Seguridad de las transacciones electrónicas

PID_00269817

César Pablo Córcoles Briongos
Ismael Peña-López

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

César Pablo Córcoles Briongos

Licenciado en Matemáticas por la Universitat Autònoma de Barcelona. Profesor de los estudios de Informática, Multimedia y Telecomunicaciones desde 2001. Coordina asignaturas del ámbito del diseño y desarrollo web del programa de Grado en Multimedia. Director del máster universitario de Desarrollo de Sitios y Aplicaciones Web. Su área de interés en investigación se centra en el uso de recursos multimedia (animación, visualización 3D) e interactivos para la docencia de las ciencias, con especial atención a las materias STEM.

Ismael Peña-López

Profesor en Estudios de Derecho y Ciencias Políticas (UOC) y investigador en Internet Interdisciplinary Institute y en eLearn Center, también de la UOC. Doctor en Sociedad de la Información y del Conocimiento, licenciado en Ciencias Económicas y empresariales (Economía), máster en Ecoauditorías y planificación empresarial del medioambiente y posgraduado en Gestión del conocimiento. Trabaja sobre el impacto de las tecnologías de la información y la comunicación en el desarrollo. En concreto, los intereses se centran en la medida de la evolución de las economías digitales y la adopción personal de lo que es digital (*e-readiness*, divisoria digital), y también el impacto de las TIC en el desarrollo y sus principales instituciones, especialmente en el ámbito de las TIC y la educación y las TIC y la democracia.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Iván Serrano Balaguer (2020)

Primera edición: febrero 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

Hasta ahora, hemos visto algunos ejemplos de interacción entre la Administración y la ciudadanía por los medios electrónicos. Una buena parte de lo que significa la Administración electrónica es la comunicación entre los distintos agentes y administraciones, el intercambio de datos, el trabajo compartido en línea. De igual modo que sucede en el mundo «real», existe el peligro de que ciertas transacciones puedan llevarse a cabo de un modo incorrecto. Y, al margen de la posibilidad de errores –humanos, técnicos– que puedan ocurrir en dichas transacciones, nos referimos en concreto a las cuestiones siguientes:

- La necesidad de garantizar que los interlocutores –tanto la Administración como el administrado– son quienes dicen ser, de manera que no haya suplantación de la identidad en ninguno de los dos casos. Es lo que en términos técnicos recibe el nombre de **autenticación**.

- Una vez los interlocutores están debidamente validados formalmente, hay que garantizar que ninguna de las partes pueda negar haber realizado o haber recibido una determinada comunicación. Esta característica se conoce como **no repudio**.

- El tercer aspecto es que la transacción que hagan sea, precisamente, la que desean hacer, sin que haya modificaciones –o injerencias– en los datos que se intercambian, garantizando, pues, la **integridad** de estos.

- El último aspecto, aunque podría ser el primero, es que los terceros no puedan acceder a los datos ni, por supuesto, utilizarlos en su provecho, con lo cual se garantiza la **privacidad**.

En cualquiera de estos casos, la pieza fundamental es demostrar que se es un usuario que tiene acceso a los datos o a las comunicaciones y que puede operar con ellos. Operaciones elementales en la Administración electrónica como hacer consultas sobre servicios o políticas, efectuar transacciones administrativas o tributarias, o incluso el ejercicio último de la democracia mediante el **voto electrónico**, son cuestiones que requieren una correcta autenticación del ciudadano –para estar seguros de que quien accede a sus datos sanitarios es el paciente correcto– y también una correcta autenticación de la Administración, para estar seguros de que pagamos nuestros impuestos al departamento correspondiente y no a un impostor. Queremos insistir en esta dualidad de la autenticación: es tan importante que el ciudadano se acredite ante la Administración como que esta lo haga ante su administrado.

Históricamente, la humanidad ha resuelto esta cuestión de la autenticación de modo que la persona que debía acreditarse convenciese al acreditador de que poseía algo que, por la naturaleza del objeto y del propietario, creaba una relación única entre ambos, con lo que se demostraba su personalidad. Personarse ante quien nos puede reconocer es, sin duda alguna, la forma de acreditación más antigua del mundo, la cual puede ser sustituida –en el caso de que personarse ya implicara un acceso que pudiera no ser deseado– por el «santo y seña» y la contraseña correspondiente.

Podemos organizar en tres categorías lo que uno puede demostrar que posee para acreditarse:

- Un **conocimiento**, que sería el caso de la contraseña, aún en uso en nuestros días.
- Un **objeto físico**, como una llave, ya sea puramente física –para entrar en casa o en el coche– o con componente electrónica, para acceder a determinada máquina o computadora.
- Nuestro propio cuerpo –**información biométrica**– que, como quien nos reconocía, será inspeccionado y reconocido por los dispositivos correspondientes. Hablamos, por supuesto, de partes de nuestro cuerpo especialmente singulares como las huellas dactilares o el iris de los ojos.

Dado que, a diferencia de la cinematográfica imagen en la que alguien llama a la puerta de una sociedad secreta, personarse mediante las TIC no es físicamente posible, resulta necesario que la información que va a acreditarnos se convierta en una serie de datos digitalizados que viajarán entre las diferentes partes de una transacción.

Sin embargo, esta última cuestión puede efectuarse de dos maneras distintas. La primera, y más intuitiva, es el caso de las **contraseñas**: un usuario tiene una contraseña que el sistema, o el otro usuario, conoce. Para demostrar su identidad, manda dicha contraseña al sistema, este la compara con la que aparece en su base de datos y, si coinciden, se verifica que el usuario es auténtico.

En el segundo caso, no es la información que se conoce la que circula de un usuario a otro, sino el resultado de una operación basada en dicha información. Este caso se llama de **reto/respuesta** que, a su vez, tiene también dos opciones:

- La primera opción es que ambos conocen una misma información. El sistema ordena al usuario que desea acreditarse que haga una operación con la información que comparten, y es el resultado de dicha operación lo que se transmite.

Ejemplo de reto/respuesta con información compartida

La Administración y el usuario saben que el documento de identidad del usuario tiene el número 1234. Al pedir la autenticación en el sistema de pago de impuestos, el sistema de la Administración pide al usuario que introduzca el número de su documento de

identidad multiplicado por dos (esta condición variará para cada autenticación, a fin de evitar que pueda llegar a deducirse el número al ser siempre la misma operación). Si el usuario teclea 2468, su autenticación será válida sin tener que haber enviado su número real, el 1234. (La operación –o serie de operaciones– a realizar, naturalmente, será mucho más compleja que «multiplicar por dos», y verificará toda una serie de condiciones para asegurar la seguridad del procedimiento.)

- En la segunda opción, solamente el usuario conoce dicha información –por lo que es el caso más seguro de todos– y el sistema, aunque no puede reproducirla, sí puede verificarla. Entraremos más adelante en esta cuestión al hablar de la firma digital.

1. Criptografía e identidad en la red

Teniendo en cuenta que este viaje es peligroso porque los datos pueden robarse o suplantarse, se hace necesario «esconderlos» de algón modo. La **criptografía** –disciplina hoy en día plenamente integrada y desarrollada en el ámbito de las matemáticas– viene a responder a dicha necesidad.

Cifrar –aunque a veces se utiliza el anglicismo «encriptar»– es el proceso de cambiar la información de un modo que aparezca como ininteligible para un tercero, pero que quienes conocen el **algoritmo** –o proceso– de cifrado puedan hacer y deshacer la operación tantas veces como sea necesario, tanto para deformar dicha información como para que vuelva a ser comprensible. De hecho, en sentido estricto no es necesario conocer el algoritmo seguido, sino que nuestro ordenador o algún otro dispositivo en nuestra posesión sí lo conozca, además de determinadas **claves** necesarias para iniciar el proceso, del mismo modo que para traducir un texto necesitamos el texto en sí, un traductor experto y, además, saber en qué idioma está escrito y a cuál queremos traducirlo.

Ejemplo de cifrado

Tomando el número del documento de identidad del ejemplo anterior, un algoritmo podría ser «sumar la clave» (teniendo en cuenta que, para **descifrar**, habrá que «restar la clave»). Si la clave es 3, el valor cifrado del documento 1234 será 1237.

En el caso de que tanto el emisor como el receptor del mensaje compartan la clave, el cifrado recibe el nombre de **cifrado simétrico o de clave compartida**. Dicho de otro modo: la clave de cifrado y la clave de descifrado son idénticas, o bien se pueden deducir la una de la otra. Cuanto mayor sea la clave, mayor será la seguridad del sistema. La longitud de la clave se mide en bits, por lo que un sistema de seguridad de 128 bits es más seguro que un sistema de seguridad de 64 bits.

La principal desventaja del cifrado simétrico es que, siguiendo con el ejemplo de la Administración electrónica, la Administración poseería nuestra clave. Este hecho implica un riesgo, ya que alguna persona de la Administración puede tener incentivos para facilitar la clave de los ciudadanos a terceros. Y aun suponiendo una total incorruptibilidad de la Administración, siempre existirá el riesgo de que los sistemas informáticos de esta sufran ataques con el objetivo de conocer todas las claves de todos los ciudadanos. Solo si el ciudadano es el único que conoce su clave correspondiente, el riesgo disminuye considerablemente.

Para evitar que ambas partes compartan una única información, con el riesgo de que se almacene por partida doble y el inconveniente de que, en algún momento, haya habido que llegar a un acuerdo –con las dificultades y riesgos que también esto implica–, para compartir o consensuar dicha información, se

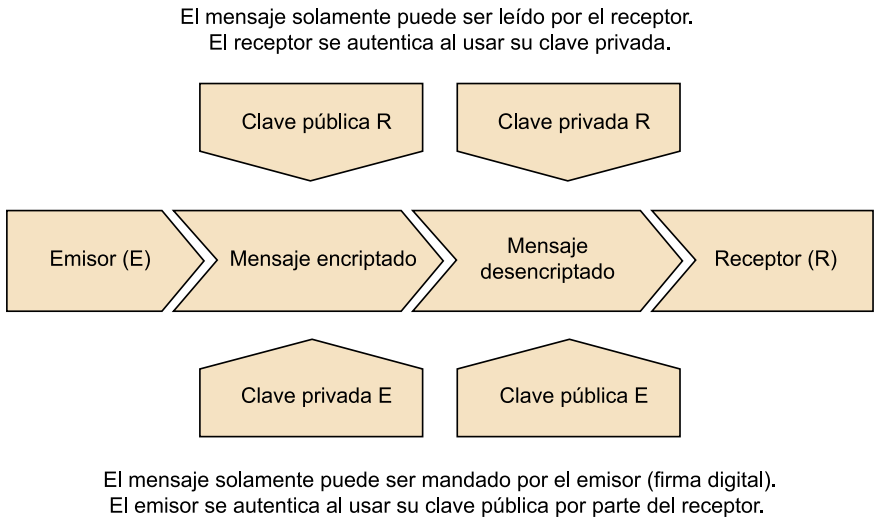
crea el **cifrado asimétrico o de clave pública**. En este sistema se crean un par de claves, la pública y la privada. Como sus nombres indican, la clave pública es conocida por todo el mundo, mientras que la clave privada queda bajo custodia de un único usuario. Para establecer una comunicación, un emisor utiliza la clave pública –que el receptor habrá puesto a su disposición bien directamente, bien facilitándola en su propio sitio web– para cifrar un mensaje que solamente el receptor con la clave privada podrá descifrar. Se garantizan con este procedimiento dos cuestiones:

- que el mensaje no sufre cambios por ocultarse a terceros;
- que solamente el receptor legítimo puede leer el mensaje.

Queda claro, por tanto, que este sistema aporta ciertas mejoras sobre la criptografía simétrica: mientras las claves no las poseen ambos interlocutores, con los riesgos e inconvenientes que ello comporta, el mensaje tiene total **integridad**, donde su contenido no puede verse y, ni mucho menos, modificarse. El sistema se muestra totalmente válido para el pago de impuestos, por ejemplo. Sin embargo, queda una cuestión en el aire: cómo saber si el emisor del mensaje es quien dice ser, ya que la criptografía de clave pública solamente garantiza la integridad del mensaje y que solo el destinatario, con su clave privada, podrá descifrarlo.

La **firma digital** viene a solucionar dichos problemas y lo hace, además, utilizando el mismo sistema: la criptografía de clave pública. Hasta ahora, habíamos considerado el par clave pública/clave privada como un sistema mediante el cual la clave pública «cierra» un mensaje que solamente puede ser «abierto» por quien tenga en su poder la clave privada, que es el «negativo» de la clave pública. Si nos paramos a pensar, si una clave deshace lo que la otra hace, parece intuitivo pensar que debería ser independiente el orden en que las operaciones tengan lugar. Y así es, al menos en este tipo de cifrado: la firma digital es la aplicación inversa del cifrado asimétrico. Un emisor cifra un mensaje con su clave privada. Solamente si es cierto que el emisor es quien dice ser, su clave pública –recordemos: al alcance de cualquiera– podrá descifrar el mensaje. Si con la clave pública del emisor se puede descifrar el mensaje, esto significa que el mensaje se cifró con la clave privada de ese emisor, que solo él posee. Podemos ver un resumen gráfico del funcionamiento del cifrado asimétrico o de clave pública en la imagen siguiente, incluido el caso de la **firma electrónica**.

Figura 1. Cifrado asimétrico o de clave pública



Fuente: elaboración propia.

Resumiendo, el **cifrado de clave pública** aporta **confidencialidad** a la comunicación. Por una parte, garantiza que el mensaje llega a quien debe llegar. Por otra parte, garantiza que el origen del mensaje también es **auténtico**. Y no solamente auténtico, sino que se hace imposible repudiar dicho mensaje o transacción: solamente el emisario con su clave privada puede haber efectuado la acción que deshace su clave pública. En la Administración electrónica, el **no repudio** es fundamental para muchos procesos administrativos del mismo modo que lo es la autenticación del ciudadano. Pensemos, por ejemplo, en la Administración electrónica de Justicia, donde hacer o dejar de hacer algo puede tener distintas consecuencias.

Resumiendo, el **cifrado de clave pública** aporta **confidencialidad** a la comunicación. Por una parte, garantiza que el mensaje solo puede ser descifrado por su destinatario. Por otra parte, garantiza que el origen del mensaje también es **auténtico**. Y no solamente es auténtico, sino que se hace imposible repudiar dicho mensaje o transacción: solamente el emisario con su clave privada puede haber efectuado la acción que deshace su clave pública, luego no puede negar haberla hecho. En la Administración electrónica, el **no repudio** es fundamental para muchos procesos administrativos, del mismo modo que lo es la autenticación del ciudadano.

Aunque en la figura 1 hemos presentado la confidencialidad del mensaje y la acreditación del receptor, por una parte, y la acreditación del emisor, por la otra, en el fondo, estas dos cuestiones pueden hacerse conjuntamente mediante dos cifrados secuenciales: en un primer paso, el emisor cifraría su mensaje con su clave privada –autenticando su autoría, es decir, firmando el mensaje electrónicamente– y, después, cifraría el resultado con la clave pública del receptor, garantizando que solamente este podrá leer el mensaje. Con este «sencillo» procedimiento –elaborado prácticamente en su integridad por los ordenadores y tan automáticamente como deseemos–, se consigue la **auten-**

tication de las partes, el **no repudio** y la **integridad**. La **confidencialidad** queda garantizada por el mismo hecho de que los mensajes están firmados y dirigidos a un receptor concreto.

2. Certificación digital

Llegados a este punto, se pone de manifiesto otra debilidad del sistema, algo menos intuitiva y, en cierto modo, mucho más filosófica: que creamos que una clave pública es la que debemos utilizar para enviar un mensaje, por ejemplo, a la Administración, no significa que esa clave pública pertenezca, realmente, a la Administración. Mientras que el edificio que obra de sede de la Agencia Tributaria en una determinada ciudad es difícil de suplantar –siempre ha estado ahí, conocemos a algunos de sus trabajadores, etc.–, que alguien nos mande una clave pública diciendo ser la Administración tributaria no nos debería merecer, *a priori*, ningún tipo de confianza.

- ¿Cómo saber que una clave pública pertenece, sin duda alguna, a quién dice ser su propietario? Supongamos que alguien nos da su clave pública diciendo ser un ciudadano que quiere interponer una denuncia (electrónica) en la Administración de Justicia. Tomaremos por válidos sus mensajes, porque podremos descifrarlos, aun cuando sea un impostor.

- ¿Cómo podemos saber que una clave pública es, sin duda alguna, la de quien nosotros creemos que es? Supongamos que encontramos la clave pública de la Agencia Tributaria en un sitio web que creemos de confianza. Nuestros mensajes podrán ser leídos por quien tenga la clave privada pareja de esa pública. Este alguien puede ser, perfectamente, un impostor que ha simulado que su clave pública era la de la Agencia Tributaria, de manera que nuestros impuestos irán, directamente, a su cuenta bancaria personal.

Hace falta, pues, que una persona o un organismo se erija en acreditador de la titularidad de las claves públicas. El organismo acreditador –como los bancos con capacidad de emitir moneda– certifica y respalda, de manera directa o indirecta, tanto la identidad digital de las personas e instituciones como la autenticidad de los documentos que estas generan.

Un **certificado digital** –emitido por una **entidad de certificación digital**– es un documento electrónico que acredita –certifica– que el nexo que existe entre quien dice poseer un determinado par de claves pública y privada y esa persona es auténtico. Es decir, que determinada clave pública pertenece realmente a quien reclama su propiedad, mientras que la relación entre la clave pública y la privada no hace falta certificarla, ya que se valida por construcción. El certificado, pues, une a una persona o una institución con una clave pública y, por norma general, le asocia otra serie de datos como la validez del certificado (incluyendo su fecha de expiración) y la firma digital de la entidad acreditadora, es decir, que el certificado digital va firmado digitalmente para garantizar su autenticidad.

Por supuesto, nos enfrentamos aquí con la antigua cuestión de quién vigila al vigilante o, en nuestro caso, quién certifica al certificador. Hay que recurrir, en última instancia, a una entidad que tenga la confianza absoluta de la población. O bien recurrimos a entidades estatales como la Fábrica de Moneda y Timbre –en el caso de España–, o bien a entidades privadas de acreditación de solvencia contrastada, como la empresa Verisign.

El certificado digital –o infraestructura de clave pública, en su nombre técnico– permite acreditar usuarios, así como sus comunicaciones, ya sean mensajes electrónicos o, muy importante para el caso de la Administración electrónica, un sitio web.

En el ejemplo de la figura 2, se puede apreciar cómo la Fábrica Nacional de Moneda y Timbre española –en sus siglas, FNMT– ha emitido un certificado para la página web w1.renfe.es garantizando que se trata, efectivamente, del sitio de la Red Nacional de Ferrocarriles Españoles (en sus siglas, RENFE). Nos indica, también, el período de validez. El uso más evidente de este certificado es garantizar al usuario que las compras de billetes de tren que haga en línea en dicha página web son, efectivamente, productos auténticos respaldados por la empresa de ferrocarriles RENFE, y que sus pagos mediante tarjeta electrónica no irán a parar a manos de terceros por ser un fraude la página en cuestión.

Figura 2. Certificado digital

Fuente: elaboración propia.

En este último ejemplo, la FNMT emite a favor de RENFE un certificado digital, firmado digitalmente por la FNMT –recordemos que la validez de la firma de la FNMT se fundamenta en una confianza total en dicha institución por parte del resto de agentes, dado que nadie certifica la validez de su firma–, de manera que garantiza que todo lo que firme digitalmente RENFE con esa firma certificada es auténtico.

Los certificados electrónicos son creados por programas especiales en los servidores de la entidad certificadora y leídos por otros programas utilizados por los clientes de manera integrada en, entre otras, las distintas aplicaciones de mensajería electrónica o páginas web. Para firmar electrónicamente, el emisor del mensaje puede hacerlo por medio de un programa a tal efecto o mediante dispositivos físicos como tarjetas magnéticas o lápices USB especialmente preparados para ello.

El **documento de identidad digital** –en España llamado DNI electrónico o digital– no es sino una herramienta física para firmar digitalmente. Este documento, que puede tomar la forma de una tarjeta de crédito aunque incorporando un chip, almacena en su interior una serie de datos sobre la persona que lo posee, así como tres certificados:

- El primero, y el más importante: el certificado de la entidad certificadora garantizando que todo el conjunto es auténtico.
- El segundo: un certificado de autenticación –así como su clave privada–, lo que nos permitirá acceder a recintos u ordenadores con solamente introducir el documento de identidad digital. Esta característica vendría a sustituir otros métodos de autentificación digital, como los basados en biometría (véase el principio de este apartado).
- Y el tercero: el certificado de firma digital –y su clave privada correspondiente–, para firmar documentos y efectuar transacciones mediante sistemas informáticos.

Los sistemas informáticos que utilizan el cifrado asimétrico se basan en el llamado **transport layer security** (**TLS**). TLS es un protocolo de cifrado asimétrico que se utiliza en diversas aplicaciones, como el correo electrónico o la comunicación por la web. El protocolos TLS utiliza los certificados electrónicos –que, recordemos, incorporan la clave pública– para establecer, entre otras cosas, la autoría de una página o un mensaje firmado con una clave privada. Podemos saber que una página web ha sido acreditada porque en su URL aparece el protocolo HTTPS, que no es sino el protocolo HTTP habitual con el añadido de la tecnología TLS, así como un candado cerrado en la barra de estado del navegador, normalmente situada en la parte inferior de este, en la barra de navegación o en ambos sitios, como puede apreciarse en la imagen siguiente, captura de pantalla de la Oficina Virtual de la Agencia Tributaria Española.

Ved también

Sobre los protocolos TLS, podéis ver el subapartado 2.1, «Internet y comunicación en red».

Figura 3. Página cifrada con protocolo SSL

Hay que tener en cuenta una cuestión muy importante: que aparezca el mencionado candado en la parte inferior del navegador no significa que la página sea auténtica –en el sentido de pertenecer a quien creemos que pertenece–, sino que se ha establecido una relación satisfactoria –certificada– entre la página y su propietario. Correspondería a todos y cada uno de los usuarios de dicha

Ved también

La suplantación, generalmente con fines delictivos, de identidades corporativas mediante páginas web falsas es tratada en el apartado 3.3.2 al hablar del *phishing*.

página el comprobar, leyendo el certificado correspondiente, que la persona u organización a quien pertenece esa página es, efectivamente, la persona u organización con quien queremos tener tratos.

Pretty Good Privacy

Existen otros métodos para proveer aspectos de privacidad y autenticación, entre los cuales probablemente el llamado Pretty Good Privacy (PGP) es el más conocido.

3. Cibercrimen

Como ocurre en la vida fuera de la red, mientras determinadas instituciones y usuarios intentan proteger su identidad o sus comunicaciones, existen terceras organizaciones y personas que persiguen, justamente, lo contrario: romper los sistemas de seguridad establecidos para acceder a datos o propiedades que puedan explotar en su propio beneficio. En el caso de internet, lo que el criminal persigue es, directa o indirectamente, apropiarse de datos que pueda utilizar fraudulentamente.

Existen, a grandes rasgos, tres maneras genéricas de apropiarse de los datos de un usuario –individual o institucional– para usarlos con fines delictivos:

- el primero, robarlos por la fuerza bruta, o bien obteniéndolos de manera presencial de un usuario, obligándolo, por ejemplo, a suministrar al ladrón su nombre de usuario y su clave secreta; o bien entrando en el sistema informático donde dicha información se guarda;

- el segundo, induciendo al usuario a suministrar dichos datos con la convicción de que no lo está haciendo, es decir, induciendo a error al usuario;

- el tercero –de hecho, en sentido estricto, no es un robo de datos–, induciendo al usuario a hacer una transacción en beneficio de un tercero en lugar de en beneficio del mismo usuario.

3.1. Ataques al sistema

Para el caso en que el criminal quiere apoderarse de los datos entrando en el sistema informático –obviamos aquí el caso en que los obtiene presencialmente–, existen una serie de dispositivos, tanto máquinas como programas, que reciben el nombre de ***firewall*** o **cortafuegos**. Del mismo modo que en el caso de un incendio, el objetivo del cortafuegos es elevar barreras que dificulten el acceso a la información sensible por parte de terceros, controlando básicamente de qué modo tiene lugar, y por parte de quién, el tráfico entre las distintas aplicaciones y espacios de un servidor. En el momento en que un usuario no autorizado intenta acceder a unos datos (zona) para los que no tiene permiso de acceso, ese acceso es denegado y el usuario es expulsado del sistema. La complejidad de este procedimiento está en detectar a tiempo las diferentes incursiones –ataques– de los criminales en el sistema, de qué modo lo están haciendo y ser capaz de expulsarlos de este. Se dice que un sistema tiene un **agujero de seguridad** cuando es posible acceder a una zona restringida sin que el sistema detecte la presencia del intruso o no le sea posible expulsarlo. A veces, este agujero de seguridad está deliberadamente creado por los diseña-

dores del software en lo que se llama **puerta trasera**, que de igual modo que en un edificio, permite acceder al programa o a la red de seguridad sin tener que pasar por los procesos de autenticación habituales. Estas puertas traseras, además de venir programadas en origen –no tienen por qué ser malintencionadas, sino que se utilizan a menudo para facilitar el trabajo a los programadores en reparaciones de los programas, aunque prácticamente siempre es una muy mala idea habilitar puertas traseras–, pueden también crearse mediante programas infiltrados que, a diferencia del caso anterior, sí pretenden abrir esa puerta con intenciones ilegítimas.

Reciben el nombre de ***malware*** o **software maligno** aquellos programas diseñados con fines dañinos. Por supuesto, por dañinos podemos entender infinidad de cosas, entre ellas, lo que hace el ***adware*** o programas de publicidad que nos muestran, generalmente contra nuestra voluntad, ofertas o descargas de material publicitario al correr determinado programa, generalmente el navegador web.

Sin embargo, el software maligno suele tener peores intenciones que la mera información sobre ofertas publicitarias, y su principal objetivo és el robo de información sobre el usuario –en el mejor de los casos– o la utilización del ordenador de este para fines propios, en el peor de ellos.

El software maligno o *malware* suele clasificarse en dos grandes grupos, cuya diferencia, que radica en aspectos técnicos más que en sus funcionalidades, es inocua para el usuario final:

- El **virus**, que necesita «contaminar» otro programa para reproducirse. La manera de «contaminar» un ordenador es, pues, añadir una porción de código a un programa ya existente en el sistema. El principal problema a la hora de eliminar un virus es que, dado que este **infecta** otro programa –el **huésped** o *host*–, puede resultar muy complicado e incluso imposible separar el código del virus del código del huésped, por lo que hay que recurrir a eliminar el huésped, con la correspondiente pérdida de los datos de este último.

- El **gusano** o *worm*, que a diferencia del virus no necesita infectar otro archivo, sino que puede autorreplicarse de manera independiente y copiarse en tantos sistemas como le sea posible. Aunque la eliminación del gusano es mucho más limpia que la del virus, la principal desventaja de este tipo de software maligno es que aprovecha los canales de comunicaciones abiertos con el exterior –correo electrónico, navegador web, compartición de espacios en una red LAN– para reproducirse en otros sistemas, enviando copias a tantos ordenadores como le sea posible, con el correspondiente consumo de ancho de banda y otros recursos añadidos.

Una de las principales maneras en que los gusanos pueden instalarse en un ordenador, además de la contaminación mediante mensajes de correo electrónico y otro tipo de comunicaciones, es mediante programas que el usuario descarga y utiliza deliberadamente. Un **caballo de troya** –o *troyano*, en honor del mito– es un programa que se aparece al usuario como una herramienta útil para hacer determinadas funciones. El usuario lo descarga de la red, lo instala y lo ejecuta. Por norma general, sí hace las funciones prometidas, pero también incluye otras funciones que pretenden, en el fondo, hacerse con el control del ordenador para recopilar información y datos sensibles. A menudo, el troyano es el modo que el cibercriminal utiliza para poder instalar el gusano en el ordenador ajeno, ya que dado que es el usuario final el que ejecuta, conscientemente, el programa, es una manera fácil y rápida de saltarse cualquier tipo de protección que el ordenador pueda tener, ya sea el cortafuegos o un programa de **antivirus**, diseñado para evitar las infecciones por virus o gusanos.

Se cambia aquí la ingeniería tecnológica por algo más sutil: la **ingeniería social**. Es antiguo el dicho que reza que una cadena es tan fuerte como el más débil de sus eslabones. En este caso, por más que se refuerce técnicamente el sistema, si el usuario es el eslabón más débil, justamente ahí incidirán con mayor fuerza los ataques del criminal.

En general, se conoce como ***spyware*** o **programas espía** todo aquel software maligno que pretende monitorizar lo que el usuario hace en su ordenador para comunicarlo, posteriormente, a otro ordenador mediante la red. Esa monitorización puede tener un bajo impacto, por concentrarse en analizar los hábitos de consumo o de navegación de páginas web del usuario, o bien tener mayor impacto al obtener información sobre nombres de usuario y sus claves secretas asociadas, ya sea de acceso a otras redes privadas –para acceder a otra información–, ya sea de acceso a cuentas bancarias o cuentas de cliente en establecimientos de venta en línea.

3.2. Engaño al usuario

En el segundo y tercer caso que mencionábamos anteriormente, donde en lugar de entrar por la fuerza en el sistema se induce a error al usuario, dos prácticas se han generalizado en los últimos años, con más o menos variaciones, aunque siempre con estrategias similares y, por supuesto, con los mismos fines. Ambas prácticas recuperan la filosofía con que concluíamos el subapartado anterior: el eslabón más débil en la seguridad del sistema suele ser el usuario, sea porque su bajo nivel de alfabetización digital hace que todos los aspectos técnicos le parecen arcanos e insondables, sea porque acaba saltándose las incómodas medidas de seguridad en aras de trabajar más cómoda y rápidamente. Bajo el estado de hipnosis que supone el apabullante bombardeo de jerga informática para el lego, este adopta una posición de inercia basada en el «sí

a todo», en la que acepta a pies juntillas todo lo que el sistema le proponga y, en el peor de los casos, lo que un supuesto experto le aconseje con el fin de facilitarle los trámites.

El ***phising*** –palabra compuesta de *password harvesting* o cultivo de claves de usuario, que además tiene una pronunciación parecida a la de *pescar* en inglés– persigue conseguir, generalmente, datos de acceso a redes o servicios en línea (como los mencionados datos bancarios o cuentas de cliente) para después utilizarlos en beneficio propio, suplantando la identidad del usuario legítimo. El proceso más habitual es mandar un mensaje de correo electrónico –o por cualquier otra vía– a un usuario solicitándole dicha información. Para justificar tal petición, se le explica, por ejemplo, que ha habido un error en la base de datos y que su cuenta tiene que reactivarse; los argumentos son infinitos, aunque suelen girar todos alrededor del mismo eje. Es sorprendente constatar que el número de personas que responden a dichas solicitudes de información proporcionando sus datos secretos es espectacularmente elevado.

El *phising*, además de utilizar argumentos más o menos convincentes, utiliza también plantillas y páginas web con la imagen de la institución (por ejemplo, la imagen de la banca virtual que se pretende suplantar) para reforzar la apariencia de veracidad de dicho engaño. En muchos casos, se llega a replicar la página original en un servidor falso, es decir, en un servidor que no es propiedad de la institución auténtica, aprovechando mínimas modificaciones de la URL para aparecer como verdadera, por ejemplo la utilización de la dirección www.mibanccoonline.com en lugar de la que sería la auténtica, www.mibancoonline.com. Nótese que en el caso de la primera URL, la falsa, hay una letra c de más. Si la réplica es lo suficientemente buena, es fácil que ese pequeño cambio en el nombre de la URL pase desapercibido, y más para el usuario no habituado a navegar en internet más que ocasionalmente.

No obstante, este punto no deja de ser un cierto fallo en el diseño de la estrategia de engaño del cibercriminal. Fallo que ha encontrado su solución en un método más sofisticado, el *pharming*.

El ***pharming*** –que a veces se confunde con la variante del *phishing* en la que se replica la página web del servicio en línea– utiliza una vulnerabilidad del sistema DNS, de manera que se puede redirigir un dominio a otro dominio, o mejor dicho, una dirección IP (la legítima) a otra dirección IP (donde reside la réplica falsa) sin que el usuario lo note, incluso cuando este teclea correctamente el nombre del dominio en su navegador. A diferencia del *phishing*, el *pharming* no solamente hace una copia falsa de la página web y la hace parecer igual a la original, sino que además enmascara la IP falsa con el nombre de dominio auténtico de la página original.

Para ello es necesario que haya, como mínimo, dos fallos en la seguridad del sistema:

- El primero es que el criminal pueda controlar el servidor DNS de la víctima, es decir, que pueda entrar en su ordenador y tomar el control del programa que dirige un nombre de dominio a determinada IP. Entre otras herramientas, se emplean a estos efectos troyanos y programas espías o *spyware*.

- El segundo fallo de seguridad es que el usuario no accede a la página mediante un protocolo seguro, a saber, mediante la combinación HTTP + TLS (o HTTPS) que comentábamos al principio de este apartado, o bien que incluso haciéndolo, no nota que ha sido redireccionado a un entorno no seguro y que, entre otras cosas, el candado cerrado no aparece en la barra de estado de su navegador web.

Para concluir con este apartado, queremos lanzar una doble reflexión.

La primera es poner de manifiesto las enormes ventajas que puede tener una identidad digital certificada correctamente, de manera que se posibilite un sinnúmero de trámites en línea con tanta o más seguridad que su contraparte presencial. Sin lugar a dudas, si la Administración electrónica quiere hacer algo más que proporcionar información mediante la red, aspectos como el cifrado de clave pública, la certificación digital o el documento de identidad digital serán tecnologías de uso común en su ámbito y, por tanto, será necesaria una amplia información a todos los niveles y a todos los agentes implicados en su uso.

La segunda reflexión, a pesar de incidir siempre en el mismo aspecto: cabe no olvidar que en estos momentos de rápida adopción de nuevas tecnologías, el desconocimiento sumado al deslumbramiento de la pasión, hace que el usuario sea poco precavido y, en consecuencia, especialmente vulnerable a engaños y malos usos de dicha tecnología. Las consecuencias, sin embargo, son mucho más graves que cuando sucede mismamente en el mundo de carne y hueso. Una vulnerabilidad en un sistema informático provocada por un descuido por parte de uno de sus usuarios no solamente pone en peligro la identidad o el patrimonio de este, sino que, al estar todos los sistemas interconectados, pone en un serio aprieto al sistema en su totalidad y, con ello, a todos y cada uno de los datos que en él residen.

Muchos tecnólogos afirman que una gran parte de los defectos de seguridad de los sistemas existen, precisamente, por el desconocimiento mismo que los propios técnicos tienen de dichos sistemas, y ya no solamente el usuario final. El argumento es que, si el código de los programas no puede ser analizado, es imposible saber qué hace exactamente un programa, de ahí que incluso en el mejor de los casos, cuando se detecta una disfunción, sea dificilísimo solucionarla al no saber qué proceso hay que modificar en concreto. En consecuencia, afirman que el software libre es el único que puede proporcionar la seguridad debida al sistema.

4. Anonimización y redes privadas virtuales (VPN)

La criptografía y la certificación digital pueden utilizarse para garantizar nuestra identidad y hacerla pública, o bien para todo lo contrario: para ocultar nuestra identidad, así como todas las operaciones que efectuemos en la red. Los motivos para ello pueden ser muchos –tanto legítimos como ilegítimos–, entre los que cabría destacar al menos dos: el primero, para evitar que en nuestro ir y venir en la red, nuestros datos puedan ser robados; el segundo, para que nuestra identidad pueda ser trazada, lo que en algunos regímenes autoritarios podría significar exponerse a la censura, la represión e incluso poner en peligro la propia vida.

Una primera manera de ocultar la propia identidad es a partir de los llamados **proxy abiertos**. Como hemos visto, el servidor proxy es el que canaliza las peticiones de un ordenador hacia internet. Un proxy abierto anónimo hace esas mismas funciones, pero oculta la IP del ordenador personal, de manera que la identidad de este queda en el tramo de comunicaciones entre el ordenador mismo y el proxy. La gran ventaja de utilizar este tipo de herramienta radica en que cualquier mensaje, visita a una web, recurso subido a internet, etc. no podrá ser trazado hasta su origen, y se preservará la privacidad del usuario.

Las desventajas de los proxy abiertos son diversas. En lo que al usuario se refiere, cada vez es más frecuente que las páginas web utilicen datos almacenados en el ordenador (mediante *cookies*, por ejemplo) para personalizar la navegación. Ello suele ser imposible de llevar a cabo con anonimizadores, por lo que la navegación puede volverse menos usable. Por otra parte, dado que la anonimización puede usarse para fines poco éticos o incluso ilegales, no deja de ser un peligro arriesgarse a hospedar, en un proxy abierto, actividades que puedan dar lugar a delitos. Dado que la trazabilidad se interrumpe en dicho proxy, es ahí donde acabará (o empezará) la investigación policial de unos presuntos delitos.

Un paso más allá de los proxy abiertos son las **redes de anonimización**, como la popular TOR (*the onion router*), que combina una red de servidores que, además de enrutar repetidas veces las comunicaciones, encriptan los datos para ocultar su significado. A diferencia del caso de los proxy abiertos, las redes de anonimización no solamente hacen opaca la identidad del usuario, sino también el mensaje en sí, lo que aumenta la seguridad de las comunicaciones.

TOR

TOR es una herramienta de anonimización popularmente utilizada en situaciones de comunicaciones de riesgo: http://www.torproject.org

Las **redes privadas virtuales** (VPN, por sus siglas en inglés) utilizan mecanismos parecidos a las redes de anonimización, pero su objetivo es el opuesto a estas: garantizar la identidad de los usuarios, así como la integridad de los mensajes. Es decir, al utilizar una VPN, el usuario se conecta con un servidor y se garantiza que tanto el uno como el otro (el usuario y el servidor) son quie-

nes dicen ser, lo que es especialmente útil para conexiones entre profesionales (sedes de una misma empresa conectadas por internet, trabajadores itinerantes que se conectan a la sede, etc.). Por otra parte, y una vez establecida la conexión entre el cliente y el servidor, la comunicación se cifra para que sea secreta. Esta funcionalidad, más allá de proteger los datos que se intercambian en la red, también sirve para proteger otros datos que igualmente circulan por internet pero que tendemos a olvidar que lo hacen, como nombres de usuario y contraseñas para acceder a cuentas remotas de correo electrónico o de acceso a redes sociales. Así, fuera del ámbito estrictamente profesional, es aconsejable utilizar las VPN cuando se accede a internet mediante una conexión poco fiable o fácilmente manipulable, como la conexión wifi de una sala de conferencias o de un hotel.

5. Otras medidas de autenticación

La autenticación en sistemas digitales tradicionalmente ha consistido en la combinación de un nombre de usuario y una contraseña. Pero como hemos visto con los casos del *phishing* y el *pharming* –y otros mecanismos de ingeniería social– engañar al usuario medio para obtener su contraseña no es excesivamente difícil, sobre todo si sus credenciales dan acceso a datos suficientemente importantes, que pueden motivar a un atacante a tomarse todo tipo de esfuerzos. Es por ello que en entornos que requieren de niveles elevados de seguridad se utilicen otras medidas. Las más frecuentes de entre ellas son la **identificación biométrica** y la **autenticación de doble factor**.

Es más que probable que el lector haya usado, o visto usar, algún teléfono móvil u ordenador que podemos desbloquear bien usando la huella dactilar bien apuntando su cámara al rostro del usuario: la cámara reconoce al usuario y desbloquea el dispositivo. Se trata de métodos muy populares por su comodidad, pero deben tenerse en cuenta algunas de sus limitaciones. La primera de ellas se refiere a la tecnología que se usa para reconocer huellas o caras. Tanto en un caso como en otro, debemos tener en cuenta dos posibles tipos de error. Por un lado, puede pasar que el sistema no nos reconozca y, por tanto, no nos dé acceso al sistema. Afortunadamente, aunque esto puede resultar incómodo, siempre dispondremos del mecanismo convencional de usuario y contraseña o de un PIN (o número de identificación personal). El segundo tipo de error es más peligroso: el sistema puede confundir una huella ajena –o una reproducción, fotográfica o de otro tipo, de nuestra cara– con la nuestra, y así dar acceso a todos nuestros datos a un atacante. Antes de usar un sistema de identificación biométrica, pues, es esencial documentarse sobre la tecnología que usa y sobre las probabilidades de que se produzca este segundo tipo de error (para una identificación facial usando cámaras convencionales, por ejemplo, la tasa de error puede ser tan elevada como uno entre diez mil, que puede ser no aceptable para muchas finalidades).

Otra limitación de la identificación biométrica esta muy relacioanada con estos tipos de errores. Hay un par de aforismos que usan con frecuencia los expertos en seguridad que la ilustran. La primera de ellas es que la identificación biométrica debería ser el equivalente del nombre de usuario, no de la contraseña. Esto es así, si se nos permite el lenguaje vulgar, por el segundo aforismo, que dice que las contraseñas son como la ropa interior: deben cambiarse con frecuencia. Es obvio que en caso de que un atacante consiga replicar nuestra huella dactilar o nuestra cara –algo más sencillo de lo que uno podría imaginar, si el atacante es lo suficientemente sofisticado y tiene suficiente interés– y nuestro sistema de autenticación depende de ello, el problema que tenemos es grave porque difícilmente vamos a poder cambiarlas.

Otro mecanismo, en apariencia más rudimentario pero en muchas ocasiones más efectivo, es la autenticación de doble factor, que nos exige, para acceder a un sistema, dos factores: el primero de ellos puede ser la habitual combinación de usuario y contraseña, pero el segundo tiene que ver con un objeto –físico o lógico– que obra en nuestro poder, y al que un atacante debería tener acceso también para obtener el acceso. Este objeto puede tener la forma de un pequeño dispositivo con una pantalla que muestra un código alfanumérico que cambia periódicamente de acuerdo con un algoritmo prácticamente imposible de descifrar, o llaves USB que desempeñan la misma función de generar periódicamente códigos pero que, en vez de mostrarnos ese código para poderlo teclear nosotros, lo introducen directamente en el sistema. En la actualidad estos dispositivos físicos son sustituidos cada vez más por pequeñas aplicaciones móviles que desempeñan esa función. Naturalmente, siempre es necesario tener en cuenta que en algún momento el usuario va a olvidar su llave USB, o incluso su móvil, y por tanto hay que dar caminos alternativos para poder acceder. Es vital para la seguridad del sistema que esas vías alternativas sean lo suficientemente seguras –lo que suele significar un cierto nivel de incomodidad para el usuario– para no ponerlo en riesgo porque, como ya hemos mencionado, la seguridad de una cadena es la del eslabón más débil.

Bibliografía

INTECO (2010). *Estudio sobre el fraude a través de Internet 2009* [en línea]. Madrid: INTECO. <http://www.inteco.es/file/xk6K9xU46WM_Q1i88xyWtA>