofrecer confidencialidad, y funciones de hash para la integridad del mensaje. La criptografía simétrica se utiliza para el cifrado de datos. Las claves utilizadas en este cifrado simétrico son únicas para cada conexión. La negociación de esta clave es segura y fiable: un atacante ni siquiera interceptando la comunicación podría conseguir la clave simétrica. Además, ningún atacante puede modificar la comunicación sin ser detectado por las partes en la comunicación.

La figura 15 muestra de forma muy simplificada cómo se establece una sesión TLS para una comunicación web segura entre un usuario y un servidor web.



Establecimiento de sesión TLS simplificada

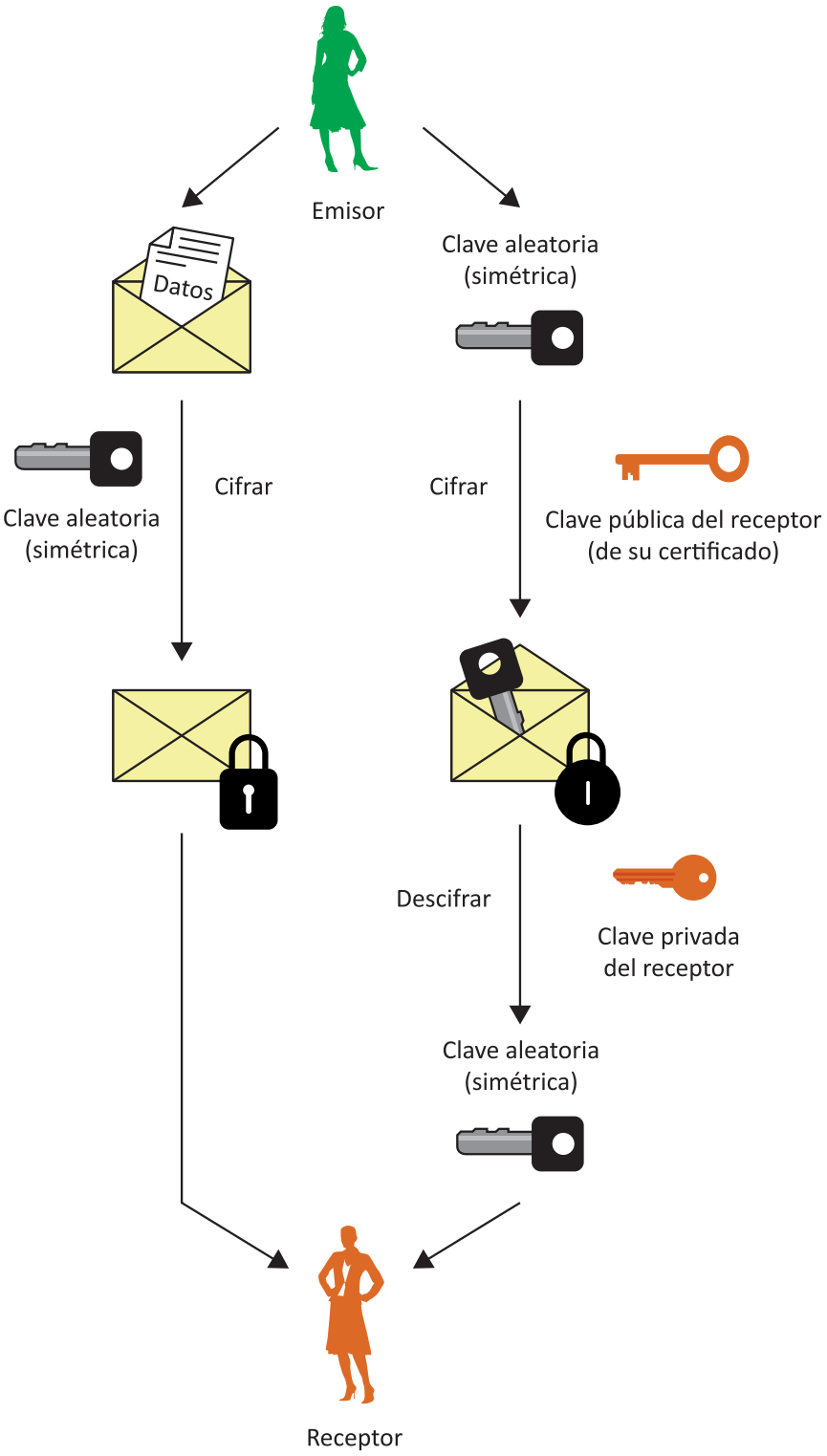
6.2 Seguridad en el correo electrónico

Por lo general, cuando el contenido de un correo electrónico es abierto para cualquier persona. Es decir, como norma general, enviar un correo electrónico es como enviar una postal: cualquier persona que la intercepte puede leer su contenido. Si se quiere que el contenido del correo sea confidencial y/o auténtico, es necesario utilizar técnicas criptográficas. En el caso de la confidencialidad, sólo el destinatario podrá descifrar el mensaje, mientras que el resto de personas vería un galimatías.

Las soluciones más aceptadas para proporcionar seguridad del correo electrónico son **S/MIME** y **PGP**.

S/ MIME es un estándar que ofrece los siguientes servicios de seguridad: autenticación, integridad de mensaje, no repudio de origen (usando firma digital) y la confidencialidad de datos (mediante cifrado). El uso de S/MIME requiere certificados digitales.

La figura 16 muestra como opera S/MIME para ofrecer el servicio de confidencialidad.



Esquema de confidencialidad de S/MIME.

6.3 Resumen

En este capítulo, hemos presentado brevemente dos protocolos seguros (TLS y S / MIME) que utilizan una combinación de clave pública y la criptografía simétrica. En ambos casos, la autenticación se proporciona mediante el uso de certificados digitales, y el cifrado de datos de usuario se lleva a cabo por medio de la criptografía simétrica.

7 Seguridad perimetral

7.1 Introducción a los cortafuegos (firewalls)

Una de las medidas de seguridad en Internet más ampliamente desplegada y conocida es el uso de lo que denominamos cortafuegos o "firewall". Muchas veces ha parecido que los firewall son como una panacea frente a muchos de los problemas de seguridad en Internet. No es así. Los firewalls son una herramienta más en la búsqueda de la seguridad del sistema. El nivel de seguridad que proporciona un firewall puede variar muchísimo, dependiendo incluso de la máquina en la que esté instalado. Cuando se utilizan siempre hay un compromiso entre la seguridad, facilidad de uso, coste, complejidad, etc.

Un firewall o cortafuegos es un dispositivo que se utiliza para proteger la red interna de una organización. Esta protección se lleva a cabo mediante la separación de la red interna del mundo exterior, o Internet. Todos los mensajes que entran o salen de la red interna a través del firewall son examinados para verificar si cumplen las normas de seguridad especificadas en las reglas del firewall.

Antes de instalar un firewall, es preciso definir un conjunto de normas o reglas que constituyen la política de seguridad. Sin este documento no se puede asegurar la red con un firewall.

Un firewall puede hacer dos cosas. Puede bloquear o permitir una comunicación. Por lo general, se permiten todas las comunicaciones de la red interna a la red externa (Internet), pero si la política de seguridad establece una regla impidiendo el paso de un tipo de mensajes, el firewall lo bloqueará. Por ejemplo, a veces se impiden conexiones a sitios que no sean de confianza ni a otros lugares considerados una amenaza para la seguridad o inapropiados para la organización.

7.2 Sistemas de detección de intrusión

Los ataques son cada vez más sofisticados. Al mismo tiempo nos encontramos con más atacantes “noveles” que aunque no tienen una gran habilidad técnica, han encontrado algún mecanismo de ataque a través de la Web. Todo esto hace que proteger la red sea cada vez más difícil. Los *sistemas de detección de intrusión* (**IDS**, *Intrusion detection systems*) aparecieron para dar respuesta al creciente número de ataques a los principales lugares de interés y redes.

Los IDS son una especie de sistema de gestión de seguridad para los ordenadores y redes. Un IDS recopila y analiza información de un ordenador o una red para identificar posibles violaciones de seguridad, incluyendo tanto el mal uso (ataques desde dentro de la organización) como las intrusiones (ataques de fuera de la organización).

Los IDS utilizan técnicas para evaluar una vulnerabilidad. Las funciones de un IDS incluyen:

- análisis de los usuarios y actividades del sistema,
- análisis de las configuraciones del sistema y de sus vulnerabilidades,
- evaluación de un sistema e integridad sus archivos,
- capacidad de reconocer patrones típicos de los ataques,
- análisis de los patrones de actividad anormales,

Un *sistema de detección de intrusos* (**IDS**) inspecciona toda la actividad entrante y saliente por la red e identifica patrones sospechosos que pueden identificar un ataque de alguien que trata de entrar o comprometer un sistema.

Hay varias formas de clasificar un IDS:

Detección de mal uso y detección de anomalías

- **Detección de mal uso**: el IDS analiza la información que recopila y la compara con grandes bases de datos de firmas de ataques. Esencialmente, el IDS busca un ataque específico que ya se ha documentado. La técnica de detección de intrusos basada en firma de ataque consiste en la búsqueda de "firmas" (secuencias de acciones típicas de un ataque) en todas las comunicaciones que pasan por la red. Igual que ocurre con los sistema de detección de virus, la calidad del software de detección depende de la base de datos de firmas de ataque utilizada, por lo que se necesita una actualización frecuente de esta base de datos.
- Detección de anomalías: el administrador del sistema define el estado normal de tráfico de la red, protocolos y tamaños típicos de los intercambios. El detector de anomalías compara el estado en cada momento con el estado

normal y a partir de las diferencias se buscan anomalías de comportamiento, que pueden ser debidas a algún ataque.

Basados en red o basados en equipos

- *Basados en red, (***NIDS***, Network-based system)*: se analizan las comunicaciones que se intercambian por la red. El NIDS puede detectar mensajes maliciosos diseñados de forma que las reglas de filtrado de un firewall no lo detecten.
- *Basados en equipo (***HIDS***, Host-based system)*: el IDS analiza toda la actividad en cada equipo individual.

Sistemas pasivos o sistemas reactivos

- **Sistema pasivo**: el IDS detecta un posible fallo de seguridad, registra la información y envía las señales de alerta.
- *Sistema reactivo*: el IDS responde a una actividad sospechosa cerrando la sesión de un usuario o reprogramando el firewall para bloquear el tráfico de red que tiene su origen en una entidad sospechosa.

La figura 17 muestra un diagrama de una red incluyendo un firewall y un IDS

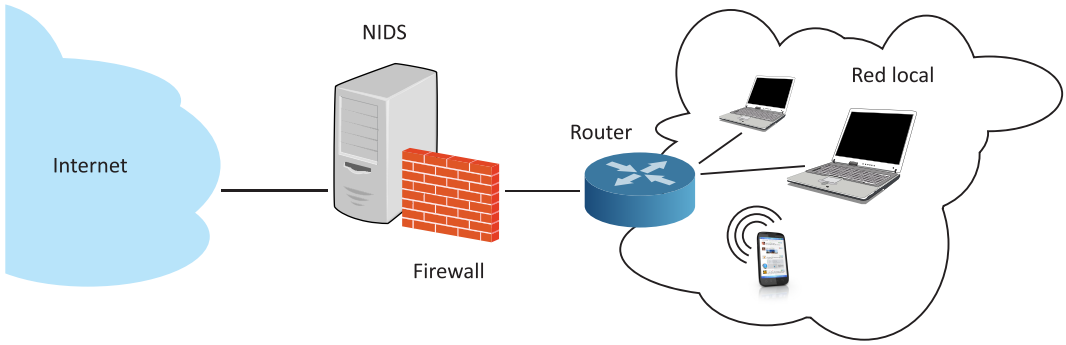


Diagrama con firewall e IDS

Un IDS se diferencia de un firewall en que este último limita el acceso entre redes con el fin de prevenir la intrusión y no indican un ataque desde el interior de la red. Un IDS evalúa una posible intrusión una vez que ha tenido lugar y señaliza una alarma. Asimismo, el IDS también analiza los posibles ataques que se originan dentro de un sistema.

7.3 Resumen

En este capítulo, hemos hablado de las típicas soluciones adoptadas para proporcionar seguridad perimetral. La seguridad perimetral es un conjunto de políticas de seguridad de hardware, software y reglas que proporcionan niveles de protección contra la actividad maliciosa remota. Se han descrito las principales características de cortafuegos y de los sistemas de detección de intrusos. Asimismo se han presentado diversos criterios de clasificación de los IDS.

8 Seguridad en redes inalámbricas

8.1 Redes inalámbricas

Las redes inalámbricas *(Wireless networks*, **WLAN**) gozan actualmente de gran popularidad ya que permiten la movilidad de los usuarios y de los equipos dentro del área de cobertura de la red. Estas redes permiten la conexión a Internet en casi todas partes y ofrecen servicios de comunicación de voz y datos.

Las comunicaciones inalámbricas presentan grandes posibilidades, pero también suponen un alto riesgo de seguridad derivados de la facilidad de acceso a la señal radio en el rango de cobertura de red inalámbrica. Por eso, la seguridad en las conexiones inalámbricas son un tema de gran actualidad.

La seguridad en WLAN implica las siguientes tareas:

- *garantizar la confidencialidad* o cifrado del contenido de la comunicación,
- *autenticación* de *usuario* o control de acceso a la red.

Es necesario tener en cuenta que casi todos los tipos de ataques en redes WLAN se realizan desde la red interior

8.2 Seguridad en redes inalámbricas

La seguridad en redes inalámbricas exige estos servicios:

- **autenticación,**
- **confidencialidad,**
- **gestión de claves.**

La autenticación es el proceso mediante el cual los usuarios se asocian a la red inalámbrica (wireless LAN, WLAN). Así pues, sólo tras una correcta autenticación se permite la asociación de usuarios a la red.

La confidencialidad en las redes WLAN se realiza mediante el uso de algoritmos criptográficos. Los algoritmos más utilizados son **RC4** (**WEP**) y **AES** (**WPA2**).

La gestión de claves incluye la generación de claves y su distribución.

8.3 Protocolo WEP

El Protocolo **WEP** *(Wired Equivalent Privacy)* se utiliza como un complemento opcional del estándar IEEE 802.11a/g/b. Está diseñado para ofrecer los servicios de control de acceso a una WLAN y para garantizar la confidencialidad de los datos transferidos. Incluye los siguientes mecanismos de seguridad:

- autenticación,
- confidencialidad.

- **Autenticación WEP**
  La autenticación de WEP se puede hacer de las siguientes dos maneras:
  - autenticación abierta,
  - clave compartida.

Los sistemas de autenticación abierta usan solo identificador de red SSID. SSID no es una contraseña password; es sólo un identificador de red inalámbrica. El punto de acceso inalámbrico (*Wireless access point* (**WAP**)) difunde este identificador de forma periódica, con intervalos de pocos segundos.

En este modo de autenticación, el usuario envía una trama de autenticación 802.11, que contiene datos de identificación del usuario. El protocolo verifica al usuario y envía una trama confirmando o denegando el acceso a la red inalámbrica.

La autenticación con clave WEP compartida usa una clave compartida de 40 bits, que es la misma para todos los usuarios de la red inalámbrica. Dicha clave es distribuida de forma secreta. El proceso de autenticación verifica la identidad del usuario.

- **Cifrado WEP**

El protocolo WEP utiliza el algoritmo de cifrado simétrico RC4, con claves de 64 o 128 bits. La clave contiene una parte secreta cuya longitud es de 40 bits o 104 y un *vector de inicialización IV* de 24 bits.

El protocolo WEP no es resistente contra los ataques conocidos (monitorización de actividad, ataque de fuerza bruta, ataque de repetición, etc. ...) y el algoritmo RC4, tal como se emplea en WEP, se rompió en 1996.

8.4 Protocolo WPA

El Protocolo ***WPA (Wi-Fi Protected Access)*** es un protocolo aceptado en 2002 para eliminar las vulnerabilidades del protocolo WEP. Este protocolo fue adoptado como una solución temporal, porque en ese momento se trabaja en un nuevo estándar, el IEEE 802.11i (que fue aprobado en 2004). El protocolo WPA contiene un subconjunto de las prestaciones del estándar 802.11i, de forma que se favoreciese la compatibilidad.

Como el protocolo WEP, WPA utiliza también el algoritmo criptográfico RC4, pero incorpora nuevos mecanismos de seguridad. Las partes principales del protocolo WPA son:

- *Temporary Key Integrity Protocol* (**TKIP**),
- *Message Integrity Check* (**MIC**),
- Control de acceso basado en el estándar 802.1x con el protocolo **EAP** (*Extensible Authentication Protocol*).

8.5 Protocolo 802.11i (WPA2)

El Estándar 802.11i, también conocido como WPA2, combina los mecanismos de 802.1x y de TKIP. El algoritmo criptográfico utilizado es AES con longitud de bloque de 128 bits.

Desde un punto de vista estructural, el estándar 802.11i tiene una estructura similar a WPA y tiene prestaciones adicionales, por ejemplo, el protocolo CCMP y los mecanismos de preautenticación que permiten que la itinerancia entre puntos de acceso sea rápida y segura.

Los principales mecanismos y servicios de seguridad del estándar 802.11i son:

- confidencialidad,
- autenticación,
- integridad.

8.6 Resumen

En este capítulo se han presentado los riesgos de seguridad derivados del uso de comunicaciones inalámbricas. En el caso de redes inalámbricas, se han adoptado diversas soluciones de seguridad, aunque alguna de ellas, por ejemplo, el protocolo WEP son vulnerables a un conjunto de ataques. La solución más aceptada para ofrecer los requisitos de seguridad necesarios en este entorno es el estándar 802.11i también conocido como WPA2.

9 Resumen

Este documento contiene una visión global de diversos aspectos relacionados con la seguridad de la información y la seguridad en redes de comunicación. El documento está dividido en ocho bloques temáticos.

El primero es una introducción que trata de motivar al lector sobre la necesidad de proteger los datos y las redes de comunicaciones. Se presentan algunas de las razones que provocan que las redes sean inseguras, así como diferentes protecciones básicas que un usuario debería adoptar para proteger sus datos. Además se incluye una sucinta clasificación de los tipos de ataques.

La segunda parte está dedicada al software malicioso y a los programas antivirus. Básicamente se introduce el concepto de software malicioso y se clasifica de acuerdo a diversos criterios: método de propagación, de instalación, características principales,... Además, el capítulo describe diversas técnicas para limpiar un ordenador infectado. Dado que estas técnicas requieren en primer lugar detectar el software malicioso, se introducen los mecanismos habituales para poder llevar a cabo dicha detección. Asimismo, el documento contiene información básica sobre software antivirus y se enfatiza en la necesidad de mantener dicho software actualizado.

La tercera parte se orienta a los servicios y mecanismos de seguridad. Se presentan los servicios de seguridad más relevantes (confidencialidad, integridad, disponibilidad, autenticación, control de acceso, no repudio y privacidad) junto con los mecanismos necesarios para poder ofrecer dichos servicios. Finalmente, se establece el mapeo entre los servicios y los mecanismos de seguridad correspondientes.

La cuarta parte contiene información básica sobre una variedad de herramientas criptográficas que permiten proteger la información. Se presentan las principales diferencias entre criptografía simétrica y criptografía de clave pública y se describen ambos tipos de algoritmos de acuerdo con su funcionalidad y prestaciones. Por último, se introducen el concepto de función de hash criptográfica, sus requisitos y se muestra como se usan estas funciones en las firmas digitales.

El quinto bloque pone de relieve el problema de la distribución de las claves públicas. Se introduce el concepto de certificado digital, ya que es la forma más habitual de solventar este problema. Además, se ilustra brevemente el problema de la revocación de claves.

El capítulo sexto incluye una breve descripción de dos de los protocolos de seguridad más extendidos: TLS y S/MIME. Ambos esquemas usan una combinación de criptografía simétrica y criptografía de clave pública y requieren el uso de certificados digitales.

El séptimo bloque trata el tema de la seguridad perimetral. Se presentan los componentes básicos (firewalls y sistemas de detección de intrusión). Además, se establece una clasificación de los IDS de acuerdo a distintos criterios.

Finalmente, la parte octava está orientada a los riesgos de seguridad inherentes al uso de redes de comunicación inalámbricas. Se muestran de forma muy esquemática algunas de las distintas soluciones que han sido adoptadas, aunque algunas de ellas como el protocolo WEP son vulnerables a diversos ataques. La solución más aceptada para ofrecer los distintos requisitos de seguridad existentes en este entorno es el estándar 802.11i, también conocido como WPA2.