Internet. Funcionamiento, aplicaciones y seguridad

PID_00250489

Joan Antoni Pastor Collado
Eduard Elias Vila

Tiempo mínimo de dedicación recomendado: 3 horas

Universitat Oberta de Catalunya

Índice

Introducción..... 5

Objetivos..... 6

1. Orígenes de la red internet..... 7

2. El funcionamiento de la red..... 10
2.1. El modelo cliente-servidor 10
2.2. La arquitectura de internet 11

3. Servicios y aplicaciones de internet..... 15
3.1. Acceso a internet 15
3.2. Sistema de nombre de dominio 15
3.3. El servicio WWW 16
3.4. Los buscadores 17
3.5. El correo electrónico 18
3.6. *Cloud computing*..... 20

4. La seguridad en internet..... 22
4.1. Fundamentos de criptografía 23
4.2. Firmas digitales 27
4.3. Certificados digitales e infraestructuras de clave pública 28
4.4. Perspectivas de futuro en materia de seguridad en internet 33
4.5. Soluciones cuánticas al problema de la seguridad 35

Resumen..... 36

Glosario..... 37

Bibliografía..... 39

Introducción

En este módulo didáctico daremos unas nociones básicas de internet desde un punto de vista tecnológico. Estas nociones técnicas nos permitirán entender un poco más el funcionamiento de la red y sus aplicaciones, de manera que las posibles actuaciones jurídicas con claras connotaciones tecnológicas puedan tener una base más fundamentada.

Describiremos los orígenes de internet: cuándo, cómo y por qué se creó la red. Es importante entender los objetivos iniciales, ya que algunas decisiones de diseño tomadas en aquel momento todavía condicionan ahora algunos aspectos de la red, como por ejemplo la seguridad.

Veremos que hoy en día internet es una red de ordenadores que interconecta millones de máquinas por medio de miles de redes. Describiremos el modelo cliente-servidor, que es el modelo de diseño de aplicaciones informáticas que ha hecho posible la expansión de la red. También veremos someramente cuáles son los protocolos que permiten que internet funcione y qué ventajas e inconvenientes aportan.

Veremos las características técnicas de algunas de las aplicaciones más importantes que se utilizan en la red, como el correo electrónico, la WWW y el sistema de nombres de dominio.

Para terminar, hablaremos sobre la seguridad en internet. Veremos cómo la criptografía se puede utilizar para lograr niveles de seguridad aceptables, explicaremos el funcionamiento de las firmas digitales y la necesidad de utilizar los certificados digitales para que las firmas digitales garanticen todas sus propiedades. Asimismo, haremos una breve descripción de la amenaza que pueda suponer, en este aspecto, la computación cuántica y las soluciones que ya están apareciendo.

Objetivos

Los materiales didácticos de este módulo deben permitir alcanzar los siguientes objetivos:

1. Conocer la historia de internet y ver cuáles eran los objetivos en su creación y cómo condicionaron su diseño.

2. Entender el modelo cliente-servidor y el funcionamiento general de los protocolos que sustentan la red internet.

3. Conocer el funcionamiento de algunos de los servicios y aplicaciones más relevantes que hay en la red.

4. Conocer los conceptos básicos de la seguridad de la información y cómo la criptografía permite conseguirlos.

5. Comprender qué es técnicamente una firma digital y qué papel tienen los certificados digitales en un esquema de firma digital.

6. Estar preparados para comprender lo que puede suceder en el campo de la seguridad en internet cuando se concrete la irrupción de la computación cuántica.

1. Orígenes de la red internet

Los orígenes de internet se remontan al año 1962, cuando en la Advanced Research Projects Agency (ARPA) se empezó a hablar de conectar diferentes ordenadores de manera que todo el mundo pudiera tener un acceso rápido a la información. En esa misma época, en 1964, de la mano de investigadores del Massachusetts Institute of Technology (MIT), aparece el primer artículo científico sobre la teoría de la conmutación de paquetes. Esta teoría establece un sistema de transmisión de la información basado en la fragmentación de esta en partes más pequeñas, los paquetes, y el envío posterior de estos paquetes de manera independiente. Esta independencia en el envío de los paquetes hace que el camino que toma cada uno para ir desde el emisor hasta el receptor pueda ser diferente. La teoría de conmutación de paquetes representó un cambio respecto a los sistemas de comunicación que había hasta ese momento, que utilizaban la conmutación de circuitos, en la que se establece un circuito o camino fijo entre emisor y receptor, por donde circula ordenadamente toda la información.

Para entender claramente la diferencia entre la conmutación de paquetes y la conmutación de circuitos podemos establecer el símil de comunicación siguiente. Imaginemos que un autor quiere enviar, desde su casa, el libro que ha escrito a la editorial donde trabaja su editor. Para hacer el envío del libro puede hacer dos cosas:

Llamar un taxi para que recoja el libro en su casa y lo lleve a la editorial.

Llamar a cinco mensajeros diferentes para que cada uno de ellos lleve un capítulo diferente del libro hasta la editorial.

En el primer caso, toda la información circulará por un mismo camino (el que decida el taxista) y llegará a la vez y por orden (todos los capítulos del libro, uno tras otro). Esto es lo que ocurre con una conmutación de circuitos.

En el segundo caso, cada capítulo del libro circulará por un camino diferente (el que cada mensajero elija) y, por tanto, puede que lleguen en diferente orden del que el autor los ha enviado, según el recorrido y el tráfico que haya encontrado cada mensajero. Este sería un ejemplo de conmutación de paquetes, en el que cada paquete representa un capítulo del libro.

Telefonía sobre internet

Si se entiende la diferencia entre conmutación de paquetes y de circuitos, se puede comprender por qué una llamada telefónica tiene más calidad cuando se hace por medio de la red telefónica que cuando se hace utilizando internet.

Las principales ventajas de la conmutación de paquetes con respecto a la de circuitos son la mejora del rendimiento de la red, ya que no necesitamos tener una conexión continua entre dos ordenadores, sino que tan solo hay que establecer las conexiones necesarias para transmitir cada uno de los paquetes de manera independiente. A pesar de esta ventaja, la conmutación de paquetes tiene algún inconveniente, como, por ejemplo, el hecho de que se incluyan pequeños retrasos en la comunicación. Estos retrasos están generados por el hecho de que cada paquete puede tomar un camino diferente y, por tanto, puede que no lleguen en el mismo orden en que han sido enviados. En este caso, habrá un proceso de ordenación de los paquetes para que la información pueda ser entregada exactamente tal como ha sido enviada. Así, para las comunicaciones en tiempo real, es decir, aquellas en las que se necesita inmediatez, como la telefonía o la videoconferencia, la conmutación de paquetes

no resulta muy adecuada si no se dispone de una infraestructura de comunicación de alta velocidad, aunque en la actualidad la velocidad disponible mayoritariamente en la red compensa.

Ataques nucleares

Otra propiedad de la conmutación de paquetes es la robustez que representa el hecho de que la eliminación de un nodo de la red no detiene una comunicación, sino que simplemente la redirecciona y pasa por otro camino. Curiosamente, se había creído que ARPANET fue una red diseñada para resistir ataques nucleares, pero la realidad es que esta resistencia a los ataques nucleares provenía de la robustez de la conmutación de paquetes, pero no era uno de los objetivos del diseño de la red.

Basándose en esta nueva técnica de conmutación de paquetes, al final de los años sesenta se creó la red ARPANET, una red que en los orígenes interconectaba cuatro centros universitarios (University of California - Los Angeles, Stanford University, University of California - Santa Barbara y University of Utah).

Al principio de los años setenta se hicieron las primeras demostraciones públicas de ARPANET junto con una de sus aplicaciones estrella: el correo electrónico.

La transformación de ARPANET en la red internet que conocemos hoy en día comenzó con el intento de superación de las limitaciones de ARPANET en cuanto que era una red con un diseño arbitrario. Para crear una red de redes, como pretendía ser internet, era necesario establecer la idea de interconexión de múltiples redes independientes, cada una posiblemente con características de diseño y desarrollo diferentes. De acuerdo con estas ideas se empezó a trabajar en 1972 para modificar el protocolo NCP (*network control protocol*), que se utilizaba en ARPANET, y así surgió el protocolo TCP/IP. Este tenía que seguir cuatro principios básicos:

1) Cada red tiene que funcionar por sí sola y no se debe hacer ningún cambio interno para conectarla a internet.

2) Las comunicaciones se llevarán a cabo sobre la base de la técnica del mejor esfuerzo[1], es decir, si un paquete no llega a su destino, se volverá a enviar.

(1)En inglés *best effort*.

3) Se utilizarán cajas negras para conectar las redes. El funcionamiento de estas cajas será lo más simple posible y no se almacenará información que circule.

4) No podrá haber un control global de las operaciones.

Enrutadores

Estas cajas negras son lo que conocemos como *enrutadores* (en inglés, *routers*).

En septiembre de 1973 V. Cerf y R. E. Kahn presentaron el protocolo TCP/IP en el International Network Working Group. Una de las filosofías seguidas para el desarrollo de este protocolo era la de diseñarlo de manera que su utilización no interfiriera excesivamente en el funcionamiento de las aplicaciones o programas informáticos. Este hecho tiene ventajas e inconvenientes.

La ventaja principal está en que aplicaciones nuevas se han podido desarrollar sobre el protocolo, como es el caso de la WWW, creado por T. Berners-Lee en el CERN de Ginebra, a finales de los años ochenta. Pero, por otra parte, algunas decisiones concretas tomadas en el diseño del protocolo TCP/IP implican que haya aplicaciones que funcionan mejor que otras.

Finalmente, cabe hacer notar que la filosofía inicial de internet, y en concreto la del protocolo TCP/IP, iba encaminada a la compartición y libre circulación de información entre los usuarios de la red. Por tanto, en este entorno no tenía sentido poner ningún tipo de restricciones en cuanto a accesos y seguridad. Por este motivo, se argumenta que internet, tal como la conocemos hoy en día, tiene una carencia estructural en cuanto a temas de seguridad.

2. El funcionamiento de la red

Internet está formada por muchos ordenadores de diferentes plataformas y sistemas y con diferentes funciones y utilizaciones.

En este apartado hablaremos de la arquitectura cliente-servidor, en qué consiste y qué propiedades aporta. Por otro lado, analizaremos la arquitectura de internet y veremos el protocolo TCP/IP, sobre el que funciona internet, para poder entender mejor las especificidades de las aplicaciones y la estructuración y circulación de la información por la red.

2.1. El modelo cliente-servidor

No hace mucho tiempo, los sistemas informáticos se basaban en un ordenador central al que se conectaba una serie de terminales. Estos terminales actuaban como terminales tontos, en inglés *dump terminals*, ya que toda la carga computacional del sistema recaía sobre el ordenador central y los terminales solo actuaban como dispositivos de salida de información (por medio de una pantalla) y de entrada (por medio de un teclado).

Estos sistemas tienen una serie de inconvenientes. Por ejemplo, el dimensionamiento de los sistemas centralizados es delicado, ya que el incremento de terminales que trabajan sobre el ordenador central implica un aumento de carga de trabajo sobre este y, por tanto, para mantener el rendimiento hace falta ampliar sus capacidades. Por otro lado, la centralización de los procesos implica, igualmente, una concentración de masa crítica, lo que implica que el mal funcionamiento del ordenador central repercute en todos los terminales que están conectados.

La seguridad

A pesar de los inconvenientes de los sistemas centralizados, desde un punto de vista de seguridad, los sistemas centralizados son, *a priori*, más seguros que los distribuidos, ya que tienen el control de toda la información y de todos los procesos para tratarla.

La aparición de los ordenadores personales con una capacidad de proceso y almacenamiento de datos hizo que los sistemas centralizados fueran perdiendo peso. Había que aprovechar las capacidades de los nuevos terminales, por lo que los ordenadores centrales se liberaban de trabajo y dejaban que lo hicieran los terminales. De esta manera los ordenadores centrales se fueron transformando en ordenadores que servían información al resto para que la procesaran como les conviniera. Este tipo de arquitectura es la que se conoce como modelo cliente-servidor.

Internet se basa en una arquitectura cliente-servidor, ya que la mayoría de las aplicaciones y los servicios que podemos encontrar siguen este modelo. La parte servidor espera permanentemente recibir peticiones del cliente. Cuando el cliente genera una petición, el servidor sirve la información o servicio que el cliente ha solicitado.

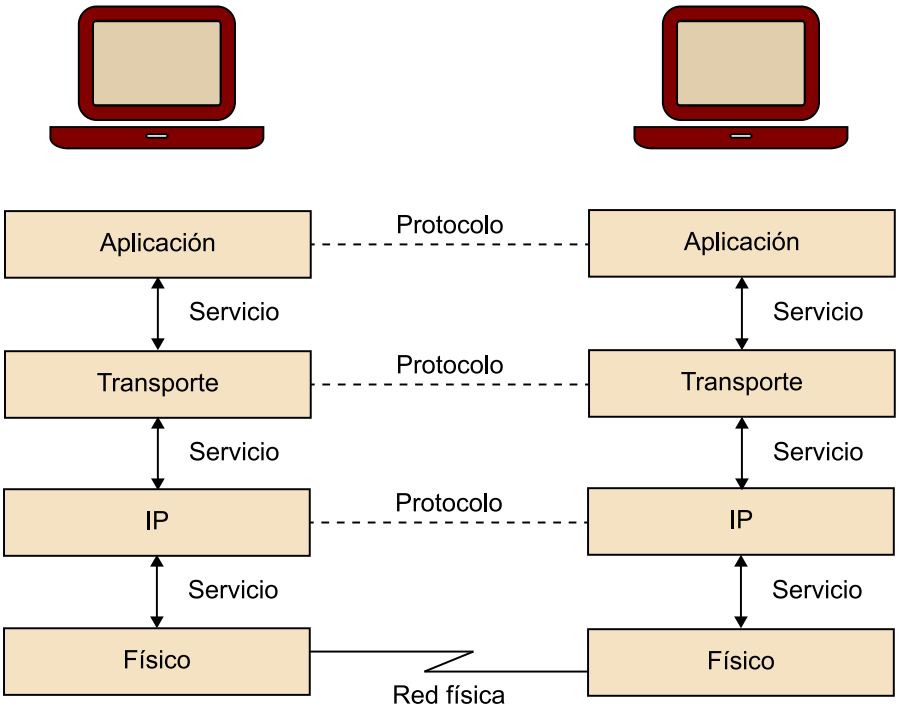
Un ejemplo de aplicación cliente-servidor lo encontramos en el correo electrónico. Un servidor de correo electrónico es el encargado de recibir y enviar los mensajes de los usuarios, mientras que el cliente de correo electrónico (el programa que utilizamos los usuarios finales de la aplicación, como por ejemplo Microsoft Outlook o Thunderbird) es el encargado de pedir al servidor que nos entregue los mensajes que han llegado a nuestro nombre, nos permite leerlos y también escribir mensajes nuevos y enviarlos al servidor para que los haga llegar al destinatario.

Es importante mencionar que, a pesar de que en la explicación que acabamos de hacer hemos distinguido entre ordenadores cliente y ordenadores servidor, la diferencia entre servidor y cliente la determina el *software* de la aplicación concreta. Así, un mismo ordenador puede actuar como servidor en ciertas aplicaciones y como cliente en otras. En cada caso dependerá de las tareas que haga.

2.2. La arquitectura de internet

Las redes de ordenadores se organizan conceptualmente en niveles para poder establecer un cierto orden en las diferentes aplicaciones y servicios que ofrecen. Cada acción que se hace dentro de un mismo ordenador queda incluida en alguno de los niveles definidos. Cada uno de los niveles intercambia información con el mismo nivel de otro ordenador de la red por medio de lo que se conoce como protocolo. Dentro de un mismo ordenador cada nivel da servicio al nivel superior.

Figura 1



La arquitectura de internet se estructura en cuatro niveles: nivel físico, nivel IP, nivel de transporte y nivel de aplicación.

El nivel físico agrupa las funcionalidades de los elementos que conectan físicamente la red. Este nivel es el que se encarga de transmitir la información mediante los dispositivos físicos correspondientes.

En cuanto al nivel de aplicación, es el que interactúa con el usuario final y es el que permite ejecutar los programas que usamos habitualmente, como los navegadores o los gestores de correo electrónico. Un ejemplo de los protocolos que hay en este nivel son el HTTP (*hypertext transfer protocol*) o el SMTP (*simple mail transfer protocol*).

Los dos niveles intermedios, que son el nivel IP y el nivel de transporte, los pasamos a describir en los subapartados siguientes.

El nivel IP

El nivel IP es el encargado de transportar la información mediante las redes. El protocolo que hace esta tarea es el protocolo de internet[2] (IP), que es el protocolo que sabe identificar cuál es la máquina a la que se debe hacer llegar la información.

(2)En inglés *Internet protocol.*

El protocolo IP trabaja con unidades de datos, los paquetes IP. Cada paquete IP contiene dos partes: la cabecera y los datos. La cabecera contiene, entre otra información, la dirección del ordenador al que se quiere hacer llegar la información, mientras que los datos son propiamente la información que se quiere transmitir.

Tal como hemos visto en el primer apartado, internet basa sus comunicaciones en la conmutación de paquetes. Por este motivo, el protocolo IP está orientado a la conmutación de paquetes y no a la conmutación de circuitos. El protocolo IP es un protocolo muy básico que solo se encarga de enviar los datos desde el emisor hasta el receptor, pero no se ocupa ni de gestionar la pérdida de paquetes ni la sincronía de emisión y receptor, es decir, no controla que el orden en que se emiten los paquetes sea el mismo en que se reciben. Veremos que de estos problemas se encarga el protocolo TCP.

Como acabamos de mencionar, los paquetes IP pueden llegar a su destino gracias a que la cabecera del paquete IP contiene la dirección del ordenador de destino. Por lo tanto, es necesario que cada ordenador que esté conectado a internet tenga una dirección, lo que se conoce como dirección IP.

El bit

Recordemos que un bit es la unidad mínima de información y es un valor que únicamente puede ser 0 o 1. Así, para almacenar dos valores bastará con un solo bit. Si queremos almacenar cuatro, necesitaremos 2 bits y los cuatro valores almacenados serán 00, 01, 10 y 11. En general, con *n* bits podemos representar 2 elevado a *n* valores. Por otra parte, es bueno recordar que 1 *byte* está formado por 8 bits. Por tanto, en un *byte* se pueden almacenar 28 = 256 valores diferentes.

Una dirección IP no es más que un identificador único de 32 bits (4 *bytes*) que identifica una máquina conectada a internet.

Dicho de una manera más informal, una dirección IP la forman cuatro números entre 0 y 255 (ambos incluidos) separados por un punto, como por ejemplo 213.73.40.217.

La estructura de las direcciones IP indica la dirección del ordenador, al tiempo que también da información sobre en qué red y subred está el ordenador. De este modo, el encaminamiento de los paquetes por medio de internet sigue una lógica jerárquica, ya que en primer lugar se envía hacia la red de la que forma parte el ordenador destinatario del paquete y posteriormente se afina el envío hasta llegar al ordenador destino.

Los *routers* son los encargados de conectar dos o más subredes IP y de redireccionar convenientemente los paquetes IP según la dirección IP de destino de cada paquete.

El nivel de transporte

Acabamos de ver que el protocolo IP es un protocolo muy simple que se encarga específicamente de guiar la transmisión de paquetes entre el ordenador de origen y el ordenador de destino, pero no se encarga ni de velar por que todos los paquetes lleguen ni que lo hagan en el orden que sea necesario.

El *transfer control protocol* (TCP) es el que se encarga de proporcionar fiabilidad al transporte de los datos. Así, este protocolo es el responsable de que los paquetes lleguen a su destino con el orden y la frecuencia que sea necesario.

La fiabilidad que aporta el protocolo TCP en el transporte de los datos la podemos sintetizar en las siguientes propiedades:

- Corrección de errores: el TCP es el encargado de realizar el control de errores que se pueden producir durante la transmisión para asegurar que el valor de los paquetes es el mismo en el destino que en el origen.

- Entrega de los paquetes: el TCP garantiza que todos y cada uno de los paquetes que se envían lleguen correctamente a su destino.

- Control de secuencia: el TCP asegura que la secuencia de los paquetes llegue al destino en el mismo orden en que ha sido enviada.

- Control de duplicados: el TCP valida que no lleguen paquetes por duplicado.

Así, por ejemplo, el TCP asegura que la información que se había fragmentado en paquetes para ser transportada se vuelve a reagrupar de manera correcta en el ordenador de destino.

3. Servicios y aplicaciones de internet

En estos apartados describiremos el funcionamiento de los servicios y las aplicaciones más utilizados en internet. Su descripción nos ayudará a entender tanto el uso como la problemática.

3.1. Acceso a internet

Los dispositivos (ordenadores, tabletas, teléfonos inteligentes…) necesitan un sistema de enlace que les permita conectarse a internet. Este enlace se soporta físicamente en tecnologías de cable (telefónico fijo, coaxial, fibra…) o en tecnologías sin cable (wifi, satélites, bandas y tecnologías de telefonía móvil –como 2G, 3G y 4G–…) Pero, además, este enlace sobre estos soportes lo suministra un proveedor de servicios de internet –ISP, *Internet service provider*. El usuario que quiere acceder a internet necesita contratar un servicio con este proveedor. Cada país tiene sus propios proveedores, aunque, por supuesto, muchos de ellos son multinacionales y dan servicio a más de un país.

3.2. Sistema de nombre de dominio

Como ya hemos comentado anteriormente, todo ordenador que esté en la red se identifica con una dirección IP de 32 bits que normalmente se representa mediante cuatro grupos de tres cifras decimales (255 es el número más alto posible) separadas por puntos. Como esta numeración es difícil de memorizar, a cada dirección IP, y por tanto a cada máquina, se le asigna un nombre para que sea más fácil de recordar.

El servidor de nombres de dominio[3] (DNS) es el servicio encargado de traducir las direcciones con nombre de ordenadores (por ejemplo, www.uoc.edu) a direcciones numéricas de 32 bits (por ejemplo, 213.73.40.217). El sistema de nombres tiene una estructura jerárquica de árbol y la base de datos, que contiene las equivalencias entre los nombres y las direcciones numéricas, es distribuida y descentralizada.

(3)En inglés *domain name system.*

Los nombres que se asocian a los ordenadores tienen una estructura concreta. Pueden estar formados por letras, dígitos decimales y el símbolo «-». En la estructura sintáctica de un nombre de ordenador los puntos separan los diferentes dominios.

Los dominios del nivel más elevado en la jerarquía figuran a la derecha del nombre. Son los llamados TLD (*top level domain*). Estos dominios representan o bien países, o bien áreas funcionales. Así, dominios como .ad, .tv, .ch y .jp corresponden a países como Andorra, Tuvalu, Suiza (Confederación Helvética) y Japón, respectivamente, mientras que dominios del tipo .edu, .com, .org corresponden a ordenadores de instituciones educativas, organizaciones comerciales y organizaciones institucionales, respectivamente.

Nombres de dominio

En los inicios, cuando comenzó a funcionar internet, la base de datos de los nombres de dominio era muy pequeña y fácil de gestionar. Pronto, el crecimiento de la red impuso la necesidad de crear un modelo jerárquico para el control de nombres de dominio.

Dentro de estos dominios generales, puede haber subdominios que correspondan a empresas o instituciones. Estos subdominios están inmediatamente a la izquierda del dominio de nivel superior y separados por puntos. Se pueden dividir en más subdominios, dependiendo de la utilización de cada recurso. Así, por ejemplo, podemos encontrar uoc.edu o bien correu.uoc.edu.

Dado que las direcciones IP deben ser únicas, también es necesario que los nombres de ordenadores lo sean (ya que están asociados a una dirección). Ahora bien, el hecho de que las direcciones IP y los nombres de los ordenadores sean únicos no quiere decir que nombres diferentes no puedan estar asignados a una misma dirección IP. Por ejemplo, las direcciones www.uoc.edu y www.uoc.es están asociadas a una misma dirección, 213.73.40.217.

La Internet Corporation for Assigned Names and Numbers (ICANN) es una organización sin ánimo de lucro que controla y asigna los nombres a las direcciones IP.

3.3. El servicio WWW

Uno de los servicios más extendidos de internet, junto con el correo electrónico, es el servicio web, conocido por las siglas WWW (*World Wide Web*). La base de este servicio es el protocolo HTTP (*HyperText Transfer Protocol*). Este servicio fue diseñado al final de la década de los ochenta por investigadores del CERN para acceder fácilmente a la información que estaba distribuida por las diferentes sedes del centro.

El servicio web permite el acceso a la información por medio de documentos de hipertexto (páginas web) que incluyen información en cualquier tipo de formato (texto, fotos, vídeos, audio) y que están referenciados entre sí.

El servicio web sigue el modelo cliente-servidor. Los servidores web conectados a internet contienen las páginas web y esperan permanentemente las peticiones de los clientes. Los clientes web, que son los navegadores, son los encargados de llevar a cabo estas peticiones. Se trata, pues, de una tecnología *pull*, en la que el usuario final debe solicitar la información para recibirla.

La manera de acceder a cada servidor es mediante su nombre. Cuando escribimos una dirección web en un navegador, por ejemplo http://www.uoc.edu/web/cat/index.html, lo que hacemos es:

- Indicar el nombre del ordenador al que queremos acceder (mediante el protocolo HTTP), en este caso http://www.uoc.edu/. El sistema se encargará de traducir esta dirección a su dirección IP correspondiente por medio del servidor DNS.

- Especificar el directorio y la página web que solicitamos, en este caso pedimos la página «index.html» del subdirectorio «web/cat/».

Los servidores web van enviando las páginas web que les solicitan. Los navegadores, por otra parte, tienen un sistema de almacenamiento de las páginas que reciben, a fin de reducir el número de transmisiones en caso de acceso continuado a una misma página. Esta información se almacena en lo que se conoce como caché[4].

(4)La palabra está tomada literalmente del inglés *cache*. Significaría 'escondrijo'.

De hecho, el protocolo HTTP va más allá y permite establecer intermediarios, llamados **servidores intermediarios** (*proxy*[5]), entre los servidores web y los navegadores para almacenar las páginas web más visitadas. Así una organización entera puede disponer de un servidor intermediario (*proxy*) que actuará como caché y permitirá optimizar recursos. Si dos usuarios de la organización visitan una misma página web, solo en la primera conexión será necesario buscar la información en internet, mientras que para responder a la petición del segundo usuario podrá utilizar la información que ya se ha almacenado en el servidor *proxy*. Aparte de estas funciones, los servidores intermediarios también se utilizan para filtrar la información y obtener cierta seguridad.

(5)En inglés, *proxy* significa 'apoderado' o 'sustituto'.

Otro protagonista que tiene su origen en las webs que visitan los usuarios y en los servidores que los alojan son las *cookies*[6]. Las *cookies* son pequeños ítems de datos, que se almacenan en los navegadores que utilizan los usuarios, y que permiten identificar qué usuario está visitando la web y, en definitiva, su actividad. Aunque tienen un origen y una función inicial clara, también es cierto que han generado diferentes problemas de seguridad, por lo que, en la actualidad, se obliga a los sitios web a informar que quieren almacenar *cookies* y pedir al usuario su aceptación; también se han desarrollado sistemas alternativos a las *cookies* para superar sus defectos.

(6)En inglés, *cookie* significa 'galleta'.

3.4. Los buscadores

En la actualidad decir Google es decir un mundo de servicios, pero está bien recordar que su origen y su función nuclear fue y sigue siendo la de buscador. Un buscador es un *software* que localiza archivos en un entorno concreto que cumplan ciertas características. Los buscadores de internet buscan archivos, principalmente de la familia HTML, que contengan las palabras clave indica-

das por el usuario: al enlazarse con un navegador, la combinación genera una experiencia de navegación completa por los resultados obtenidos tras solicitar una búsqueda. El corazón de los buscadores es el motor de búsqueda y su estrategia consiste en monitorizar automáticamente los cambios que se producen en cada momento en las páginas web de todo el mundo, utilizando su *spider*, una parte concreta de su *software*.

Los buscadores, al integrarse en los navegadores y con otras funciones muy populares –como la gestión del correo, de mapas o de multimedia–, se han convertido en una herramienta básica para dar respuesta a las necesidades concretas de cada usuario que expresa en su búsqueda. Sin embargo, también capturan, a menudo alegalmente, muchos datos de usuario, y a menudo los usan para una explotación comercial intensa. Y esto tiene una clara implicación ética y en la privacidad de los usuarios.

Aunque es preeminente en Europa (con más de un 95 % de cuota), Google comparte todavía el mercado mundial con otros buscadores como Yahoo! o Bing.

3.5. El correo electrónico

Como ya hemos comentado anteriormente, el correo electrónico es una de las aplicaciones más antiguas de internet porque ya fue diseñado en 1972 sobre ARPA-NET, la predecesora de internet.

El correo electrónico es una aplicación que permite enviar mensajes entre usuarios de una red. Estos mensajes pueden contener cualquier tipo de información en formato digital: texto, imágenes, vídeos, audio.

Los clientes de correo electrónico

Las aplicaciones cliente de correo electrónico más conocidas son el Netscape Messenger, Microsoft Outlook, Eudora y Thunderbird, entre otras.

Del mismo modo que la WWW, el correo electrónico es una aplicación cliente-servidor y, como tal, el servicio que ofrece está diferenciado en una parte cliente y una parte servidor. La parte servidor es la que se encarga de recibir y enviar los mensajes de cada usuario. La parte cliente es la que permite escribir y leer los mensajes, y en último término, almacenarlos.

El funcionamiento general del correo electrónico es muy parecido al del correo postal. De hecho, los correos electrónicos tienen una estructura similar a la de las cartas convencionales. Constan, por un lado, de una cabecera, que sería el equivalente al sobre postal, que contiene una serie de datos, como la dirección del destinatario o destinatarios y el asunto. Por otro, lo que se conoce como cuerpo del mensaje sería el equivalente a la misma carta postal, que es donde se incluye la información del mensaje.

El protocolo que se utiliza para transferir los mensajes es el SMTP (*simple mail transfer protocol*). Este protocolo utiliza direcciones del tipo usuario@uoc.edu, en las que la parte que hay a la derecha de @ indica el dominio que gestiona el servidor de mensajería, mientras que la parte que hay a la izquierda de @ identifica al usuario de la dirección del correo, dentro del dominio en cuestión.

El protocolo SMTP, como el sistema de correos tradicional, está basado en el almacenamiento y reenvío de los mensajes. Cada mensaje es almacenado y reenviado a diferentes servidores intermedios hasta llegar al destino final, al igual que las cartas van pasando por las diferentes sucursales de correos.

En la aplicación de correo electrónico, aparte del protocolo SMTP que permite hacer la transferencia de mensajes, también están los protocolos que permiten el acceso al buzón de correo, es decir, los protocolos que transfieren el mensaje de la parte servidora de la aplicación a la parte cliente. Los dos protocolos que regulan este acceso son el POP3 (*post office protocol* v.3) y el IMAP (*Internet message access protocol*).

Protocolos relacionados con el correo

SMTP permite la transferencia de mensajes entre servidores de correo. POP3 e IMAP permite el acceso del cliente (el programa de lectura de correo) a su correspondiente servidor.

La principal diferencia entre estos dos protocolos radica en el almacenamiento de los mensajes leídos. En POP3, para leer los mensajes, se bajan del servidor al ordenador local en que estemos leyendo el correo. Por defecto, se borran del servidor y, por lo tanto, quedan almacenados únicamente en el ordenador local. En IMAP, por el contrario, los mensajes son leídos en el servidor y se quedan en él, e incluso permite organizarlos en carpetas en el propio servidor.

Diferencia entre POP3 e IMAP

POP3 descarga los mensajes del servidor al ordenador local, IMAP los lee y gestiona en el propio servidor.

Ambas opciones tienen ventajas e inconvenientes. A favor de POP3, se puede argumentar:

- Los mensajes descargados se pueden volver a leer, incluso sin disponer de conexión a la red.

- Borrar los mensajes del servidor cada vez que se lee lo mantiene poco cargado, con lo que se evita el rechazo de mensajes por acumulación en exceso.

Sin embargo, a favor de IMAP, se cuenta con estos otros:

- Permite una gestión unificada del correo, aunque sea consultado desde distintos dispositivos (como varios ordenadores, tabletas y teléfonos móviles). Al mantener los mensajes en el servidor, todas las modificaciones que se hagan (eliminado de mensajes, organización en carpetas, etc.) será visible con absoluta igualdad desde todos los clientes de correo.

- La pérdida de datos, contaminación por virus o destrucción total del ordenador donde se lee el correo no afecta a los mensajes, que siguen seguros en el servidor, habitualmente alojado en un proveedor que toma medidas

de seguridad y realiza copias de seguridad, sin que tenga que ocuparse de ello el usuario.

- El hecho de que los mensajes se conserven en el servidor y el usuario solo pueda acceder a ellos por medio de un protocolo que solo le permite organizarlos en carpetas y borrarlos, pero no alterarlos, mantiene intacta la validez probatoria de los correos, en caso de tener que usarlos en un juicio.

El hecho de que cada vez sea más frecuente usar distintos dispositivos para leer el correo y el aumento casi ilimitado de las capacidades de los buzones de correo están haciendo que el protocolo de conexión del cliente al servidor más utilizado vaya siendo cada vez más el IMAP.

3.6. *Cloud computing*

Más que una tecnología, el concepto de *computación en la nube* (en inglés, *cloud computing*) es un modelo de negocio que consiste en explotar las posibilidades de conexión de internet para que un usuario pueda hacer uso de recursos que no están inmediatamente en sus instalaciones, sino que pueden estar físicamente muy alejados, cuestión que el usuario ni siquiera necesita saber.

La idea es, pues, que ya no sea necesario adquirir, con el correspondiente desembolso, costoso *hardware* como discos de gran capacidad o dispositivos de impresión de altas prestaciones, y poderlos usar como un servicio, por medio de la red.

El primer servicio que se popularizó de forma extensa, siguiendo este modelo, fue el de almacenamiento de datos. Varias empresas empezaron a ofrecer la posibilidad de utilizar almacenamiento remoto de grandes cantidades de datos por medio de internet a cambio de un precio mucho menor que el de los discos de esa capacidad o, incluso, para espacios más modestos se ofrecía gratuitamente, únicamente con la contrapartida de ver publicidad al conectarse para gestionar o recuperar los datos guardados.

Además del ahorro inversor de evitar la adquisición de los correspondientes discos, el almacenamiento «en la nube», es decir, en servidores remotos accesibles por medio de internet, ofrecía y ofrece algunas ventajas:

- La ubicuidad de los datos: se pueden recuperar desde cualquier lugar en cualquier momento.

- La posibilidad de compartir datos: se pueden enviar grandes cantidades de datos a terceros simplemente abriéndoles el acceso al espacio en la nube donde se encuentren.

- Desentenderse de la seguridad: la empresa que presta el servicio se compromete, incluso contractualmente, a tomar las medidas de seguridad (anti-

virus, sistemas de alimentación ininterrumpida, etc.) necesarias para proteger los datos y poder garantizar su integridad.

- La escalabilidad: uno de los problemas de cualquier proyecto de instalación informática es el dimensionado de sus distintos componentes y, en especial, prever el futuro crecimiento de las necesidades de la organización. Utilizando los recursos como un servicio por medio de la red, tanto el dimensionado como el escalado se pueden ir adaptando a las necesidades de la empresa, y únicamente se paga en cada momento aquello que se necesite.

No tener el control y la inmediatez de los datos en las propias instalaciones de la organización también puede tener algunos inconvenientes:

- En países con poca extensión de la red o poca fiabilidad de esta, el acceso a los datos puede resultar difícil o incluso se puede perder dicho acceso durante períodos de horas o días.

- Con datos que requieran medidas de protección elevadas (secretos industriales, información sobre clientes, etc.), el hecho de que «acceder» a ellos suponga hacerlos circular por internet puede suponer un riesgo (aunque muchas empresas ya ofrecen la posibilidad de recibir, almacenar y enviar los datos encriptados).

- Como un caso particular de lo anterior, alojar en la nube datos que, por ley, requieran una protección especial por ser datos de carácter personal puede suponer problemas jurídicos graves. La mayoría de las empresas que ofrecen servicios de almacenaje de datos en la nube no garantizan que dichos datos sean almacenados en países con el mismo nivel de protección exigido en Europa y eso puede llevar al usuario a vulnerar la legislación vigente en esta materia, incluso sin siquiera saberlo.

Actualmente, bajo este modelo de negocio, se pueden utilizar por medio de la red, además del almacenaje de datos, voluminosos medios de impresión que un particular jamás se podría permitir; capacidad de cálculo, como el acceso a supercomputadores; *software* de todo tipo, y un largo etcétera. De hecho, sería posible fundar una empresa y disponer de todos los recursos informáticos que requiriese en cuestión de minutos. Bastaría con tener acceso a «la nube».

También se están diversificando las modalidades de pago de estos servicios. Desde el coste nulo, a cambio del visionado de publicidad, normalmente para volúmenes bastante limitados, al pago por uso, pasando por fórmulas cada vez más flexibles de alquiler o tarifas planas. Las ventajas de estas modalidades son más tema de un curso de economía y gestión de costes que de un módulo tecnológico como el presente.

4. La seguridad en internet

La seguridad en internet es un tema muy controvertido, ya que por un lado es necesaria para que algunos usos, como el comercio electrónico, se puedan llevar a cabo sin tropiezos. Por otro, en algunos casos, puede limitar las libertades de los usuarios de la red.

El problema principal de la seguridad en internet es que su base tecnológica, es decir, el protocolo TCP/IP, no fue diseñada para ofrecer las propiedades de seguridad necesarias en muchas aplicaciones. Por este motivo, se han ido desarrollando diferentes mecanismos para dotar de seguridad algunas de las aplicaciones que utilizan internet.

Para entender qué papel tiene la seguridad en las redes de comunicaciones, como internet, primero es necesario definir diferentes conceptos que fijan diferentes niveles de seguridad de la información.

Si tomamos como ejemplo la compra de un libro en una tienda en línea, en la que hacemos el pago con nuestra tarjeta de crédito convencional, podemos identificar los cuatro conceptos clave de seguridad de la información: confidencialidad, autenticación, integridad y no repudio.

1) Confidencialidad: no debe ser posible que ningún otro individuo que no sea la tienda pueda ver los datos de nuestra tarjeta de crédito.

2) Autenticación: es preciso que «la identidad» de la tienda en línea no pueda ser suplantada, es decir, no puede ser que alguien cree una página web igual que la de una tienda conocida para hacernos creer que compramos en ella.

3) Integridad: es necesario que la información de la transacción de la compra que viaje por la red no se pueda modificar ni alterar sin que se detecte.

4) No repudio: la parte que haya hecho una determinada declaración, aceptación, pedido, etc. no puede negar haberla hecho.

Para ser más precisos, podemos definir estos conceptos de esta manera:

La confidencialidad es la propiedad que asegura que solo aquellos que están autorizados tendrán acceso a la información. A menudo esta propiedad se conoce también con el nombre de privacidad.

La integridad es la propiedad que asegura la no alteración de la información. Esta alteración puede ser insertar, borrar o sustituir información.

La autenticación es la propiedad que hace referencia a la identificación. Es el nexo de unión entre la información y el emisor de esta información.

El no repudio es la propiedad que impide que alguna de las partes niegue algún compromiso o acción adoptados con anterioridad.

En inglés

La palabra *privacidad* se conoce en inglés como *privacy*. Para el mismo concepto también se utiliza la palabra *secrecy*.

Para obtener estas propiedades fundamentales de la seguridad de la información, la herramienta básica que se utiliza es la criptografía, de la que introduciremos algunos conceptos en los apartados siguientes.

4.1. Fundamentos de criptografía

Antiguamente la criptografía se definía como el arte de la escritura secreta, tal como su etimología indica (del griego *krypto*, 'secreto', y *grapho*, 'escritura'). En la actualidad, una de las definiciones más precisas de este término es la siguiente:

La criptografía es la ciencia que estudia las técnicas matemáticas relacionadas con los diferentes aspectos de la seguridad de la información.

La criptología

La criptología es la ciencia que engloba la criptografía y el criptoanálisis. El criptoanálisis es el estudio de las técnicas que permiten romper los criptosistemas que diseña la criptografía.

Desde un punto de vista histórico, la criptografía hace muchos años que se utiliza, pero fue durante la Primera y la Segunda Guerra Mundial y con la introducción de los ordenadores cuando experimentó una evolución mayor.

Una cifra o criptosistema es un método secreto de escritura por medio del cual un texto en claro se transforma en un texto cifrado. El proceso que transforma el texto en claro en texto cifrado se llama *cifrado* y el paso inverso, que transforma el texto cifrado en texto en claro, *descifrado*. Ambos procesos son controlados por una clave secreta.

Uno de los principios básicos que rigen la criptografía es el principio de Kerckhoffs. Este principio se fundamenta en el hecho de que la seguridad de un criptosistema se basa únicamente en su clave secreta. Es decir, un criptosistema es bueno cuando podemos describir todo el funcionamiento y, sin embargo, un adversario nunca podrá descifrar el texto cifrado del criptosistema sin saber su clave.

Ejemplo del principio de Kerckhoffs

Imaginemos que tenemos un criptosistema que a partir de un texto en claro devuelve el texto cifrado siguiente:

OD FULSWRJUDILD SUHVHUYD OD FRQILGHQFLDOLGDG

Con ello es prácticamente imposible saber cuál es el texto en claro que le corresponde. Pero no indica que sea un buen criptosistema, porque aquí lo que es secreto no es solo la clave, sino también el mismo método de cifrado.

La descripción del método de cifrado es:

Dada una letra del texto en claro, para obtener el texto cifrado le sumamos un valor secreto *k*, en este caso *k* = 3. Con estos datos, podemos descifrar el texto anterior y vemos que dice:

LA CRIPTOGRAFÍA PRESERVA LA CONFIDENCIALIDAD

A pesar de que la frase cifrada podía parecer muy complicada, la dificultad residía en el método de cifrado, no en la clave. Una vez descrito el método de cifrado, aunque no nos hubieran dado el valor *k* = 3, habríamos podido encontrarlo fácilmente y descifrar la frase. En este caso, vemos que este criptosistema no es tan seguro porque siguiendo la suposición de Kerckhoffs es fácil de romper.

Encriptación juliana

Este método, hoy en día considerado demasiado simple y fácil de romper, se conoce como encriptación juliana por haber sido usado por Julio César durante sus campañas militares y para comunicarse con Cicerón.

Teniendo presente el principio de Kerckhoffs que acabamos de anunciar, queda clara la importancia de las claves de cifrado en la criptografía. Estas claves son las que encapsulan toda la seguridad de los algoritmos. Dado que uno de los posibles ataques que se puede dar en un criptosistema es el de intentar probar todas las claves, el número de claves posibles es un factor importante a la hora de trabajar con un criptosistema. Ahora bien, teniendo en cuenta que la clave suele ser un número, el número de claves posibles está estrechamente ligado con la longitud de la clave. Así, en una longitud de la clave de cuatro dígitos sabemos que con 10^4 = 10.000 pruebas ya habremos probado todas las claves, mientras que si hablamos de claves de ocho dígitos necesitamos 10^8 = 100.000.000 pruebas para verificar todas las claves. Este hecho hace que se hable de criptografía fuerte o de criptografía débil según la longitud de la clave que se utiliza. Hasta hace poco tiempo, la exportación de criptografía fuerte estaba prohibida en Estados Unidos, ya que se consideraba tecnología militar.

Ataque de fuerza bruta

Son los ataques que consisten en probar todas las claves posibles y ver cuál es la buena.

Los sistemas criptográficos se pueden dividir en dos grandes grupos: la criptografía de **clave simétrica** (también llamada criptografía de clave compartida o secreta) y la criptografía de **clave pública** (o criptografía asimétrica).

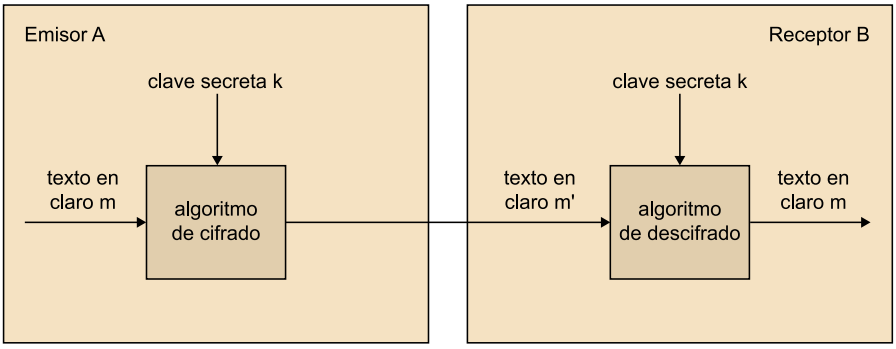
Longitud de la clave en bits

Normalmente se hace referencia a la longitud de la clave en bits. Así una clave de 128 bits de longitud indica que se necesitan 2^{128} pruebas para encontrarla por fuerza bruta.

La criptografía de clave simétrica (secreta o compartida) incluye aquellos métodos de cifrado en los que el emisor y el receptor comparten una misma clave para cifrar y descifrar los mensajes.

La figura muestra el esquema general de cifrado y descifrado:

Figura 2



En este caso, A quiere enviar un mensaje m a B. Para ello cifra el mensaje m con la clave secreta K y el algoritmo de cifrado. Así envía el texto cifrado m' a B. B aplica a m' el algoritmo de descifrado con la clave K y obtiene el mensaje en claro m.

Los criptosistemas más antiguos que se conocen están dentro de este grupo. Un ejemplo son los criptosistemas de sustitución, entre los que se encuentra la encriptación juliana que hemos visto en el ejemplo del principio de Kerckhoffs.

Como criptosistemas de clave simétrica más importantes está el *data encryption standard* (DES), que es el estándar que el NIST (National Institute of Standards and Technology) de Estados Unidos tiene definido como estándar desde el año 1977, y el *advanced encryption standard* (AES), que es el algoritmo que desde el 2002 sustituye al DES, que ha quedado obsoleto debido al aumento de la potencia de cálculo de los ordenadores.

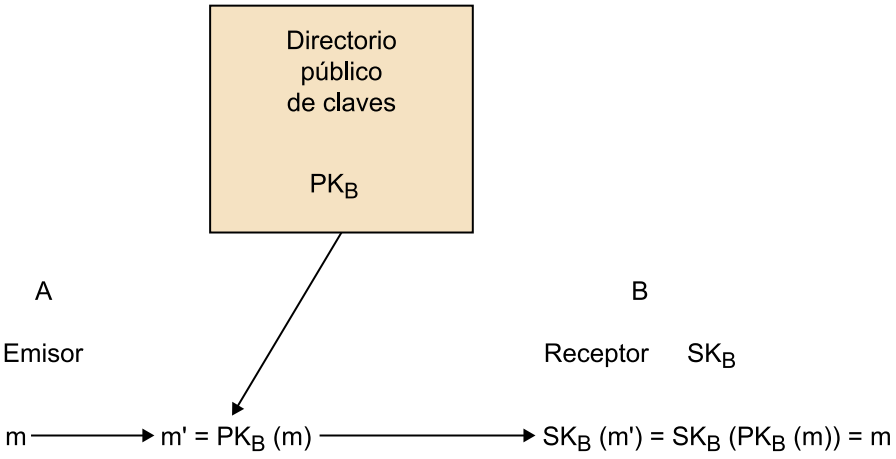
Los criptosistemas de clave pública o asimétrica nacen en 1976 de la mano de W. Diffie y M. Hellman. La idea es totalmente diferente de lo que se había hecho hasta ese momento para los criptosistemas de clave simétrica.

En la criptografía de clave pública cada usuario tiene un par de claves: una pública (PK) y una privada o secreta (SK). Ambas claves son inversas, es decir, lo que hace una lo deshace la otra, aunque no se puede obtener una clave a partir del conocimiento de la otra. Una de las dos claves se da a conocer de manera pública y la otra se mantiene en secreto.

Criptografía europea en Estados Unidos

El NIST (National Institute of Standards and Technology) de Estados Unidos ha decidido adoptar como AES el criptosistema Rijndael desarrollado por los criptógrafos belgas Joan Daemen y Vincent Rijmen.

Figura 3



m = mensaje en claro; m' = mensaje cifrado

PK = clave pública (*public key*); PK_B = clave pública de B

PK_B (m) = aplicación de la clave pública de B al mensaje en claro m

SK = clave privada o secreta (*secret key*); SK_B = clave privada de B

SK_B (m') = aplicación de la clave privada de B al mensaje cifrado m'

El gráfico anterior muestra cómo se utilizan los esquemas de clave pública para cifrar. Cuando Ana, A, quiere enviar un mensaje cifrado a Bernardo, B, obtiene la clave pública de Bernardo (PK_B), lo utiliza para cifrar el mensaje m y obtiene el mensaje cifrado m'. Este mensaje solo puede ser descifrado con la clave privada correspondiente, que tan solo Bernardo conoce (SK_B). Esto es lo que se conoce como **sobre digital**. Realmente, es como si Ana hubiera enviado su mensaje cerrado en un sobre que solo Bernardo podrá abrir.

El criptosistema de clave pública que más se utiliza en la práctica es el RSA. Este criptosistema debe el nombre a sus creadores: Rivest, Shamir y Adleman, y fue propuesto en 1978.

La criptografía de clave simétrica y la criptografía de clave pública tienen una serie de ventajas complementarias que hacen que la combinación de los dos esquemas sea el que se utiliza más en la práctica.

En concreto, es habitual el uso de una variación del sobre digital. Se utiliza un criptosistema de clave simétrica para cifrar la información. Posteriormente, la clave que se ha utilizado para cifrar la información se cifra utilizando un criptosistema de clave pública, concretamente, con la clave pública del destinatario. Es decir, se cifra con una clave simétrica y esta se envía junto con

el mensaje cifrado, cerrada en un sobre digital que solo el destinatario podrá abrir con su clave privada. Así se consigue sacar partido de las ventajas de los dos sistemas.

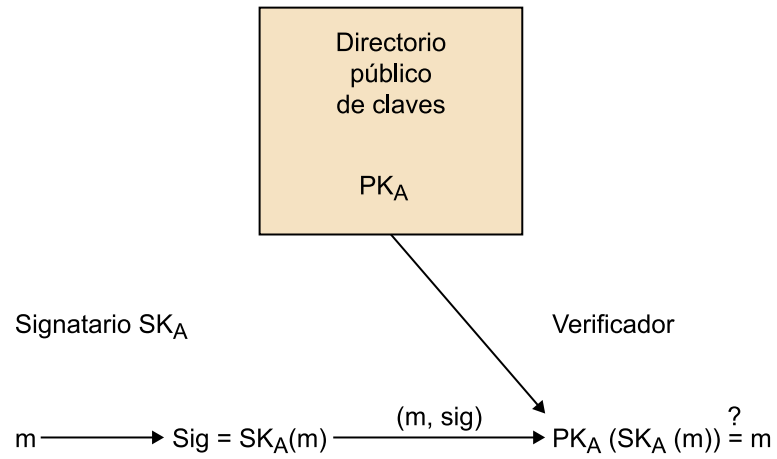
4.2. Firmas digitales

Una firma digital es el equivalente electrónico de la firma convencional.

En un esquema de firma digital, el signatario utiliza su clave privada para firmar digitalmente. Así pues, la firma digital va ligada a un criptosistema de clave pública y, por tanto, podemos firmar digitalmente utilizando por ejemplo el RSA u otros esquemas de criptografía de clave pública.

El esquema general de una firma digital se puede considerar como «el inverso» de un esquema de cifrado de clave pública, tal como se muestra en la figura siguiente:

Figura 4



Significado de las expresiones:

m = mensaje en claro

sig = firma

SK = clave privada o secreta (*secret key*); SK_A = clave privada de A

SK_A (m) = aplicación de la clave privada de A al mensaje m, y se obtiene la firma del mensaje (sig)

PK = clave pública (*public key*); PK_A = clave pública de A

PK_A (SK_A (m)) = aplicación de la clave pública de A a la firma, es decir, el mensaje que se había cifrado con la clave privada de A (SK_A)

El signatario A que quiere firmar un mensaje m coge su clave privada SK_A y la aplica al mensaje. La pareja m y sig formará la firma digital del documento m (de hecho, la firma digital propiamente dicha será sig). Para verificar la firma, un verificador obtendrá la clave pública de A, PK_A, y la aplicará al valor sig. Como las acciones de PK_A y SK_A son inversas, el verificador podrá comprobar que el resultado es exactamente el mensaje firmado m.

Si nos fijamos, la firma digital ofrece propiedades diferentes, algunas de las cuales no ofrece la firma convencional:

- Autenticidad: dado que la clave privada que se utiliza para firmar solo la conoce A, la firma autentica el documento.

- No repudio: otra vez, gracias a que solo A conoce su clave privada, A no puede negar haber firmado un documento que verifica el proceso de firma digital y utiliza la clave pública de A.

- Integridad: esta propiedad, que no ofrece la firma convencional, se desprende del hecho de que el contenido del mensaje se utiliza (junto con la clave privada) para crear la firma. En caso de que se modifique el mensaje, la verificación de la firma con el nuevo mensaje modificado no será correcta.

Es importante destacar que en un proceso de firma digital se envía el mensaje en claro (junto con la firma), es decir, el contenido del mensaje m es totalmente público y, por tanto, el proceso de firma por sí solo no aporta la propiedad de confidencialidad, porque si un tercero intercepta el mensaje lo podrá leer.

Aparte de las propiedades mencionadas anteriormente, la seguridad que aporta la firma digital es muy superior (*a priori*) a la que aporta la firma convencional, ya que esta última puede ser falsificada de manera más o menos eficaz utilizando fotocopiadoras, escáneres, impresoras, etc., mientras que para falsificar una firma digital (sin tener la clave privada, claro) se necesita romper el criptosistema de la firma, lo que, para los buenos criptosistemas, es computacionalmente inviable.

4.3. Certificados digitales e infraestructuras de clave pública

Por lo que hemos visto hasta ahora, puede parecer que la criptografía de clave pública resuelve todos nuestros problemas, ya que la firma digital nos ofrece las propiedades de integridad, autenticación y no repudio y, además, si ciframos la información también obtenemos la propiedad de confidencialidad.

A pesar de todo esto, hay ciertos problemas de fondo a la hora de implementar los esquemas de criptografía de clave pública que hacen que su utilización no esté tan extendida como cabría imaginar.

La criptografía de clave pública permite comprobar técnicamente que la clave que se utiliza para descifrar o verificar la firma es la complementaria de la que se ha utilizado para cifrar o firmar, respectivamente. Pero esto, por sí solo, no ofrece ninguna información sobre la identidad del propietario de las claves.

Por lo tanto, se necesita un mecanismo que permita asociar una clave pública a la identidad de su propietario.

Un certificado digital es un documento digital que vincula una determinada clave pública a un individuo.

Es importante, pues, no confundir el certificado digital con la clave privada ni la clave pública. En algunos casos se habla indistintamente de la clave pública o del certificado digital, pero no porque sea lo mismo, sino porque un certificado digital, por definición, incluye la clave pública.

La información básica que contiene un certificado digital es la siguiente:

- El número de serie del certificado.
- La identificación del algoritmo criptográfico de firma.
- El nombre de la entidad emisora del certificado.
- El período de validez del certificado.
- La clave pública.
- La identidad y los datos más relevantes de la persona o entidad propietaria de la clave pública.
- La firma digital del certificado por la entidad emisora de este.

El certificado también puede contener detalles sobre los servicios que certifica, cuando puede ser utilizado, posibles restricciones sobre certificaciones cruzadas con otras autoridades de certificación, etc.

Si nos fijamos, los certificados incorporan la firma digital de la entidad emisora del certificado, lo que hace que se designe como entidad certificadora o, en inglés, *certification authority* (CA). Es precisamente esta firma la que confiere validez a los certificados, según el grado de confianza que se tenga en la CA firmante.

Así, la validez de un certificado digital dependerá de quién ha expedido este certificado, es decir, de quién lo ha firmado digitalmente y qué mecanismos tenemos para validarlo.

Desde un punto de vista general, este proceso de certificación puede ser centralizado o descentralizado.

Las estructuras en los sistemas de certificación centralizados son jerárquicas: arriba de todo hay una CA, de la que todo el mundo conoce la clave pública sin lugar a dudas y en la que todo el mundo confía. Este tipo de certificación es la que se utiliza en la gran mayoría de las aplicaciones comerciales.

Estándar X.509

El sistema centralizado de certificación se denota por X.509, según la recomendación del ITU-T sobre los esquemas de autenticación en sistemas abiertos.

El caso de PGP es un ejemplo de modelo de certificación descentralizado y se basa en la confianza que tienen los usuarios entre ellos. Cada usuario genera su certificado y este certificado lo firman las personas más próximas, que pueden verificar el vínculo entre clave pública y usuario. De este modo, el certificado personal puede incluir todas las firmas que se quiera y, según los usuarios que lo hayan firmado, tendrá validez ante ciertas personas y no frente a otras.

PGP

Pretty good privacy es un *software* criptográfico de libre distribución que permite cifrar y firmar archivos electrónicos con criptosistemas de clave pública.

Los sistemas descentralizados como el PGP eliminan la vulnerabilidad del ataque al sistema central y también el abuso de poder que puede presentar. El problema de este sistema es que cada usuario debe gestionar los certificados él mismo (revocación, modificación, etc.), porque no hay una autoridad común. Esto, para un número de usuarios elevado, es costoso y hace que estos esquemas no se puedan aplicar a gran escala.

Volviendo a los esquemas de certificación centralizados, es evidente que la CA debe ser una entidad en la que nosotros confiamos. Para simplificar el discurso, hablaremos indistintamente de «confiar en la autoridad» o «tener la clave de la autoridad», porque asumiremos que si tenemos la clave es porque tendremos validado que proviene de una fuente en la que confiamos.

A continuación, una vez identificada la necesidad de los certificados digitales, describiremos cuáles son los pasos necesarios para una verificación correcta de una firma digital. Esta visión detallada de cada paso, nos permitirá terminar de conocer el resto de los mecanismos necesarios para que la criptografía de clave pública pueda ofrecer las propiedades de seguridad que hemos mencionado.

Para cifrar

Si bien en este apartado nos centramos en la firma digital, prácticamente los mismos pasos son los que se deberían seguir en el cifrado de un criptosistema de clave pública para asegurarnos de que el destinatario del mensaje cifrado es el que se quiere.

Las acciones que deben llevarse a cabo para verificar correctamente una firma digital son las siguientes:

1) Leer el certificado digital que acompaña la firma.

2) Verificar la firma del certificado hecha por la CA.

3) Verificar la validez del certificado.

4) Extraer del certificado la clave pública del emisor del mensaje.

5) Verificar la firma del mensaje hecha por el emisor.

Pasamos a describir más detalladamente cada uno de estos pasos.

1) Leer el certificado digital que acompaña la firma

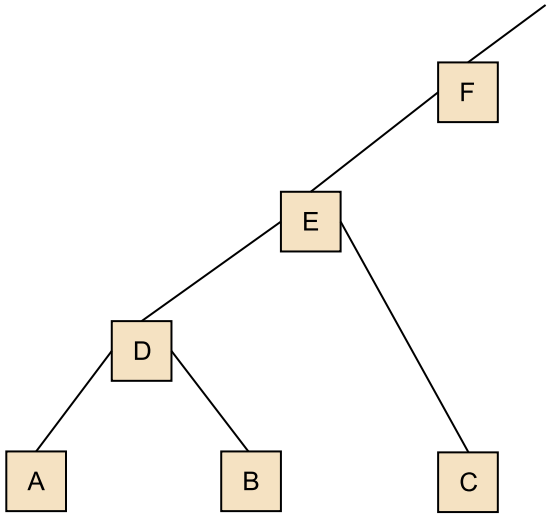
La verificación de una firma digital debe comenzar por el procesamiento del certificado digital para conocer los datos básicos del propietario de la clave pública.

2) Verificar la firma del certificado hecha por la CA

Para probar la autenticidad del certificado necesitaremos verificar su firma, y para ello necesitaremos la clave pública de la autoridad que ha emitido el certificado. Si el certificado ha sido emitido por una CA de la que nosotros tenemos la clave pública, la validación de la firma del certificado será directa utilizando la técnica de verificación de firma digital especificada en el apartado anterior.

En caso de que no tengamos la clave pública de la CA, su obtención nos puede llevar a una recurrencia de tareas, ya que, para obtenerla, la deberemos obtener junto con otro certificado emitido por una tercera CA de la que nosotros tengamos la clave. Así, tendremos que establecer un camino de certificación entre la CA del certificado que validamos y la CA de la que nosotros tenemos la clave.

Figura 5



En la figura adjunta se muestra un posible árbol de certificación. Si nos fijamos, los usuarios A y B comparten directamente la misma CA y, por tanto, podrán validar sus certificados directamente, ya que ambos tienen la clave pública de D. Pero, para que C pueda validar el certificado de A, deberá obtener la clave pública de E y, posteriormente, el certificado de la clave pública de D debidamente firmado por E.

3) Verificar la validez del certificado

Una vez verificada la firma digital del certificado, la tarea siguiente que se debe hacer es asegurarse de que el certificado, a pesar de estar correctamente firmado, es válido. Hay dos aspectos básicos de validez del certificado. El primero es simplemente asegurarse de que el certificado no ha caducado, es decir, que estamos dentro del período de validez especificado. El segundo aspecto de la validez de un certificado hace referencia a su revocación.

Período de validez

Si validamos una firma digital, el período de validez debe hacer referencia a la fecha en que se firmó el documento y no a la fecha en que comprobamos su firma. Lo mismo ocurre con la fecha de revocación del certificado.

Diremos que un certificado ha sido revocado por su autoridad de certificación si, a pesar de estar firmado correctamente por la autoridad y encontrarse dentro del período de validez especificado, la autoridad de certificación no lo reconoce como válido.

Este proceso puede parecer contradictorio, pero hay situaciones en las que la revocación de certificados es necesaria. Por ejemplo, si el propietario de un par de claves pública-privada pierde su clave privada o sospecha que alguien la conoce, debe tener un mecanismo para poder evitar que alguien firme en su nombre. Este mecanismo es el que se conoce como revocación del certificado. El propietario de las claves avisará a la autoridad de certificación, que revocará el certificado. La revocación del certificado se hace por medio de su inclusión en lo que se conoce como **listas de revocación de certificados** (*certification revocation list*, CRL). Por lo tanto, antes de aceptar como bueno un certificado,

aunque la validación de la firma haya sido correcta, necesitaremos confirmar que no ha sido revocado y mirar que no esté incluido en la CRL de la autoridad de certificación.

4) Extraer del certificado la clave pública del emisor del mensaje

Una vez se han hecho todas las verificaciones y los resultados han sido satisfactorios, se extraerá del certificado la clave pública del emisor. Habrá que saber también qué algoritmo de firma corresponde a aquella clave.

5) Verificar la firma del mensaje hecha por el emisor

En este punto ya estamos en posesión de la clave pública del emisor y tenemos la certeza de que esta clave pública pertenece al emisor. Así, solo queda llevar a cabo la verificación de la firma digital, tal como se ha descrito en el apartado anterior.

En resumen, cuando el receptor de un mensaje quiere comprobar la validez de una firma digital debe estar seguro de que la clave pública que utiliza para verificarla pertenece al emisor del mensaje. Esta verificación recae en el certificado digital que ha firmado una autoridad de certificación.

Por lo tanto, los certificados digitales y las autoridades de certificación son la pieza clave para el uso de la criptografía de clave pública, y en concreto para las firmas digitales.

Toda la estructura (certificados, CA, CRL, estructuras jerárquicas, etc.) que rodea a la criptografía de clave pública y que sirve para obtener en la práctica las propiedades teóricas de la criptografía de clave pública es lo que se conoce como infraestructura de clave pública, en inglés *public key infrastructure* (PKI).

A menudo, sin embargo, el concepto de PKI se extiende además al conjunto de protocolos, sistemas de cifrado y servicios en general que permiten desarrollar aplicaciones de criptografía de clave pública.

4.4. Perspectivas de futuro en materia de seguridad en internet

En el momento de redactar estas líneas, la computación cuántica está todavía a medio camino entre el mito y la realidad, pero ya nadie se atreve a dudar de que su inminencia y su irrupción en el panorama internacional puede conllevar muchos cambios, incluso en el ámbito político.

No es este el punto en el que hacer un tratado sobre este nuevo modelo de computación. Bastará con un vistazo sobre la materia con el fin de comprender sus consecuencias sobre la seguridad en internet, que es lo que nos ocupa.

La idea de la computación cuántica se basa en la posibilidad de codificar un bit (recordemos: la mínima unidad de información, que solo puede valer 0 o 1) a escala atómica, aprovechando propiedades de las partículas subatómicas. Esto tiene dos consecuencias: comentaremos, en primer lugar, la más irrelevante, que es el importante aumento de las posibilidades de miniaturización. La más importante es que las mencionadas propiedades de las partículas que componen los átomos permiten la obtención de lo que se denomina un *quantum-bit*, o *qbit*: un bit que es capaz de almacenar, a la vez, un 0 y un 1. Eso supone que, cuando se calcula con ese *qbit*, se están realizando dos operaciones a la vez: la que tendría lugar considerando el 0 y la que ocurriría con el 1. Con *n qbits* se pueden realizar, al mismo tiempo, 2^n operaciones.

qbit

Un ***qbit***, contracción del inglés *quantum-bit*, puede almacenar a la vez un 0 y un 1, y eso permite realizar a la vez las dos operaciones que tendrían lugar considerando el 0 y el 1.

Eso supone que problemas que hasta la fecha eran inabordables para la computación tradicional pasan a ser solucionables con computación cuántica. Por ejemplo, podemos pensar en los denominados ataques de fuerza bruta para romper claves. Si una clave tiene *n* bits, con un ordenador cuántico de *n qbits*, se pueden probar todas las claves en una única aplicación del algoritmo de encriptación. Basta con comprobar (se puede hacer con un simple diccionario) cuál de los 2^n resultados obtenidos muestra un resultado coherente para identificar cuál era la clave correcta.

Este es el motivo por el que todas las grandes potencias (Estados Unidos, Canadá, China, Rusia y la Unión Europea, por lo menos) están invirtiendo ingentes cantidades de dinero para conseguir el primer ordenador cuántico. El primero que lo consiga podrá desencriptar todos los documentos cifrados con los mecanismos actuales de encriptación.

Nadie se atreve a dar fechas de cuándo va existir dicho ordenador. Algunas voces más agoreras afirman que ya existe y que se mantiene en secreto para que los adversarios sigan encriptando con los métodos corrientes y, así, el que ya dispondría de dicho ordenador podría seguir disfrutando de su enorme ventaja.

No vamos a aventurar nosotros esa fecha ni a dar credibilidad a explicaciones más propias de películas de espías que de un curso como el presente, pero sí es conveniente tener en cuenta que, tarde o temprano, la computación cuántica va a llegar y va a suponer una revolución, especialmente en lo que se refiere a la seguridad.

4.5. Soluciones cuánticas al problema de la seguridad

De hecho, los primeros dispositivos cuánticos ya están en el mercado y giran, precisamente, alrededor del problema de la seguridad, el mayor cambio que va a suponer el nuevo paradigma de computación.

Dado que poner toda la base de la seguridad en la dificultad de los cálculos para romper la clave parece una estrategia con poco futuro cuando llegue la computación cuántica, las nuevas estrategias apuntan en otra dirección: la posibilidad de detectar que se ha producido una lectura.

Las mismas propiedades que se aprovechan para codificar a la vez un 0 y un 1 en un *qbit* hacen que sea imposible leer dicho *qbit* sin alterar su valor. Esa es la propiedad que se utiliza para segurizar las comunicaciones: se establecen canales de comunicación cuántica (se sabe que China ya tiene en el espacio varios satélites de comunicación cuántica, por ejemplo) y se codifica la información de modo que se puedan detectar las alteraciones que habría producido una lectura.

Es decir, la nueva estrategia de segurización no consiste en impedir la lectura, sino en detectarla y paralizar la comunicación por un canal que se sabe que ya no es seguro. La información se fragmenta de forma que la lectura de un único paquete resulte totalmente inútil.

Probablemente, en un futuro cercano irán apareciendo los mecanismos y algoritmos que ofrezcan las mismas posibilidades de seguridad de que disponemos hoy día. Con toda seguridad, en ese momento, habrá que reescribir completamente el presente capítulo, pero seguiremos pudiendo disfrutar de niveles razonables de seguridad en la red. Lo único que mantiene en vilo a las más altas autoridades del planeta es la transición de los modelos actuales de computación a la computación cuántica, el «interregno» que se pueda producir durante esa transición.

Resumen

En este módulo didáctico hemos visto cómo el nacimiento de internet se debe a la evolución de la red ARPANET hacia una red con una filosofía más abierta. Hemos visto que el protocolo TCP/IP se centra en la necesidad de crear un protocolo de interconexión de redes genérico que no dependa de ninguna aplicación en concreto.

También hemos visto en qué consiste el modelo cliente-servidor, sobre el que se basan la mayoría de las aplicaciones de la red internet. Hemos explicado las características básicas del protocolo TCP/IP y hemos hecho énfasis, por un lado, en la tarea de direccionamiento que hace el protocolo IP con la ayuda de los enrutadores de red y, por otro, en la fiabilidad que aporta el protocolo TCP a la hora de controlar el comportamiento de los paquetes IP.

Hemos incidido en el funcionamiento de algunas de las aplicaciones y los servicios más utilizados en internet, como la WWW, el correo electrónico o el servidor de nombres de dominio (DNS), así como usos actuales más intensivos, como el *cloud computing*.

Asimismo, hemos hecho un repaso a los temas de seguridad, hemos explicitado los conceptos básicos y hemos visto cómo se pueden conseguir por medio de la criptografía, ya sea cifrando la información o utilizando las firmas digitales.

Por último, hemos hecho una breve perspectiva de futuro sobre el impacto que la irrupción de la computación cuántica pueda suponer sobre la seguridad en la red y las metodologías para asegurarla que puedan surgir en relación con este nuevo paradigma de computación.

Glosario

Dirección IP *f* Identificador de 32 bits que identifica unívocamente un ordenador conectado a internet.

ARPA *f* Agencia que a lo largo de los años ha ido cambiando de nombre. Actualmente es la DARPA, *Defense Advanced Research Projects Agency*.

ARPANET *f* Red de ordenadores creada por el ARPA y precursora de internet.

Autenticación *f* Propiedad que hace referencia a la identificación. Nexo de unión entre la información y el emisor de esta información.

Autoridad de certificación *f* Entidad que da validez a un certificado digital.

Bit *m* Unidad mínima de información que puede tomar dos valores: 0 o 1.

Byte *m* Conjunto de 8 bits.

CA *f* Véase *autoridad de certificación*.

Certificado digital *m* Documento digital que vincula una determinada clave pública a un usuario.

Cloud computing *m* Es un nuevo modelo de prestación de servicios de negocio y tecnología, que permite incluso al usuario acceder a un catálogo de servicios estandarizados y responder con ellos a las necesidades de su negocio, de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo efectuado.

Confidencialidad *f* Propiedad que asegura que solo aquellos que están autorizados tendrán acceso a la información. A menudo esta propiedad también se conoce con el nombre de *privacidad*.

Criptografía *f* Ciencia que estudia las técnicas matemáticas relacionadas con los diferentes aspectos de la seguridad de la información.

DNS *Domain name system*.

Firma digital *f* Equivalente electrónico de la firma convencional.

HTTP *Hypertext Transfer Protocol*.

Infraestructura de clave pública *f* Toda la estructura (certificados, CA, CRL, estructuras jerárquicas, etc.) que rodea la criptografía de clave pública y que sirve para obtener en la práctica las propiedades teóricas de la criptografía de clave pública.

Integridad *f* Propiedad que asegura la noalteració de la información.

IP *m* *Internet protocol*.

Modelo cliente servidor *m* Esquema conceptual de funcionamiento de aplicaciones informáticas en el que se distingue una parte cliente que lleva a cabo las peticiones de servicio y una parte servidor que las satisface.

No repudio *m* Es la propiedad que preserva que alguna de las partes niegue algún compromiso o acción adoptados con anterioridad.

Paquete *m* Unidad de datos básica sobre la que trabaja el protocolo IP.

SMTP *Simple mail transfer protocol*.

Sobre digital *m* Uso del cifrado de clave asimétrica en el que el emisario encripta su mensaje con la clave pública del destinatario, de modo que solo este lo podrá descifrar con su clave privada.

TCP *m* Protocolo de control de transmisión (*Transmission Control Protocol*).

TIC *f* Tecnologías de la información y las comunicaciones.

TLD *Top level domain*.

WWW *World Wide Web*.

SaaS *Software as a Service*.

Software as a Service Es un modelo de distribución de *software* en el que tanto el *software* como los datos manejados son centralizados y alojados en un único servidor externo a la empresa.

Bibliografía

Domingo, J.; Herrera, J. (1999). *Criptografía*. Materiales de la UOC.

Stallings, W. (1997). *Comunicaciones y redes de computadores*. Hertfordshire: Prentice Hall.