Departamento Tecnología
2017-2018

Bloque 3: Seguridad

Seguridad informática

IES Poeta Julián Andúgar de Santomera - Murcia
AUTOR: ANTONIO RUIZ

1. INTRODUCCIÓN

Como ya hemos visto, Internet tiene muchísimas ventajas pero también está lleno de peligros y riesgos. Cuando salimos a la calle estamos atentos de que no nos quiten o se nos pierdan nuestras carteras o monederos donde llevamos toda nuestra documentación, todos esos datos que nos identifican, como el DNI, nuestras fotos, esa entrada de tu concierto favorito, en definitiva protegemos nuestra intimidad. ¿Por qué no hacemos lo mismo en Internet? Es sorprendentemente alto el porcentaje de usuarios que ni siquiera saben si su ordenador está protegido por antivirus o antiespías. En la tranquilidad de nuestras habitaciones nos creemos a salvo del mundo, pero en el momento en el que nuestro ordenador se conecta a la telaraña mundial, que es Internet, estamos totalmente desprotegidos, expuestos a millones de riesgos que nos traerán consecuencias graves si no tomamos las medidas oportunas.

2. TU ORDENADOR: "UN ROBOT CLASIFICADOR"

Tu ordenador lo apunta todo, guarda todas las páginas *web* que has visitado, las películas, o la música que has descargado, las búsquedas que has hecho en Google o Yahoo, tu correo electrónico, los datos que has rellenado en algún formulario de inscripción, tus contraseñas, tus conversaciones de Programa de mensajería instantánea…, todo. Nunca olvida nada a no ser que tú se lo digas y lo peor de todo: cualquiera que tenga unos conocimientos mínimos de informática podrá saberlo todo sobre ti y utilizar tus datos de forma inadecuada. Pero vamos por partes; tu ordenador lo tiene todo clasificado y guardado en distintos lugares, antes de darte algunos consejos informáticos para estar protegido de los ladrones de datos veamos que se guarda en cada sitio:

• **Historial**: Aquí se almacenan la gran mayoría de las páginas *web* que has visitado. Son algunas de las "huellas" que vas dejando por la Red, así que conviene borrarlas para que nadie las siga.

• **Cookies (huellas)**: Son archivos que contienen la dirección de la página que acabas de visitar. Algunas son temporales, pero otras pueden permanecer en tu ordenador durante años. Los espías pueden hacer un seguimiento de las páginas *web* que has visitado y acceder a tus archivos, de esta manera sabrán tus gustos y preferencias; con ello crean listas de posibles clientes que luego venden a empresas comerciales. Es importante que cada cierto tiempo las elimines.

• **Archivos**: Las imágenes y contenidos de las páginas *web* que has visitado se almacenan en nuestro ordenador para así acelerar la carga de la página cuando vuelvas a visitarla. Pero a partir de estos archivos se puede acceder a los datos que has escrito en las páginas *web* que has visitado. Al borrar estos archivos tardará un poco más en cargarse la página pero estarás protegido de los espías y ladrones informáticos.

Ahora que ya sabes que guarda tu ordenador y donde lo guarda, te aconsejamos que cada cierto tiempo, al menos cada semana dediques cinco minutos a borrar todos estos datos que se quedan en tu ordenador y evitar que los ladrones de datos invadan tu intimidad. ¿Cómo? Realiza la siguiente actividad:

Abre el Internet Explorer, e investiga cómo se eliminan el Historial, las Cookies y los Archivos Temporales. Escribe detalladamente la secuencia de pasos a seguir para conseguirlo.

Realiza las mismas operaciones del ejercicio anterior con el navegador Mozilla Firefox. Escribe, de nuevo, la secuencia de pasos a seguir.

3. EL ATAQUE DE LOS VIRUS

Ahora ya sabes más sobre tu ordenador, pero todavía no estas a salvo y tienes una nueva misión: no dejar que se convierta en un zombi manejado por extraños y protegerle de todos los peligros que existen en Internet. ¿Todavía no sabes los nombres de estos atacantes? Hay una plaga de ellos en Internet y aunque te sorprenda saberlo, también en el teléfono móvil. Son programas informáticos que se propagan con muchísima facilidad y son muy dañinos. A veces se manifiestan y sabemos que están ahí pero otras muchas se esconden en archivos o programas que nos descargamos pudiendo con ello destruir los datos de tu ordenador, sustraer tus datos personales, tus fotos… En definitiva manejando tu ordenador por ti, convirtiéndolo en un zombi.

A continuación te damos toda la información que necesitas sobre estos malhechores y los escudos para estar protegidos:

3.1 ¿Qué son los virus?

> Virus: Cualquier programa informático malicioso creado para manipular el normal funcionamiento de los sistemas informáticos, sin el conocimiento ni consentimiento de los usuarios.

Actualmente, por sencillez, el término virus es ampliamente utilizado para referirse genéricamente a todos los programas que infectan un ordenador, aunque en realidad, los virus son sólo un tipo específico de este tipo de programas. Para referirse a todos ellos también se suelen emplear las palabras: código malicioso, software malicioso, software malintencionado, programas maliciosos o, la más usual, malware que procede de las siglas en inglés malicious software.

Los programas maliciosos pueden alterar tanto el funcionamiento del equipo como la información que contienen o se maneja en ella. Las acciones realizadas en la máquina pueden variar desde el robo de información sensible o el borrado de datos hasta el uso del equipo como plataforma para cometer otro tipo de actividades ilegales –como es el caso de las redes zombies-, pudiendo llegar incluso a tener importantes consecuencias legales.

En sus comienzos la motivación principal para los creadores de virus era la del reconocimiento público. Cuanta más relevancia tuviera el virus, más reconocimiento obtenía su creador. Por este motivo las acciones a realizar por el virus debían ser visibles por el usuario y suficientemente dañinas como para tener relevancia, por ejemplo, eliminar ficheros importantes, modificar los caracteres de escritura, formatear el disco duro, etc.

Sin embargo, la evolución de las tecnologías de la comunicación y su penetración en casi todos los aspectos de la vida diaria ha sido vista por los ciberdelincuentes como un negocio muy lucrativo. Los creadores de virus han pasado a tener una motivación económica, por lo que actualmente son grupos mucho más organizados que desarrollan los códigos maliciosos con la intención de que pasen lo más desapercibidos posibles, y dispongan de más tiempo para desarrollar sus actividades maliciosas.

3.2 ¿A qué afectan los códigos maliciosos?

Los programas maliciosos afectan a cualquier dispositivo que tenga un Sistema Operativo que pueda entender el fichero malicioso, es decir:

- Ordenadores personales
- Servidores
- Teléfonos Móviles

- PDAs
- Videoconsolas

Esto implica que para utilizar cualquiera de estos dispositivos de manera segura debemos verificar que no está infectado, además de tomar las medidas necesarias para prevenir una infección en el futuro.

3.3 ¿Por qué hay gente que crea programas maliciosos?

Cuando surgieron los primeros virus y programas maliciosos solía ser muy sencillo darse cuenta de que el ordenador estaba infectado, ya que los virus generalmente realizaban alguna acción visible en el equipo, por ejemplo, borrar ficheros, formatear el disco duro, cambiar los caracteres de escritura, etc.

Actualmente los programas maliciosos han evolucionado y suelen perseguir un fin lucrativo. Para lograr más fácilmente su cometido suelen pasar desapercibidos para el usuario, por lo que son más difíciles de detectar de forma sencilla. Hay varias formas en las que el creador del programa malicioso puede obtener un beneficio económico, las más comunes son:

- Robar información sensible del ordenador infectado, como datos personales, contraseñas, credenciales de acceso a diferentes entidades…
- Crear una red de ordenadores infectados -generalmente llamada red zombie o botnet- para que el atacante pueda manipularlos todos simultáneamente y vender estos servicios a entidades sin escrúpulos que puedan realizar acciones poco legítimas como el envío de SPAM, envío de mensajes de phishing, realizar ataques de denegación de servicio, etc.
- Vender falsas soluciones de seguridad que no realizan las acciones que afirman hacer, por ejemplo, falsos antivirus que muestran mensajes con publicidad informando de que el ordenador está infectado cuando en realidad no es así, la infección que tiene el usuario es el falso antivirus.
- Cifrar el contenido de los ficheros del ordenador y solicitar un “rescate” al usuario del equipo para recuperar la información, como hacen los criptovirus.

4. TIPOS DE VIRUS

Los distintos códigos maliciosos que existen pueden clasificarse en función de diferentes criterios, los más comunes son:

- Por su capacidad de propagación
- Por las acciones que realizan en el equipo infectado.

Algunos de los programas maliciosos tienen alguna característica particular por la que se les suele asociar a un tipo concreto mientras que a otros se les suele incluir dentro de varios grupos a la vez. También cabe mencionar que muchas de las acciones que realizan los códigos maliciosos, en algunas circunstancias se pueden considerar legítimas, por lo tanto, como dijimos anteriormente, sólo se considera que un programa es malicioso cuando actúa sin el conocimiento ni consentimiento del usuario.

Los posibles tipos de virus y sus clasificaciones son los siguientes:

4.1 Según su capacidad de propagación

Atendiendo a su capacidad de propagación, o mejor dicho de autopropagación, existen tres tipos de códigos maliciosos:

- ***Virus:***

Su nombre es una analogía a los virus reales ya que infectan otros archivos, es decir, sólo pueden existir en un equipo dentro de otro fichero. Los ficheros infectados generalmente son ejecutables: .exe, .src, o en versiones antiguas .com, .bat; pero también pueden infectar otros archivos, por ejemplo, un virus de Macro infectará programas que utilicen macros, como los productos Office.

Los virus se ejecutan cuando se ejecuta el fichero infectado, aunque algunos de ellos además están preparados para activarse sólo cuando se cumple una determinada condición, por ejemplo que sea una fecha concreta. Cuando están en ejecución, suelen infectar otros ficheros con las mismas características que el fichero anfitrión original. Si el fichero que infectan se encuentra dentro de un dispositivo extraíble o una unidad de red, cada vez que un nuevo usuario acceda al fichero infectado, su equipo también se verá comprometido.

Los virus fueron el primer tipo de código malicioso que surgió, aunque actualmente casi no se encuentran nuevos virus pasando a hallarse en los equipos otros tipos de códigos maliciosos, como los gusanos y troyanos que se explican a continuación.

• *Gusanos:*

Son programas cuya característica principal es realizar el máximo número de copias de sí mismos posible para facilitar su propagación. A diferencia de los virus no infectan otros ficheros. Los gusanos se suelen propagar por los siguientes métodos:

- Correo electrónico.
- Redes de compartición de ficheros (P2P).
- Mensajería instantánea.
- Canales de chat

Generalmente los gusanos utilizan la ingeniería social para incitar al usuario receptor a que abra o utilice determinado fichero que contiene la copia del gusano. De este modo, si el gusano se propaga mediante redes P2P, las copias del gusano suelen tener un nombre sugerente de, por ejemplo, alguna película de actualidad; para los gusanos que se propagan por correo, el asunto y el adjunto del correo suelen ser llamativos para incitar al usuario a que ejecute la copia del gusano.

Eliminar un gusano de un ordenador suele ser más fácil que eliminar un virus. Al no infectar ficheros la limpieza del código malicioso es más sencilla, no es necesario quitar sólo algunas partes del mismo basta con eliminar el archivo en cuestión.

Por otro lado, como los gusanos no infectan ficheros, para garantizar su autoejecución suelen modificar ciertos parámetros del sistema, por ejemplo, pueden cambiar la carpeta de inicio con el listado de todos los programas que se tienen que ejecutar al arrancar el ordenador, para incluir en el listado la copia del gusano; o modificar alguna clave del registro que sirva para ejecutar programas en determinado momento, al arrancar el ordenador, cuando se llama a otro programa…

• *Troyanos:*

Carecen de rutina propia de propagación, pueden llegar al sistema de diferentes formas, las más comunes son:

- Descargado por otro programa malicioso.
- Descargado sin el conocimiento del usuario al visitar una página Web maliciosa.
- Dentro de otro programa que simula ser inofensivo.

5. Cómo llegan al ordenador y cómo prevenirlos

Existen gran variedad de formas por las que los virus, gusanos y troyanos pueden llegar a un ordenador; en la mayoría de los casos prevenir la infección resulta relativamente fácil siguiendo unas sencillas pautas. Las formas en que un programa puede llegar al ordenador son las siguientes:

- ***Explotando una vulnerabilidad:***

Cualquier programa del ordenador puede tener una vulnerabilidad que puede ser aprovechada para introducir programas maliciosos en el ordenador. Es decir, todos los programas que haya instalados en el equipo, ya sean: Sistemas Operativos -Windows, Linux, MAC OS, etc-, navegadores Web -Internet Explorer, Firefox, Opera, Chrome, etc-, clientes de correo –Outlook, Thunderbird, etc- o cualquier otra aplicación –reproductores multimedia, programas de ofimática, compresores de ficheros, etc-, es posible que tengan alguna vulnerabilidad que sea aprovechada por un atacante para introducir programas maliciosos. Para prevenir quedarse infectado de esta forma, recomendamos tener siempre actualizado el software el equipo.

- ***Ingeniería social:***

Apoyado en técnicas de ingeniería social para apremiar al usuario a que realice determinada acción. La ingeniería social se utiliza sobre todo en correos de phishing, pero puede ser utilizada de más formas, por ejemplo, informando de una falsa noticia de gran impacto, un ejemplo puede ser alertar del comienzo de una falsa guerra incluyendo un enlace en que se puede ver más detalles de la noticia; a donde realmente dirige el enlace es a una página Web con contenido malicioso. Tanto para los correos de phishing como para el resto de mensajes con contenido generado con ingeniería social, lo más importante es no hacer caso de correos recibidos de remitentes desconocidos y tener en cuenta que su banco nunca le va a pedir sus datos bancarios por correo.

- ***Por un archivo malicioso:***

Esta es la forma que tienen gran cantidad de troyanos de llegar al equipo. El archivo malicioso puede llegar como adjunto de un mensaje, por redes P2P, como enlace a un fichero que se encuentre en Internet, a través de carpetas compartidas en las que el gusano haya dejado una copia de sí mismo…La mejor forma de prevenir la infección es analizar con un antivirus actualizado todos los archivos antes de ejecutarlo y evitar descargar archivos de fuentes que no sean fiables.

- ***Dispositivos extraíbles:***

Muchos gusanos suelen dejar copias de sí mismos en dispositivos extraíbles para que automáticamente, cuando el dispositivo se conecte a un ordenador, ejecutarse e infectar el nuevo equipo. La mejor forma de evitar quedarse infectados de esta manera, es deshabilitar el autoarranque de los dispositivos que se conecten al ordenador.

6. HERRAMIENTAS PARA PROTEGER UN ORDENADOR

En la primera parte de esta unidad nos hemos familiarizado con las amenazas que circulan por la red global, y que ponen en riesgo la integridad de nuestros equipos informáticos. Para proteger nuestros ordenadores, necesitaremos utilizar una serie de herramientas básicas. Es fundamental te familiarices con éstas, y que las instales y mantengas actualizadas, para evitar que el malware pueda tener acceso.

Las tres herramientas básicas de protección – a veces integradas en un mismo programa- son: Antivirus, Antispyware (Antiespías) y Firewall (Cortafuegos).

Veamos en detalle cada uno de estos útiles:

6.1 ANTIVIRUS

Son programas diseñados para detectar, bloquear y/o eliminar el software dañino. Tienen dos mecanismos básicos de detección de amenazas:

- **Comparación**: Buscando entre los programas el patrón de código que coincida con los almacenados en una biblioteca de patrones de virus conocidos.
- Detección de programas hostiles **basados en su comportamiento**. El antivirus conoce una serie de comportamientos sospechosos y estudia a los programas que, por su código, estén preparados para llevarlos a cabo.

Es importantísimo que tengas instalado en tu ordenador un antivirus. Estos paquetes son algo parecido a nuestros guardaespaldas; se mantienen siempre alerta de posibles programas dañinos que puedan colarse en tu ordenador y hacer uso de los datos y archivos que tienes guardados. Por ello es básico que tengas instalado un antivirus.

Además preocúpate de actualizarlo cada cierto tiempo, ya cada día aparecen nuevos virus, y si no tienes las últimas "vacunas" serás vulnerable a sus ataques.

6.2 ANTISPYWARE (ANTIESPÍAS)

Son aplicaciones que se encargan de que en tu ordenador no haya programas que roben tus datos.

Aunque hoy en día los antivirus tratan de ampliar su protección hacia cualquier tipo de malware, y suelen incluir esta función, en ocasiones es necesario utilizar programas específicos para detectar el spyware, que complementan la actividad del antivirus.

Por otro lado, la mejor manera de protegerse de los programas hostiles es ser consciente de su existencia y hacer un uso de la red y del software que minimice el riesgo de que puedan entrar en el sistema. La prudencia es la principal herramienta y se ha de extremar la cautela a la hora de enfrentarse a un programa desconocido. No todos los programas que se reciben por correo o se descargan gratuitos de la red están limpios de amenazas. Es importante comprobar y pensar antes de ejecutar.

6.3 FIREWALL (CORTAFUEGOS)

Un cortafuegos o firewall es un elemento encargado de controlar y filtrar las conexiones a red de una máquina o conjunto de máquinas. Se trata de un mecanismo básico de prevención contra amenazas de intrusión externa. Supone la barrera de protección entre un equipo o red privada y el mundo exterior. Controla el acceso de entrada y salida al exterior, filtra las comunicaciones, registra los eventos y genera alarmas.

Este tipo de programas son como el portero de tu ordenador: nadie pasará sin que él les dé permiso para hacerlo. Te avisa de posibles programas que quieren hacer algo malo en tu ordenador y te hacen invisible ante los posibles ladrones en busca de víctimas. En algunas páginas web encontraras descargas gratuitas de cortafuegos y es recomendable que te hagas con uno de estos "porteros".

7. Seguridad en la transmisión de información

A lo largo de la historia el ser humano siempre ha desarrollado sistemas de seguridad que le han permitido comprobar en una comunicación la identidad del interlocutor (ej. tarjetas de identificación, firma), asegurarse de que sólo obtendrá la información el destinatario seleccionado (ej. correo certificado), que además ésta no podrá ser modificada (ej. notariado) e incluso que ninguna de las dos partes podrá negar el hecho (ej. Notariado, firma) ni cuándo se produjo (ej. fechado de documentos).

En la mayor parte de los casos el sistema de seguridad se basa en la identificación física de la persona, información que se contrasta con el documento de identidad.

Actualmente cada vez mayor número de actividades se está trasladando al mundo electrónico a través de Internet. Después de haber estudiado todas las amenazas que se ciernen sobre nosotros y nuestros ordenadores cada vez que navegamos por Internet, puede que tengáis la impresión de que la red es un lugar tremendamente inseguro, en que es delicado realizar operaciones bancarias, administrativas,… sin correr el riesgo de caer presa de los piratas informáticos. Por suerte esto no es así. Fruto del trabajo y la imaginación de matemáticos e informáticos, se han generado sistemas de protección y certificación de contenidos que permiten a Entidades Bancarias, Administraciones y Empresas, realizar de forma segura operaciones de todo tipo (incluso las que implican el envío de información estrictamente personal y confidencial).

Se han trasladado los sistemas de seguridad a este contexto en el que el principal problema reside en que no existe contacto directo entre las partes implicadas. Necesitamos un documento digital que ofrezca las mismas funcionalidades que los documentos físicos con el plus de ofrecer garantías aún sin presencia física. ¿Cómo se resuelve este problema?

En los siguientes apartados de la unidad vamos a estudiar qué recursos existen para garantizar la seguridad de estas operaciones en la red global.

7.1 CRIPTOGRAFÍA.

La criptografía (*kryptos* = oculto + *graphe* = escritura) es el arte de escribir en clave o de forma enigmática. En principio se puede expresar como el conjunto de técnicas que permiten asegurar que un mensaje solo es entendible por aquel al que va dirigido. En la actualidad estas técnicas permiten además, asegurar que el mensaje no se ha modificado, reconocer al emisor del mensaje, probar la emisión y recepción del mensaje.

Para comprender correctamente conceptos como firma electrónica y certificado digital es necesario partir de los conceptos más básicos sobre criptografía.

Como ya hemos dicho, a lo largo de la historia siempre ha habido necesidad de proteger la información. Así, la criptografía tiene su origen durante el Imperio Romano, en la época del Emperador Julio César. César utilizó un esquema criptográfico simple pero efectivo para comunicarse con sus generales. El esquema de César consistía en desplazar cada letra del alfabeto un número determinado de posiciones. Por ejemplo, la letra "A" podría ser codificada como "M", la "B" como "N", la "C" como "O" ... así sucesivamente. En este caso, el número que se sumaría a cada letra para realizar la codificación sería el 13.

Así pues, el mensaje "ATAQUEN HOY AL ENEMIGO" podría transformarse en "MFMCGQZ TAK MX QZQYUSA", sin poder ser reconocido por el enemigo.

El método de cifrado introducido por Julio César introduce el concepto de "clave criptográfica".

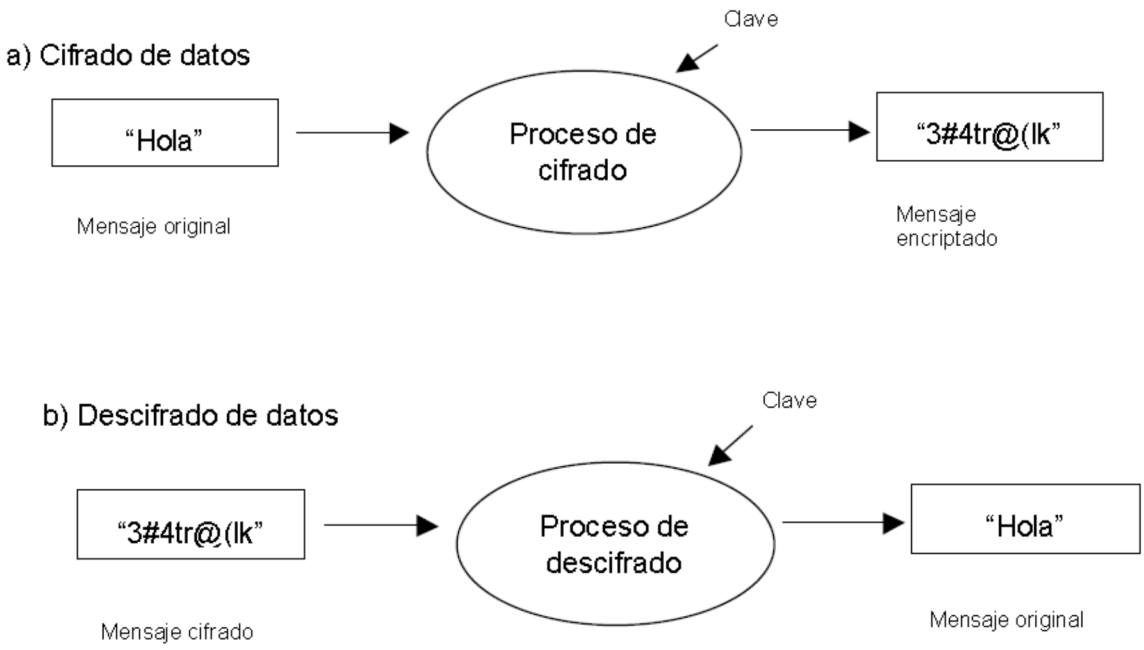
El "desplazamiento de 13 letras" es la clave que se utiliza por César para cifrar el mensaje, necesitándose la misma clave para descifrarlo. El ejemplo de César muestra un criptosistema de *clave simétrica* en el que se utiliza la misma clave para cifrar y descifrar el mensaje.

Por supuesto hoy en día los sistemas criptográficos que se emplean en Internet son mucho más complicados, aunque la base es la misma. No lo olvide: una clave cifra el mensaje. A continuación veremos su aplicación al mundo de las telecomunicaciones.

7.2 LA ENCRIPTACIÓN

La encriptación o cifrado es un mecanismo de seguridad que permite modificar un mensaje de modo que su contenido sea ilegible, salvo para su destinatario. De modo inverso, la desencriptación o descifrado permitirá hacer legible un mensaje que estaba cifrado.

A grandes rasgos, la criptografía es una rama de las matemáticas que se ocupa del proceso de encriptación de información. El encriptación o cifrado de datos es una técnica que permite transformar cierta información en una serie de datos ininteligibles o "datos cifrados", como se muestra a continuación:



Como se observa en la figura, para poder ejecutar ambos procesos de cifrado y descifrado, se necesita utilizar un clave secreta, de manera de sólo quien la conoce puede efectuar dichas operaciones.

De esta manera, por ejemplo, si dos personas se ponen de acuerdo en el valor de una clave secreta, y la mantienen privadamente sólo entre ambos, pueden intercambiar información cifrada. Esto permite que si un agente externo intercepta las comunicaciones, no podrá conocer el contenido original de los mensajes, pues sólo observara datos ininteligibles o cifrados. Para descifrar se necesita conocer la clave.

A las claves usadas para encriptar también se les denomina comúnmente "llaves criptográficas".

En el ejemplo anterior, se uso la misma clave para encriptar y desencriptar. A ésta técnica se le llama "**criptografía simétrica**", y es una técnica limitada porque no permite asegurar la identidad de quién genera el mensaje, puesto que la clave la conocen, al menos, 2 personas.

Criptografía Asimétrica: El concepto de clave pública

El concepto de criptografía de clave pública o "asimétrica" fue introducido por W. Diffie y M. Hellman en el año 1976. Está basada en el uso de un par de claves que cumplen, entre otros requisitos, que lo que somos capaces de cifrar con una de ellas, somos capaces de descifrarlo con la otra y sólo con ella.

Una de las claves solo está en poder del propietario, que debe conservarla de forma segura, y se denomina clave privada.

La otra clave es publicada para que la conozcan todos aquellos que quieran comunicarse de modo seguro con el propietario mencionado, a esta última se la denomina clave pública.

La ventaja de estos sistemas criptográficos es que la denominada clave pública puede ser usada por cualquier persona para encriptar mensajes (transformarlos a texto ininteligible) bajo la premisa que solo quien posea la clave privada podrá desencriptar (ver en forma legible) dichos mensajes.

> Supóngase que dos personas deseasen intercambiar información confidencial; digamos, Bernardo y Carolina.
>
> 1.- Si Bernardo envía a Carolina un mensaje cifrado usando su propia llave privada, Carolina lo puede recuperar usando la llave pública de Bernardo, la cual es conocida. Carolina estará segura que el mensaje venía de Bernardo, pues solo él lo pudo cifrar usando su llave privada. Esto garantiza la autenticidad.
>
> 2.- Asimismo, si Carolina enviase a Bernardo un mensaje cifrado usando la llave pública de Bernardo, está seguro que sólo Bernardo puede recuperar o leer el mensaje, pues solo él tiene el otro par de la llave necesario para descifrar (la llave privada de Bernardo). Esto garantiza confidencialidad.

La idea básica de un sistema de clave pública radica en que es infactible (aun utilizando el mejor computador disponible) determinar la clave privada a partir de la clave pública.

Además, una vez encriptado un mensaje, para cualquier persona que no sea el enviador o el receptor es computacionalmente infactible encontrar el mensaje que lo generó.

El concepto de Firmas Digitales

La criptografía de clave pública también permite disponer de una herramienta análoga a las firmas convencionales: las 'firmas electrónicas o digitales'. Así, de la misma manera en que una firma manuscrita 'convencional' puede ser utilizada en cartas o cheques para especificar la persona responsable por el documento, una firma digital permite enlazar unívocamente a un documento almacenado digitalmente con una persona específica y verificar la autenticidad del contenido del documento.

En particular, un sistema de firmas electrónicas establece un esquema por el cual un 'firmante' puede acompañar un documento por cierta información (una 'firma digital'), generada a partir del contenido del documento y de la clave privada del firmante tal que permita al receptor comprobar que el autor del documento es quien dice ser y que el documento no ha sido alterado.

El concepto de Certificados de Identidad Digital

En los ejemplos mencionados, un aspecto fundamental es poder garantizar que la llave pública de Bernardo que tiene Carolina sea la que le corresponde a Bernardo realmente, y no de un

impostor. Esta garantía es la que brindan los certificados digitales de identidad emitidos por Autoridades Certificadoras (AC). Una Autoridad de Certificación (AC, en inglés CA) es una entidad de confianza del emisor y del receptor del mensaje.

Para garantizar que una llave pública le pertenece a cierta entidad, una AC emite un documento electrónico denominado "certificado digital" en el cual aparecen una serie de datos de la entidad, como el nombre que la identifica, su llave pública, el periodo de validez de dicho certificado, más otros datos como el e-mail, restricciones de uso, etc.

La autenticidad de estos datos es asegurada pues la AC anexa en el mismo certificado su propia "firma digital", tal como se mencionó anteriormente.

En resumen, podría decirse que el certificado digital es una especie de "pasaporte electrónico", que luego puede utilizar la entidad para identificarse (por ejemplo, en el contexto de una transacción electrónica, envió de e-mail, etc). Así, los certificados digitales permiten efectuar comunicaciones electrónicas seguras, garantizando:

- La **autenticidad** de las personas y entidades que intervienen en el intercambio de información.
- **Confidencialidad**: que solo el emisor y el receptor vean la información.
- La **integridad** de la información intercambiada, asegurando que no se produce ninguna manipulación.
- El **no repudio**, que garantiza al titular del certificado que nadie más que él puede generar una firma vinculada a su certificado y le imposibilita a negar su titularidad en los mensajes que haya firmado.

Para el formato de los certificados digitales, existe un estándar internacional ampliamente reconocido, denominado "X.509". El uso de un estándar permite que un certificado sea reconocido y compatible con distintas aplicaciones de software y en variados ambientes.

Por último, cabe señalar que la tecnología de certificados de identidad digital ya viene incorporada en aplicaciones usadas en Internet, como son el correo electrónico y los navegadores. Por ejemplo, Microsoft Outlook permite enviar e-mails firmados digitalmente, y transmitir e-mails encriptados. Para ello basta con tener previamente instalado un "certificado digital" de identidad. Asimismo, con los populares navegadores Internet Explorer o Netscape Navigator, reconocen y manejan íntegramente certificados de identidad digital.

Los ejemplos más típicos de certificados electrónicos son:

- DNI electrónico: DNIe.
- Fábrica Nacional de Moneda y Timbre: Certificado de clase 2 (persona física).

¿Cómo obtener un Certificado Electrónico?

Las gestiones para la obtención de un certificado electrónico deben realizarse ante una

Autoridad de Certificación, reconocida oficialmente.

En particular, para obtener el Certificado de Clase 2 de la Fábrica Nacional de Moneda y Timbre, una vez realizada la solicitud vía internet, deberá acreditar su identidad en una oficina de registro.

Aplicaciones prácticas de los Certificados Electrónicos

Con los certificados electrónicos, es posible realizar consultas y efectuar gestiones a través de la webs de Administración Electrónica o Banca On-Line, permitiendo:

– Autentificar la identidad del usuario, de forma electrónica, ante terceros.

Firmar electrónicamente de forma que se garantice la integridad de los datos trasmitidos y su procedencia.

Cifrar datos para que sólo el destinatario del documento pueda acceder a su contenido.

El protocolo HTTPS

Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP. El sistema HTTPS utiliza un cifrado basado en SSL/TLS para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. De este modo se consigue que la información sensible (usuario y claves de paso normalmente) no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.

Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

La idea principal de https es la de crear un canal seguro sobre una red insegura. Esto proporciona una protección razonable contra ataques *eavesdropping* y *man-in-themiddle*, siempre que se empleen métodos de cifrado adecuados y que el certificado del servidor sea verificado y resulte de confianza.

La confianza inherente en HTTPS está basada en una Autoridad de certificación superior que viene preinstalada en el software del navegador (Es el equivalente a decir "Confío en la autoridad de certificación (p.e. VeriSign/Microsoft/etc.) para decirme en quien debería confiar"). Los protocolos HTTPS son utilizados por navegadores como:

Safari, Internet Explorer, Mozilla Firefox, Opera y Google Chrome, entre otros.

Algunos navegadores utilizan un icono (generalmente un candado) en la parte derecha de la barra de direcciones para indicar la existencia de un protocolo de comunicaciones seguro e incluso cambian el color del fondo de la barra de direcciones para identificar páginas web seguras.

Para conocer si una página web que estamos visitando utiliza el protocolo https y es, por tanto, segura en cuanto a la trasmisión de los datos que estamos transcribiendo, debemos observar si en la barra de direcciones de nuestro navegador aparece https al comienzo, en lugar de http.

8. Ejercicios

1. Abre el Mozilla Firefox, e investiga cómo se eliminan el Historial, las Cookies y los Archivos Temporales. Escribe detalladamente la secuencia de pasos a seguir para conseguirlo.
2. Realiza las mismas operaciones del ejercicio anterior con los navegadores Internet Explorer y Google Chrome. Escribe, de nuevo, la secuencia de pasos a seguir.
3. ¿Cuál es término correcto para referirse genéricamente a todos los programas que pueden infectar ordenador?
4. Indica si la siguiente afirmación es verdadera o falsa, y justifica tu respuesta: “Los software maliciosos son programas que solamente pueden afectar al normal funcionamiento de ordenadores”
5. Investiga en Internet qué caracteriza el comportamiento de los siguientes tipos de malware (son algunos de los más conocidos):
    a. Adware:
    b. Bloqueador:
    c. Bulo (Hoax):
    d. Capturador de pulsaciones (Keylogger):

   e. Espía (Spyware):
   f. Ladrón de contraseñas (PWStealer):
   g. Puerta trasera (Backdoor):
   h. Rootkit:
   i. Secuestrador del navegador (browser hijacker):
6. Diferencia entre Virus, Gusano y Troyano.
7. Resume en una frase corta las vías de entrada típicas de los software maliciosos a los ordenadores.
8. Busca en Internet 5 software antivirus de reconocido prestigio. ¿Qué precio tendría para un usuario particular comprar uno de estos antivirus?
9. Encuentra 3 antivirus gratuitos en la red. Incluyen Antispyware o Firewall entre sus funcionalidad.
10. Visita las siguientes webs e indica en un párrafo en qué consiste cada una de ellas:
    a. http://www.osi.es/
    b. http://cert.inteco.es/
11. Busca en la Wikipedia información sobre el programa Spybot-Search & Destroy. ¿Para qué sirve? ¿Quién lo creó? ¿Cuánto cuesta?
12. Si en una página web encuentras disponible un Antispyware gratuito, que dice detectar amenazas graves presentes en tu PC ¿Crees que sería conveniente descargarlo e instalarlo? Justifica tu respuesta.
13. Investiga cómo se configura el Firewall que viene incluido en el Sistema Operativo Windows. Explica para qué crees que sirven las Excepciones del Firewall.
14. ¿Cuál es el origen histórico de la encriptación, y con qué finalidad se utilizó?
15. Diferencia entre criptografía simétrica y asimétrica. ¿Qué ventajas ofrece el sistema de claves públicas de la criptografía asimétrica?
16. ¿Qué es una autoridad de certificación (AC)?. Escribe el nombre de al menos 2 AC.
17. Visita la página oficial del DNI electrónico (DNIe), e investiga qué trámites electrónicos se pueden hacer con el DNIe (SERVICIOS DISPONIBLES). ¿Se te ocurre algún otro trámite que podría agilizarse haciéndolo de forma electrónica utilizando el DNIe?
18. ¿Qué elementos necesitas en tu ordenador para poder utilizar el DNIe?
19. ¿Qué coste puede tener un lector de tarjetas con chip, como las del DNIe?
20. ¿Qué 4 cualidades garantizan los certificados digitales a nuestras comunicaciones electrónicas?
21. Investiga en Internet en qué consisten el *eavesdropping* y el *man-in-themiddle.*
22. ¿Qué es y para qué sirve el protocolo HTTPS?. ¿Utilizan hotmail o gmail un protocolo HTTPS?
23. Busca alguna página que utilice el protocolo HTTPSs, y haz una captura de pantalla de los detalles de su certificado.