Unidad 2

Seguridad activa

Seguridad y alta disponibilidad

Índice

2.1. Terminología

2.2. Un poco de historia

2.3. Sistemas de cifrado
- 2.3.1. Algoritmos simétricos o de clave privada
- 2.3.2. Algoritmos asimétricos o de clave pública
- 2.3.3. Principales algoritmos de cifrado
- 2.3.4. Cifrado híbrido

2.4. Huella digital

2.5. Protocolos seguros

2.6. Firma electrónica y certificado digital
- 2.6.1. Autoridades certificadoras de confianza
- 2.6.2. Autoridades certificadoras raíz e intermedias
- 2.6.3. Almacén de certificados
- 2.6.4. La problemática de la CA raíz españolas
- 2.6.5. Infraestructura de clave pública (PKI)
- 2.6.6. Consejos sobre certificados digitales

2.7. Malware
- 2.7.1. Tipos de malware
- 2.7.2. Software de seguridad
- 2.7.3. Desinfección

2.8. Spam
- 2.8.1. Software antispam
- 2.8.2. Registros SPF
- 2.8.3. Correo legítimo

2.9. Actualización del sistema y de las aplicaciones
- 2.9.1. Windows Server Update Services (WSUS)
- 2.9.2. Repositorios locales en Linux

2.10. Hardening

2.11. Seguridad en la red corporativa
- 2.11.1. Seguridad de redes cableadas
- 2.11.2. Seguridad de redes inalámbricas
- 2.11.3. Monitorización del tráfico de red

Introducción

Uno de los principales problemas que nos encontramos en la gestión del almacenamiento y las redes es la posible pérdida o sustracción de los datos que lo contienen. Por eso mismo, vamos a analizar la importancia de una buena gestión y uso de los dispositivos con los que contamos para gestionar la información o documentación que manejamos día a día.

Es necesario tener una buena formación respecto a la configuración de programas, así como un especial cuidado en el manejo de todo tipo de herramientas que tenemos a nuestra disposición.

El mal uso conlleva a la perdida de información y en muchas empresas, se traduce en una pérdida de tiempo o lo que es peor, de beneficios. Por lo que es necesario que pongamos especial atención cuando se trata de manejar cierto tipo de información.

Al finalizar esta unidad

- Aprenderemos la importancia de la criptografía, sobre todo, en la seguridad informática.
- Conoceremos la historia de la criptografía.
- Estudiaremos los sistemas de cifrado simétrico y asimétrico.
- Describiremos las ventajas y las desventajas de los sistemas de cifrado.
- Definiremos las instrucciones en la resolución de scripts en PHP.
- Conoceremos los actores participantes en el proceso de firma electrónica.
- Analizaremos las principales medidas de seguridad activa.
- Conoceremos los tipos de malware y las herramientas que se utilizan para combatirlo.
- Estudiaremos el spam y cómo se lucha contra él.
- Pondremos en práctica algunos métodos para corregir vulnerabilidades, como actualizaciones, hardening y aislamiento de aplicaciones.
- Valoraremos ciertas soluciones que aportan seguridad.

2.1. Terminología

La palabra *criptografía* deriva del griego *kryptós*, "oculto". y *grafé*, "escritura". La Real Academia, describe la *criptografía* como el "arte de escribir con clave secreta". Esto implica que, gracias al uso de la *criptografía*, podemos adquirir una serie de ventajas respecto al ámbito de la seguridad informática. Véase:

- Confidencialidad
- Integridad
- Autenticidad
- No repudio

Si enviamos un mensaje cualquiera y es interceptado por un agente externo, este no tiene autorización o no posee la clave necesaria para ello, lo cual no podrá descifrarlo. No obstante, si el usuario utilizase alguna de las técnicas conocidas como *romper el código*, tendría posibilidad de romper la seguridad, pero supone una gran pérdida de tiempo con su respectiva inversión.

De esta manera, podemos decir que no existe ningún método de cifrado seguro, pero dependiendo del tiempo empleado en tratar de romperlo, supone una escala de seguridad para diferenciar entre métodos seguros o menos seguros. Todos, a la larga, sufren algún tipo de vulnerabilidad.

Una de las técnicas utilizadas para romper códigos consiste en el *ataque por fuerza bruta*, es decir, probar de manera constante todas las posibles combinaciones de la clave hasta dar con la utilizada en el cifrado previo. Así mismo, es uno de los métodos que más tiempo requiere e incluso se calcula, que el ordenador más potente tardaría siglos en descifrarlo.

Actualmente, la criptografía está tan extendida que se utiliza tanto de manera consciente como de forma inconsciente.

2.2. Un poco de historia

¿Sabías que la criptografía es una rama que pertenece a las matemáticas? Así es. De hecho, los métodos de cifrado se basan en complejos teoremas y profundos cálculos matemáticos.

Uno de los sistemas de cifrado más famosos es que utilizo Julio Cesar a principios del siglo I a. C. Se trata de un cifrado básico, pero consiste en el desplazamiento de cada letra del abecedario, de manera que, al moverlas un número determinado de posiciones, se reemplazan por otras.

ORIGINAL	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
CIFRADO	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

Este sistema funciona de la siguiente manera. Imaginemos que queremos mandar la palabra *Universae* de manera cifrada con este método. El texto original sería de la siguiente manera:

UNIVERSAE

Si queremos cifrarlo, tenemos que fijarnos que, al desplazar las letras, se han reemplazado por otras totalmente diferentes. Vamos a usar ese sistema para cifrar la palabra *Universae*. Basándonos en el cuadro anterior, tendríamos que hacerlo de la siguiente manera

Palabra original: UNIVERSAE

Palabra cifrada: ASÑBKXYGK

Siguiendo el método de encriptado, podemos desencriptar la palabra para saber el contenido original. Un sistema simple, entendible y representa cómo funcionan los métodos de cifrado.

- La *clave* de este algoritmo es el movimiento de 6 posiciones a la izquierda en el alfabeto.
- Tanto el emisor como el receptor deben *conocer la clave* previamente a cualquier envío de mensaje cifrado.
- Podemos expresarlo *matemáticamente*.
- Era un sistema dotado de una gran seguridad. En aquella época, era tremendamente difícil encontrar enemigos con la capacidad de leer.
- Vulnerable a *ataques con fuerza bruta* si conocían ele método de Julio Cesar

Por ello, a través de la historia los métodos utilizados se fueron perfeccionando con tal sofisticación, que algunos de ellos no han podido ser descifrados en todos estos siglos, como es el famoso caso del sistema utilizado entre Fernando el Católico y su general de aquel entonces, Gonzalo Fernández de Córdoba. Hasta mediados del año 2018 no se había conseguido descifrar ninguna de sus cartas escritas entre 1502 y 1506.

2.3. Sistemas de cifrado

2.3.1. Algoritmos simétricos o de clave privada

Reciben ese nombre porque utilizan la misma clave tanto para el cifrado como el descifrado del mismo.

Ambos receptor y emisor deben conocer la clave con el fin de poder tanto descifrarlo como cifrar el mensaje. Motivo por el cual conocemos este tipo de clave como *clave privada*.

Este algoritmo cuenta con la ventaja de la rapidez de su cálculo ya que cualquier ordenador actual cuenta con la capacidad de convertir el mensaje cifrado con mucha rapidez. El único inconveniente que presenta es la poca seguridad, porque es necesario transmitir la clave a través de la red, haciendo que esta sea vulnerable de manera casi instantánea.

Imagen 1 Algoritmo de clave simétrica

2.3.2. Algoritmos asimétricos o de clave pública

Este tipo de algoritmos utilizan dos pares de claves (cuatro en total). Tanto el emisor como el receptor disponen de dos tipos de claves, una pública y otra privada. En este caso, solo comparten la clave pública.

En este caso, el cifrado es más seguro ya que para esto, se necesita la clave privada del emisor y la clave pública del receptor, y para descifrar el mensaje, es necesaria la clave privada del receptor y la clave pública del emisor.

Imagen 2. Algoritmo de clave asimétrica

El funcionamiento de este algoritmo sería de la siguiente manera:

- La pareja de claves (pública + privada) se genera a través de unas complicadas fórmulas matemáticas basadas en números primos. Aunque las dos claves tengan relación entre sí, *es imposible averiguar la clave privada partiendo de la clave pública*. Cuanto mayor sean esos números, mayor seguridad.
- Emisor y receptor deben intercambiar sus claves públicas. En este caso, con la tranquilidad de que alguien pueda interceptar la clave gracias a lo comentando anteriormente.
- El emisor combina el mensaje que desea enviar con su clave privada y la clave pública del receptor. Por el contrario, el receptor utiliza la otra pareja de claves para descifrar.

Es el algoritmo más adecuado para las transmisiones de datos por internet, aunque presenta un inconveniente: *el cifrado asimétrico es lento*.

2.3.3. Principales algoritmos de cifrado

La robustez o fortaleza de estos algoritmos ya sean simétricos o asimétricos, se basa en la longitud (expresada en bits) de la clave. Entre los que se encuentran los siguientes.

Simétricos:

- **DES.** Clave de 52 bits. Es vulnerable y se puede romper la clave en un plazo de 24 horas.
- **TDES.** 192 bits. Equivale a aplicar 3 veces el algoritmo anterior.
- **RC2.** Varía entre 62 y 128 bits. Hasta 3 veces más rápido que DES y mucho más seguro
- **ICE.** Su longitud se basa en un múltiplo de 64.
- **IDEA.** Clave de 128 bits. Considerado como uno de los algoritmos más seguros actualmente.
- **AES.** Contempla claves de 128, 192 o 256 bits. Es el más utilizado actualmente.
- **Blowfish.** Claves entre 32 y 448 bits. Muy seguro, aunque lento.

Asimétricos:

- **RSA.** Clave de 128, 256, 1024 o 2048. Ampliamente utilizado
- **DSA.** Claves entre 1024 y 3072 bits. Creado para el uso de firmas digitales, aunque está en constante desarrollo para mejorar su nivel de protección.
- **ECC.** Ofreciendo el mismo rendimiento que los anteriores con claves equivalentes, pero más cortas.

2.3.4. Cifrado híbrido

Consiste en utilizar un algoritmo asimétrico para intercambiar una clave de cifrado simétrico. En este caso, si algún usuario intercepta el mensaje, solamente le serviría para descifrar ese mensaje en concreto ya que el resto de los mensajes utiliza otra clave (en este caso aleatoria).

2.4. Huella digital

Es un conjunto de bytes que se generan a partir de un documento mediante un algoritmo en concreto. De esta manera, garantizamos que:

- Cualquier mínimo cambio en el documento, produce una huella diferente.
- Es imposible obtener documento original a partir de la huella.

No sirven para cifrar un documento, pues sirven como señal de que el documento no ha sido alterado de ninguna manera. Para comprobar que esto funciona, basta con el receptor compruebe ambas huellas. Basta con que sean idénticas para saber que el documento no ha sido alterado y contiene el mensaje original sin que nadie haya podido descifrarlo.

Hay un determinado algoritmo, *hash*, que las huellas producidas por este tienen siempre el mismo tamaño en bytes. Es decir, cuantos mas bits tenga una huella, más difícil sería para que dos documentos diferentes lleguen a tener la misma huella.

Los algoritmos más utilizados son:

- **MD5:** se utiliza para generar huellas de 128 bits. 32 caracteres hexadecimales.
- **SHA1:** se utiliza para generar huellas de 160 bits. 40 caracteres hexadecimales.
- **SHA2:** dependiendo del número de bits: SHA-224, SHA-256, SHA-384 y SHA-512. Pudiendo llegar hasta los 128 caracteres hexadecimales.

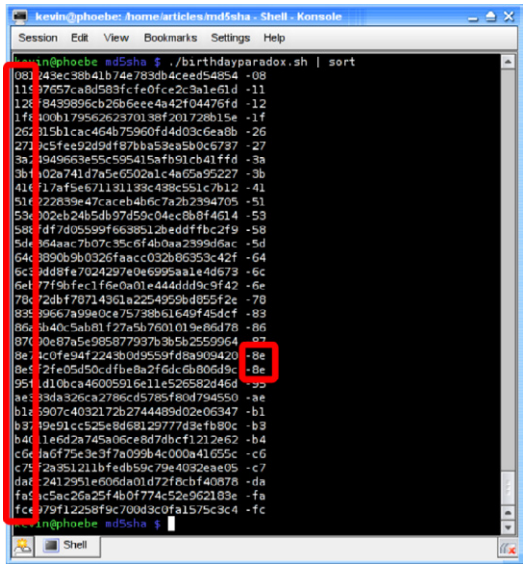


Imagen 3. Huellas generadas a partir de SHA-1

Se puede obtener un documento que genere la misma huella digital que otro mediante una técnica conocida como colisión. Aunque esto es muy difícil con algoritmos de huella digital modernos como SHA-2, MD5 y SHA-1 son vulnerables a este tipo de ataques y no se recomienda su uso para aplicaciones críticas de seguridad.

2.5. Protocolos seguros

Antes de empezar, no debemos confundir términos como *protocolo seguro* con *algoritmo de cifrado*. Un protocolo seguro no es más que un protocolo de comunicación entre usuarios para encriptar el tráfico de datos.

Tenemos el *protocolo seguro* WPA2, presentes en redes wifi, y que hace uso del algoritmo de cifrado CCMP. Este algoritmo a su vez se basa en otro algoritmo asimétrico, AES.

Otro caso conocido es el de HTTPS, la versión cifrada de HTTP, utilizado básicamente por servidores y clientes web. Este protocolo implica la instalación de un certificado digital, cuyo objetivo es el doble certificado gracias al uso del algoritmo TLS. De esta manera:

- Se consigue plena *integridad* y *confidencialidad*.
- Garantizamos a los clientes *autenticidad*,

TLS es un certificado que puede funcionar de dos maneras. De manera directa o *simple*, tan solo necesita seleccionar el certificado digital del servidor al que estemos accede. O modo *mutuo*, necesitando que el cliente se identifique con su propio certificado. En las conocidas *sedes electrónicas* es donde podemos hacer uso del algoritmo TLS en su modo *mutuo*.

2.6. Firma electrónica y certificado digital

Podemos decir que, en términos generales, la firma electrónica es un conjunto de autenticaciones electrónicas involucradas en un documento de manera digital, que pueden ser utilizadas como medio de identificación, sustituyendo a la firma autógrafa, es decir, aquella manuscrita en papel.

Permite que ambos usuarios, emisor y receptor, puedan identificarse evitando así, que terceras personas intercepten esos contenidos.

La firma utiliza medios informáticos añadiéndose así al documento digital firmado, formando un conjunto de autenticaciones.

Ese fichero electrónico es el equivalente al DNI en el mundo informático ya que:

- Garantiza una identidad única como el DNI
- Tiene fecha de caducidad y ha de ser renovado
- Es emitido por una *autoridad certificadora*. Organismos tales como la FNMT, que opera a nivel nacional.
- Tal y como ocurre con el DNI, puede requerir un pago de unas tasas.

NOTA

La firma electrónica y el certificado digital son herramientas fundamentales para garantizar la autenticidad, integridad y confidencialidad de los documentos y transacciones electrónicas en el ámbito empresarial y gubernamental, y que se utilizan en una variedad de procesos, como la firma de contratos, la presentación de declaraciones fiscales y la solicitud de servicios en línea.

2.6.1. Autoridades certificadoras de confianza

Tal y como ocurre en el mundo real, cualquier persona puede generar certificados digitales *autofirmados* para firmar o cifrar documentos, a finde cuentas, contiene una serie de claves que pueden ser utilizadas para identificarse ante otras personas, pero generan desconfianza al no tratarse de certificados generados o firmados por una *autoridad certificadora* de confianza. Se trata pues, del equivalente a un DNI falso.

En muchos sitios web que usan protocolos como HTTPS, existen este tipo de conductas. Portales que ofrecen certificados propios permitiendo el cifrado de las comunicaciones, pero a la hora de comprobar la autenticidad, resultan ser certificados digitales *autofirmados*. Por ello, al acceder a una web de este tipo, se muestra en pantalla un mensaje de advertencia, que, en cualquier caso, asusta al usuario porque no lo comprende.

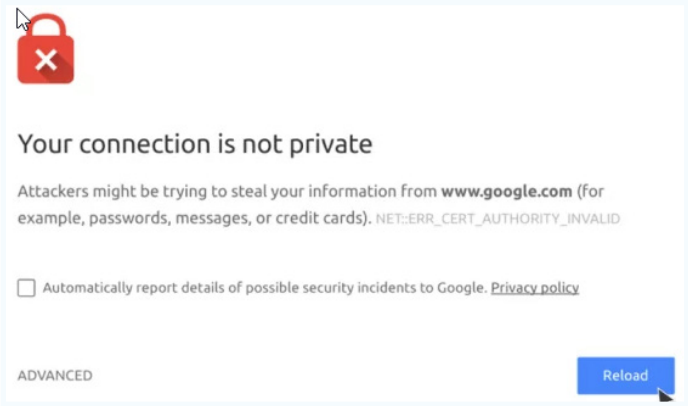


Imagen 4. Mensaje de advertencia en Google Chrome

Podríamos decir que una web que no haga uso de un certificado de confianza se tratara de una suplantación (*web spoofing*).

Todos los navegadores indican en su barra de direcciones datos de certificados bajo un candado, pudiendo ser verdes, si está todo correcto, o naranjas, si ocurre algo fuera de lo común, o rojo, cuyo significado es que el certificado está caducado o autofirmado.

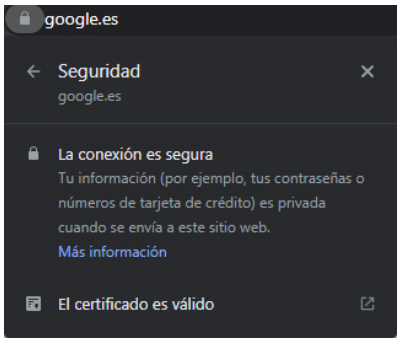


Imagen 5. Información en Google Chrome sobre la conexión de su web

Otro concepto a tener en cuenta es el llamado *revocación*. Es por el cual una CA (autoridad certificadora) decide revocar un certificado emitido por ella antes de su fecha de vencimiento, convirtiéndose en no válido. Un certificado digital válido cumple lo siguiente.

- Comprobar si lo ha emitido una CA de confianza.
- Comprobar si la fecha del certificado es vigente.
- Consultar, si fuera necesario, con la CA si el certificado sigue siendo válido para su uso.

Una página web HTTPS con una advertencia de color rojo, significa que el certificado ha sido rechazado por una autoridad certificadora. Al tratar de acceder a una sede electrónica, tendrá el acceso denegado.

Un certificado web sirve para identificar a una persona física o una entidad judicial. Del mismo modo, también se usa para identificar a servidores o usuarios via web. Dentro del propio certificado vienen una serie de especificaciones para conocer para conocer si se trata de un tipo de persona, entidad o servicio.

2.6.2. Autoridades certificadoras raíz e intermedias

Existen diferentes entidades subordinadas que, elegidas por una CA, se encargan de la tarea de generar y firmar certificados digitales.

De esta manera, un CA delegada será de confianza si su CA raíz lo es. Se crea con ello una *cadena de confianza* ya que la comprobación de un certificado digital emitido por una CA intermedia implica que llegue desde hasta la CA raíz.

La existencia de estas autoridades intermedias genera una confianza en el usuario final en nombre de las CA de la raíz nacional. Sin embargo, las CA intermedias pueden revocar solamente los certificados emitidos por ellas, pero no los de la CA raíz. Al contrario que una CA raíz, la cual puede revocar certificados emitidos por cualquier CA delegada por ella misma.

2.6.3. Almacén de certificados

Existen en todos los sistemas operativos un *almacén de certificados* donde se almacenan todos los certificados, según su tipo y el uso que se vaya a hacer de ellos. Está dividido en carpetas y es el desarrollador del sistema el que se encarga de seleccionar los que quiera incluir en su sistema. Las actualizaciones del sistema permiten renovarlos, eliminar los que no sean de confianza y la inclusión de nuevos certificados de la CA raíz.

Windows 10 dispone de una herramienta llamada *Administrar certificados de equipo* para gestionar dicho almacén dentro del sistema operativo.

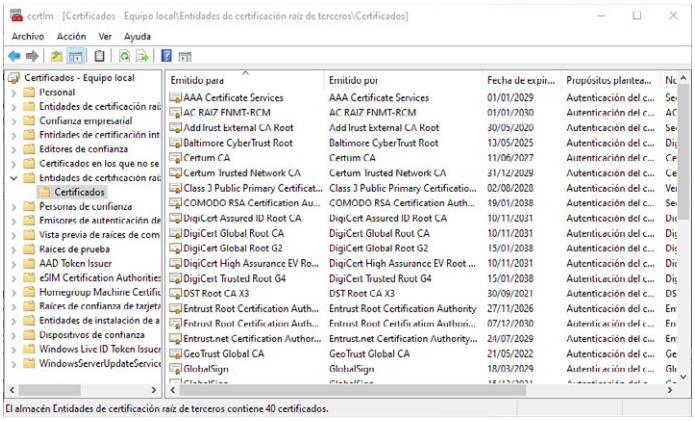


Imagen 6. Lista de certificados de la raíz intermedia o de terceros

Cabe destacar que ciertas aplicaciones (como el caso de Google Chrome), actúan con su propio almacén de certificados, el cual solo sirve para obstaculizar el uso al usuario, desconcertándolo en todo caso ante problemas de autenticación.

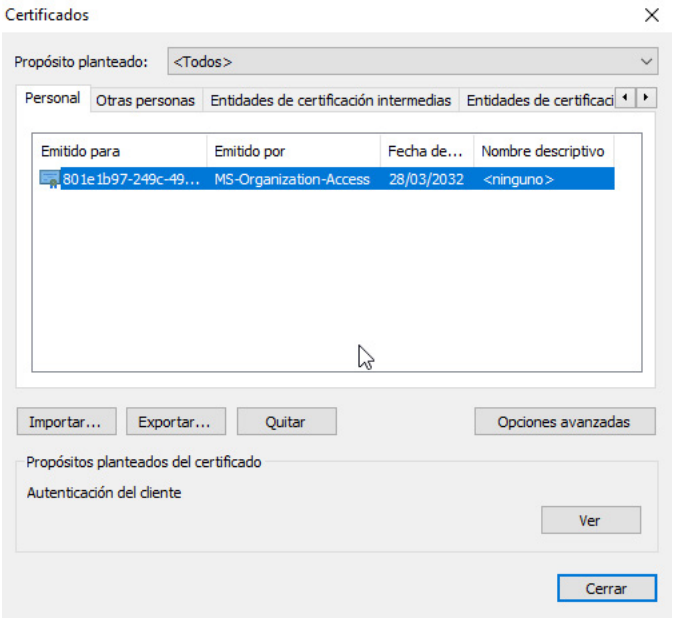


Imagen 5. Ventana de gestión de certificados en Chrome

2.6.4. La problemática de la CA raíz españolas

La obtención de un certificado por parte de una entidad raíz puede ser un proceso tedioso y complicado, similar a la obtención del DNI, y la falta de conocimiento por parte del usuario es uno de los principales problemas.

Además, la FNMT es reconocida como una CA raíz de confianza por algunos sistemas operativos, como Windows, pero no por otros como Mac o Linux. Por lo tanto, los usuarios pueden verse obligados a descargar los certificados e instalarlos manualmente en la carpeta correspondiente. Es cierto que los navegadores pueden tener algoritmos de cifrado diferentes, lo que puede provocar problemas al utilizar la firma electrónica, y que el software que permite la firma electrónica es escaso. Además, algunas páginas web de organismos oficiales pueden resultar incomprensibles para el usuario.

Los principales problemas son:

- Falta de conocimiento por parte del usuario. Al final, este *no sabe que debe instalar* o no sabe cómo hacerlo. Ocurre lo mismo si es el instalado con el DNIe, no disponiendo de lector de tarjetas o de los *drivers* de este.
- La FNMT *no se tiene en cuenta como raíz de confianza* por ningún sistema operativo de uso genérico. Windows, Mac, Linux. El usuario se ve obligado a descargar los certificados e instalarlos en la carpeta correspondiente.
- Todos los navegadores *trabajan con algoritmos de cifrado diferentes*. Es asiduo que una sede electrónica funcione con un navegador, pero no con otro.
- El *software que permite la firma electrónica* es escaso.
- Es muy habitual ver varias páginas de *organismos oficiales* que, intentando aclarar ideas, resultan incomprensibles para el usuario.

Muchas sedes electrónicas se ven obligadas a proporcionar al usuario un paquete *software* que solucione el acceso al usuario, que, al ser instalado, cuenta con una serie de certificados y librerías haciendo posible la instalación adicional de otro tipo de *software* de firma electrónica.

Que claro que el principal obstáculo es que no está normalizado, por eso hay una *falta de formación* en un tema tan complicado como este.

2.6.5. Infraestructura de clave pública (PKI)

El término PKI o *infraestructura de clave pública*, se utiliza para referirse al conjunto de procedimientos necesarios para crear, manipular, distribuir y utilizar cifrados de clave pública. Existen además de las CA, autoridades encargadas de otros cometidos, como las *autoridades registradoras* (RA), cuya misión es aceptar cualquier petición de certificados por parte de personas u organismos que lo soliciten, garantizando con ello su autenticidad.

Podría decirse que, en realidad, las PKI son el *sotfware* y *hardware* necesario para dar servicio de certificación digital.

2.6.6. Consejos sobre certificados digitales

Hay que seguir una serie de consejos, que son:

- Evitar la instalación del certificado en ordenadores no seguros. Si no hubiera alternativa, desinstalarlo después de su uso.
- Si el equipo en el que va a instalar el certificado es usado por varias personas, procurar instalar este dentro de la sesión del propio usuario, nunca compartido.
- No llevar documentación sin cifrar en dispositivos de almacenamiento externo.
- Si disponemos de lectores con código pin, como es el caso del DNI 3.0, podemos hacer uso de certificados con tarjeta y código PIN.

2.7. Malware

Términos como *malware* o *software* malicioso, engloban aquel *software* intrusivo y molesto, que no debe confundirse con un *virus informático*, pero que, en realidad, es uno de estos diversos tipos.

El *malware* es un *software* que se instala en el sistema operativo sin que el usuario sea consciente, y se ejecuta sin su consentimiento. Su objetivo abarca desde pequeñas bromas o demostraciones de que alguien ha entrado al sistema a su antojo, hasta el borrado o secuestro de datos, pasando por la apropiación de contraseñas.

Las medidas que se adoptan se denominan *seguridad activa*, pues están en constante supervisión por un administrador, por ejemplo, la actualización de un sistema operativo. Las medidas a adoptar son las siguientes:

- **Uso de software legal.** El *software* ilegal puede contener *malware*. Normalmente se ha de desconfiar de cualquier *software* gratuito, a excepción del *open source*.
- **Mantener siempre el sistema operativo actualizado.** Las compañías informan junto a cada actualización, la información de las vulnerabilidades conocidas y que se han solucionado con esa actualización.
- **Instalar un software antivirus.** Este tipo de aplicación monitorea el sistema operativo en busca de actividades sospechosas.

En entornos empresariales, es altamente recomendable contar con una solución *antimalware*. Se trata de aplicaciones muy similares a un antivirus doméstico, pero que cuentan con actualizaciones centralizadas que simplifican la labor del administrador.

Se podría decir que una buena medida de protección es la suma de *antivirus* + *sentido común.* Así mismo, una buena formación ayuda a que la suma tenga mejores resultados.

2.7.1. Tipos de malware

Malware infeccioso: virus y gusanos

Es aquel cuyo ciclo de vida consta de dos fases: infección de ficheros ejecutables o sistemas a través de la red y ejecutar su cometido hostil. Recibe el nombre de *virus informático*, aunque es importante distinguir entre *virus* y *gusano*. Mientras que el virus necesita la intervención del usuario para ejecutarse e iniciar su infección, el gusano aprovecha ciertas vulnerabilidades del sistema (vectores de infección o ataque) para instalarse en él y autoejecutarse.

Un ejemplo de lo que sería un virus, es el contenido en un fichero adjunto recibido por correo electrónico y que el usuario, sin darse cuenta, lo ejecuta y se propaga.

Un ejemplo de gusano es, el hasta la fecha considerado el último de los grandes ciberataques masivos, WannaCry.

Puerta trasera

Una puerta trasera o *backdoor* es un método para iniciar sesión en un sistema evitando el proceso de autenticación. Es instalado por un virus que ya se encuentra en el sistema que se auto elimina una vez que ha conseguido su cometido. Permanece oculto esperando un vínculo con algún servidor exterior y que, una vez conectados, su fin es la sustracción de datos o el uso de recursos ajenos con fines delictivos, como el envío de *spam*. Este servidor controlador puede manipular los equipos *zombis* a través de una *botnet*, es decir, envío de spam y de ataques DoS.

Drive-by downloads, adware, hijackers, phishing

Cuando un servidor web es atacado, se hace principalmente a través del código HTML que este alberga, de manera que se introducen una serie de *scripts* maliciosos que los clientes ejecutan sin saberlo. Si se trata de una descarga no consentida, se trata de un *drive-by downloads*; la aparición de ventanas de publicidad emergente de forma descontrolada se llama *adware*, y si hablamos de *hijack*, es un tipo de *malware* que secuestra de alguna manera la configuración del navegador pudiendo mostrar publicidad o pornografía.

Una de las amenazas de seguridad a las que se exponen los usuarios durante la navegación web es el conocido *phishing*. Consiste en páginas web falsas que suplantan la identidad a las verdaderas para que el usuario, sin darse cuenta, introduzca información sensible. Es muy común en entornos bancarios online, donde se busca recopilar las credenciales de los usuarios que acceden a estos portales vía web.

Un camino muy parecido lleva a cabo el *software* de *pharming*. Este altera el funcionamiento del DNS para redirigir el dominio de una web a otra maliciosa.

Para evitar eso, el *software* antivirus "vigila" las URL a las que accede el usuario, informando de que el sitio visitado es malicioso.

Las empresas suelen utilizar un sistema *proxy* para vigilar la actividad de las páginas webs a las que acceden sus empleados, ya sea por motivos de seguridad como para evitar que sean menos productivos.

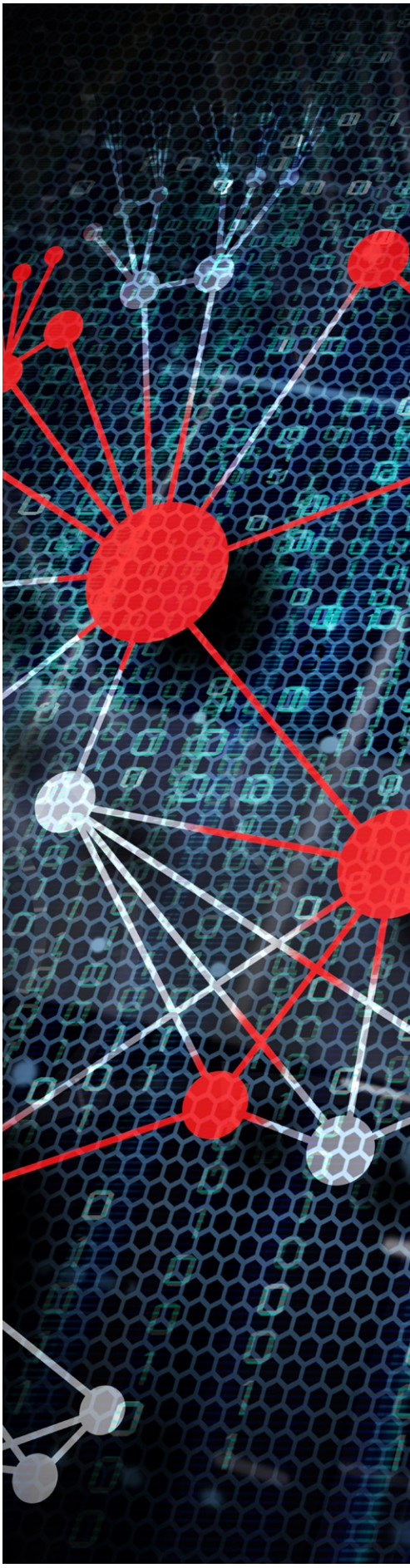
Otra medida de seguridad más simple es aquella la cual utiliza un servidor DNS para redirigir los dominios a los que permite conexión. Un producto que representa este tipo de servicio es OpenDNS (www.opendns.com). Entre sus productos encontramos una solución doméstica que funciona de la siguiente manera:

1. Los equipos deben utilizar los siguientes servidores DNS: 208.67.222.123 y 208.67.220.123
2. Cuando un usuario se conecta a una URL, consulta primero en el servidor DNS la dirección IP del dominio al que intenta acceder.
3. Si OpenDNS considera esa IP como maliciosa, se le devuelve un mensaje de aviso en pantalla y evitando el acceso a la misma.

Troyanos

Es un *malware* oculto dentro de un *software* que invita a ser ejecutado por parte del usuario. Una vez que el usuario ejecuta el *software*, realiza su tarea maliciosa o si instala de manera silenciosa sin que se percate el usuario, para actuar pasado cierto tiempo.

La gran diferencia entre troyano y virus es que un virus, es un fragmento de código que se adhiere un *software* seguro, infectándolo. Un troyano es un programa que se supone que va a realizar algún tipo de acción, pero realmente su intención es dañina. Por lo tanto, hay que tener mucho cuidado con la descarga de programas gratuitos.



Rootkits y bootkits

Un rootkit es un código que los atacantes utilizan para dar más privilegios al administrador. Bootkit es una versión de rootkit que ataca al sector de arranque (MBR, Master Boot record), por lo que es difícil de detectar. Es por esto por lo que hay que confiar plenamente en el software de seguridad que nos proteja.

Keyloggers, stealers y spyware

Un *keylogger* es un tipo de *malware* que registra las pulsaciones de teclado del usuario en busca de patrones repetidos, pudiendo ser contraseñas o números de tarjetas de crédito. De hecho, en el momento que obtiene ese tipo de información, la envía de vuelta al creador del *malware*. Otra forma de trasmitir al delincuente este tipo de contraseñas, son los llamados *stealers*, que obtienen los datos de los repositorios en los que los navegadores guardan la información referente a contraseñas y auto rellenado de formularios.

Las webs de muchos bancos muestran un teclado en pantalla, para que el usuario pueda introducir su contraseña mediante clics de ratón en lugar de teclear, ya que es una medida de seguridad ante los *keylogger*.

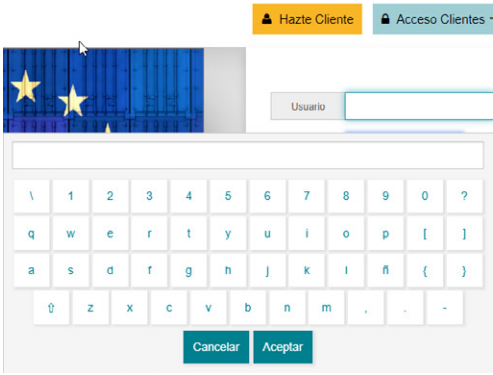


Imagen 7 Teclado en pantalla en el acceso a la banca online. *Fuente: cajamar.es*

Los programas *spyware* se dedican a recopilar información sobre diversas actividades del usuario para venderla posteriormente a empresas de publicidad.

Ransomware

Posiblemente sea el *malware* más peligroso de todos, debido a los efectos que provoca. Suele infectar los equipos a través de puertas traseras como los troyanos y una vez acceden al sistema, se encargan de la encriptación de todos los ficheros que puedan contener información vital. Para ello utilizan una serie de algoritmos de cifrado que resultan muy complicados de romper sin el uso de la contraseña. El famoso WannaCry mostraba directamente una ventana que bloqueaba el equipo por completo.

Imagen 8 Ventana de advertencia de WannaCry

Minería

Este malware llamado minería de monedas se apropia de los sistemas para minar o crear criptomonedas sin el consentimiento de la víctima.

2.7.2. Software de seguridad

Muchos fabricantes pretenden destacar el hecho de que son capaces de impedir diferentes tipos de amenazas, no solo las que tengan relación con los virus. Todo *software* de seguridad realiza más o menos las mismas tareas:

- Emplea una base de datos donde el fabricante almacena información del *malware* que conoce junto con lo imprescindible para detectarlo (patrones de código). Esta base de datos se actualiza *diariamente*.
- Examina el contenido de la memoria RAM, de los ficheros del sistema y de otros directorios en busca de amenazas.
- Si encuentra una amenaza que no conoce, analiza su comportamiento a través de reglas *heurísticas*.
- Cuando encuentra una amenaza, bloquea su acceso hasta que infiera el usuario y lo mantiene en cuarentena por si prefiere borrarlo o restituirlo.
- Puede enviar datos al fabricante sobre las amenazas que encuentra para que este sea investigado con mayor detenimiento

El malware solo resulta una amenaza cuando está incluido en ficheros ejecutables. En sistema Linux y Mac, solo los ficheros con permiso de ejecución (x) y las librerías pueden contener amenazas. Sin embargo, en sistemas Windows, existen varias extensiones que pueden contener un trozo de código ejecutable, siendo las principales .exe, .com y .dll.

Así mismo, además de este tipo de archivos, hay otros muchos tipos de ficheros en los que actúa el *software* de seguridad, tales como zip, rar, iso, etc.

Para finalizar, existen otro tipo de documentos que pueden contener *macros*. Por ejemplo, un documento Excel (.xlsx). Este puede contener una macro que se ejecute cuando el usuario hace clic en algún elemento ubicado en una celda. Suelen contener rutinas maliciosas, y el principal problema es que cierto tipo de macros simplemente se activan al abrir el documento.

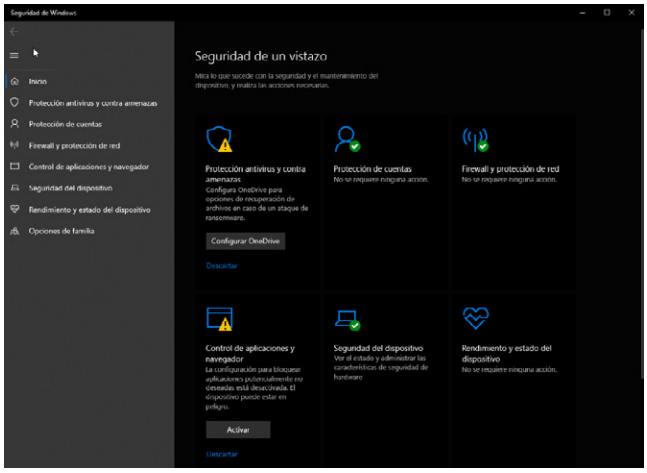


Imagen 9 Windows Defender

Lo que es imposible es que cualquier formato de archivo de imagen, tipo JPG o PNG contenga ningún tipo de *malware*. A la hora de configurar el *software* de seguridad, es posible definir qué archivos o carpetas del sistema van a ser analizados, el horario de ejecución, etc.

NOTA

Además, es importante tener en cuenta que los archivos de imagen como JPG o PNG pueden contener exploits que aprovechan las vulnerabilidades del software que los abre para ejecutar malware. Por lo tanto, es importante mantener actualizado el software de seguridad y evitar abrir archivos de fuentes desconocidas o sospechosas.

2.7.3. Desinfección

Tras detectar un tipo de *malware*, siempre hay que tener en cuenta lo siguiente:

- ¿Cabe la posibilidad de desinfectar el sistema y devolverlo a un estado anterior la infección?
- ¿Se pueden eliminar o mitigar los efectos del *malware?*

Si el *software* no consigue eliminar el virus y el sistema se ve afectado, es el propio administrador el encargado de llevar a cabo una restauración o instalación del sistema operativo desde cero.

Existen otras soluciones como las imágenes de respaldo, pero para que esta solución sea efectiva, se deberá tener en cuenta el momento preciso de la infección, o de lo contrario se podría estar perdiendo el tiempo.

En la mayoría de los casos, los efectos provocados por *malware* dentro del sistema se desvanecen una vez eliminado del mismo. Mientras que un *keylogger* deja de enviar información por la cual haya sido creado, no ocurre lo mismo con un *ransomware*, ya que ha dejado al sistema inservible desde el inicio de la infección.

En cuanto al malware más difícil de eliminar, nos encontramos con el sistema *botnet,* puesto que aprovecha la puerta trasera. En estos casos, se realizará lo siguiente.

1. Cerrar la puerta trasera por la que accede el *malware*. En muchos casos, se corrige con la actualización del sistema.
2. Detener la comunicación con el servidor controlador.
3. Verificar con qué tipo de privilegios se está ejecutando el *malware*.
4. Analizar la forma de actuar del *malware*.

2.8. Spam

En España, el correo electrónico no solicitado, spam o correo basura, la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) de 2002 y el Reglamento general de Protección de Datos (RGPD) establece ciertas condiciones que deben cumplirse para enviar correos publicitarios y exige la posibilidad de darse de baja de esas suscripciones en cualquier momento. Por otro lado, el Reglamento General de Protección de Datos (RGPD) establece que el correo electrónico no solicitado debe contar con el consentimiento previo y explícito del destinatario.

Al enviar correos de spam, se atenta contra los datos privados de los usuarios. Además, este tipo de spam puede portar un *malware* y llevar a cabo *physing*.

2.8.1. Software antispam

Las medidas antispam son unas estrategias efectivas que evitar que el correo no deseado sea recibido. El software que lo ejecuta se instala en los servidores de correo electrónico y evalúa los mensajes para decidir si son spam o no. Según como se configure ese software, este almacenará los correos con una etiqueta diferente o directamente los eliminaré. Para clasificar estos mensajes como deseados o no deseados, se siguen dos métodos:

- Comprobar la lista negra de dominios (Realtime Blackhole List, BHL) en la que se recogen los dominios de los que se desea no recibir mensajes.
- Emplear algoritmos de inteligencia artificial para calcular la probabilidad de que ciertos mensajes sean spam. Normalmente, estos mensajes basura cuentan con un número de destinatarios y de enlaces elevado.

Sin embargo, hay que tener cuidado con los mensajes que son clasificados como spam cuando no lo son en realidad. Por otro lado, la gran mayoría del spam proviene de servidores *botnets* o secuestrados, por lo que debemos protegernos de las puertas traseras.

El principal sistema para añadir dominios de correos no deseados consiste en ofrecer un número de direcciones de correo trampa, llamadas honeypots o tarros de miel, para que, si les llegan los correos basura a esas direcciones, se confirmaría el caso de spam y podrían clasificarse como tal.

2.8.2. Registros SPF

Para evitar ser detectado por la RBL como spam al enviar correos electrónicos masivos pero necesarios, por ejemplo, en el mundo empresarial, se utiliza el Sender Policy Framework (SPF). Este sindicato recoge información sobre los servidores que sí están autorizados. El DNS registra comprueba si el dominio es fraudulento o legítimo y así actuará para clasificarlos.

Las fases de este proceso son:

1. El servidor SMTP fraudulento envía un mensaje que, aparentemente, es spam.
2. El servidor DNS comprueba la IP de origen para asegurarse de si se trata de un servidor legítimo o fraudulento.
3. El mensaje es clasificado como spam si es fraudulento; si no, es legítimo y se saca de la clasificación de spam.

2.8.3. Correo legítimo

No siempre el correo publicitario ha sido enviado de forma ilegal, sino que el usuario ha firmado o dado su consentimiento para recibir ese tipo de envíos. Sin embargo, esos dominios tienen que permitir al usuario darse de baja de esa suscripción de correos en cualquier momento mediante un enlace denominado "darme de baja".

2.9. Actualización del sistema y de las aplicaciones

Los ataques externos aprovechan las vulnerabilidades o *exploits* del software para entrar en el sistema, que se deben intentar evitar con parches en el proceso de actualización. Con el parche, los ficheros defectuosos de actualizan con una versión actualizada del código erróneo. Que exista una actualización no implica necesariamente que no pueda haber errores, de hecho, si esto sucede, se puede volver a la versión anterior, llamada *downgrade*. Por este motivo, los administradores tienen la posibilidad de aceptar o de desestimar las actualizaciones. Los desarrolladores de software clasifican las actualizaciones entre normales y de seguridad (*security updates*) para que los administradores sepan cuáles deben aceptar y cuáles pueden desestimar.

Los certificados de vulnerabilidad de las actualizaciones disponibles se denominan CVE (Common Vulnerabilities and Exposures). Este certificado fue creado para determinar el nivel de vulnerabilidad de las actualizaciones mediante los identificadores CNA (CVE Numering Authorities).

2.9.1. Windows Server Update Services (WSUS)

El objetivo de WSUS es convertir el servidor en un banco de actualizaciones disponibles para servidores y equipos. Este servidor conlleva la instalación del servicio ISS (Internet Information Services) para comunicarse mediante HTTP.

Las ventajas de este servidor son:

- **Ahorro de ancho de banda**, puesto que la mayoría de los servidores atacan a los servidores llamados *upstream servers* en lugar de conectarse directamente a Microsoft.
- **Control de paquetes de actualizaciones**, ya que se pueden clasificar las actualizaciones según el destinatario y la estabilidad para aplicarlas o rechazarlas.
- **Automatización de la distribución de actualizaciones**, porque se puede determinar el momento en el que se quiere aplicar la actualización para evitar parones de productividad.

2.9.2. Repositorios locales en Linux

Linux crea una copia espejo local de los repositorios oficiales. Después, el administrador pueda controlar las actualizaciones de los equipos de las siguientes formas:

- No sincronizando la copia espejo con el repositorio original.
- Conectar aptget solamente en algunos equipos en remoto para comprobar la estabilidad de las actualizaciones y, así, poder descargarlas en el resto de los equipos de la copia espejo.
- Sincronizando la actualización únicamente cuando se confíe en su estabilidad y seguridad. Para garantizarlo, el comando debmirror (existen otras alternativas como "apt-mirror" o "reposync".) utiliza la herramienta rsync de manera interna.

2.10. Hardening

Se trata de un término que puede traducirse como "endurecimiento" de las políticas de seguridad en las opciones de configuración de un *software* o *hardware* para adaptarlo a las necesidades del usuario.

Existen entidades que se encargan de clasificar los posibles ataques y elaborar un paquete de soluciones a los administradores del sistema, facilitando así la labor de estos. Se pueden buscar en internet y seguir ciertas pautas de diseño o implementar las reglas recomendadas. Los tres casos más relevantes son:

- **Fundación OWASP (open Web Application Security Project).** Esta entidad se centra en la seguridad de las aplicaciones web y en los riesgos asociados a su desarrollo y uso. Proporciona información sobre las vulnerabilidades más comunes, así como herramientas y recursos para mejorar la seguridad de las aplicaciones.
- **Consorcio WASC (Web Application Security Consortium).** Al igual que OWASP, esta entidad se enfoca en la seguridad de las aplicaciones web, proporcionando información y herramientas para proteger las aplicaciones de los ataques.
- **CIS (Center for Internet Security).** Esta entidad ofrece guías detalladas sobre cómo endurecer la seguridad de los sistemas operativos, aplicaciones y dispositivos de red, entre otros. Sus guías de seguridad, conocidas como benchmarks, se pueden descargar gratuitamente después de un registro.
- **CNN (Centro Criptológico Nacional),** perteneciente al CNI (Centro Nacional de Inteligencia). Analiza y elabora informes sobre seguridad y hardening en general y de manera particular.

2.11. Seguridad en la red corporativa

Una red es un conjunto de nodos que se comunican entre ellos al estar unidos, pudiendo hacer referencia a servidores, equipos, routers... la seguridad de la red corporativa o empresarial es necesaria para garantizar que solo se conecten a una red concreta los equipos autorizados.

2.11.1. Seguridad de redes cableadas

En una red cableada, para acceder sin ser detectado no es necesario conectarse físicamente a la red a través de un cable. De hecho, es posible acceder de manera remota mediante herramientas de hacking y técnicas de penetración. Sin embargo, para conectar físicamente un equipo a una red cableada, efectivamente se puede hacer a través de:

- Router o *switch* de la red; sin embargo, no es posible si los dispositivos están en un CPD protegido.
- Toma de datos de red (roseta) libre.
- Suplantando a un ordenador autorizado a través del latiguillo (cable de red).

Control de equipos por dirección MAC

Los servidores DHCP se utilizan para facilitar la configuración de las interfaces de los quipos de una red. A través de una asignación fija o estática de direcciones IP, se puede asignar una misma IP para una misma MAC. Por tanto, para asegurar la red cableada ante accesos no autorizados se puede asignar una lista de direcciones IP fija y deshabilitar la asignación dinámica.

La opción *IP-MAC binding* permite que los *switchs* sean configurados para que cada equipo se conecte desde un determinado puerto. Por otro lado, también se puede crear una lista de control de acceso (ACL).

Sin embargo, cuando un atacante accede mediante un *sniffer* y analiza los rangos de IP y MAC para suplantarlos, un equipo extraño accede a la red con la misma IP que otro equipo ya reconocido.

Servidores rogue DHCP

Un servidor rogue DHCP es aquel que no está controlado por un administrador, por lo que los dispositivos que utilicen una dirección IP de manera ilegítima podrán acceder a la red antes que los servidores de la empresa. Este ataque de intermediario (*man in the middle* o MITM) implica que el atacante configure en la red un servidor DNS o *gateway*.

Registro de equipos en un dominio

El administrador es el único que da acceso a los dominios Active Directory. Este dominio almacena los usuarios y equipos autorizados en su base de datos mediante certificados digitales. Estas configuraciones de realizan a través del sistema de políticas de grupo (GPO). Por consiguiente, si un atacante consiguiera acceso a la red, no podría iniciar sesión por no estar reconocido por el dominio. Esta medida no se puede desactivar puesto que forma parte de la configuración propia de Active Directory.

IEEE 802.1X

Este protocolo es utilizado para autenticar a usuarios y equipos tanto de redes cableadas como inalámbricas. Este protocolo surgió como una alternativa más segura de PPP (Point-to-Point protocol), dejando de utilizar el usuario y su contraseña para utilizar el protocolo EAP, pudiendo elegir distintos tipos de autenticación.

Ningún intruso o atacante podrá acceder a una red cableada basada en IEEE 802.1X, pues su transmisión será denegada al no poder iniciar sesión. Para poder acceder, es necesario que:

- Todos los equipos de la red o suplicantes (*supplicants*) y los *switchs* o autenticadores (*authenticators*) deben estar configurados siguiendo el protocolo IEEE 802.1X.
- Debe existir un servidor de autenticación (*authentication server*) que verifique las credenciales a través del protocolo RADIUS.

VLAN

La función de un *switch* es la de reenviar paquetes. Cada paquete incorpora en su cabecera una dirección IP origen y su dirección destino. Gracias a este tipo de información, el *switch* la guarda en su memoria y la usa para crear una "agenda" de los equipos conectados a la red. Si el paquete viene por un puerto con una determinada IP, el *switch* redirige ese paquete a su destino a través del mismo puerto.

Pero esto no ocurre en entornos empresariales en los que, en muchas ocasiones, los paquetes van redirigidos a uno o varios puertos, lo que conocemos como paquete *broadcast*. De esta manera, nace la necesidad de configurar un grupo de puertos de manera independiente, para evitar la propagación innecesaria de la información. Si un paquete tiene orden de entrar por esos puertos, no podrá reenviarse por los que no formen parte de ese grupo. Es lo que se conoce como *red virtual* o *VLAN*.

Un *switch* avanzado tiene la posibilidad de trabajar con una sola VLAN o con varias, así como un mismo puerto puede pertenecer a más de una VLAN.

SNMP

Este protocolo (Simple Network Management Protocol) se utiliza para obtener información de equipos y dispositivos para poder configurarlos según dos comunidades:

- **Lectura o public:** permite que cualquier equipo pueda enviar los comandos a otro dispositivo para obtenerinformación, solicitando OID (*Object Identifier*).
- **Lectura y escritura o private.**

Los valores de estas comunidades pueden modificarse a través de un comando similar llamado snmpset. SNMP puede implicar ciertos problemas puesto que cualquier usuario puede indagar y obtener información. Sin embargo, su tercera versión solucionó este problema añadiendo autenticación y cifrado a las comunicaciones.

2.11.2. Seguridad de redes inalámbricas

Hay un gran número de problemas de seguridad ocasionados por los accesos no autorizados y no controlados en redes inalámbricas, puesto que en las redes cableadas necesitan un acceso físico y en las redes inalámbricas no. De hecho, cualquier atacador que pueda acceder a la cobertura de la red wifi, puede conseguir acceso y conexión. Además, cualquier dispositivo inalámbrico puede detectar las redes wifi-existentes en su entorno (SSID) y analizar el tráfico sin ser detectado.

El cable virtual que une al equipo con el punto de acceso facilita al intruso comunicarse con el resto de los equipos de la red.

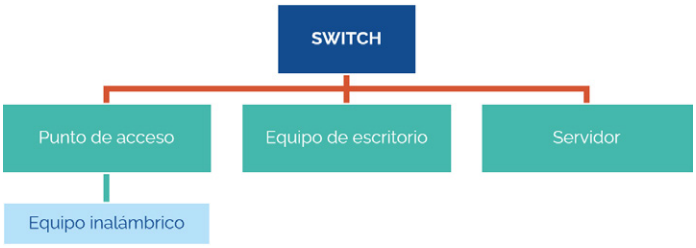


Imagen 10. Red mixta (cableada e inalámbrica).

Línea roja: cable ethernet.

Línea verde: cable virtual (inalámbrico).

WEP, WPA y WPA2

El protocolo WEP (Wired Equivalent Privacy) utilizaba un cifrado RC4 con claves de 64/128 bits, que era muy vulnerable a ataques estadísticos y podía ser descifrado fácilmente. Además, su método de detección de errores mediante CRC podía ser sustituido o alterado sin necesidad de conocer la clave WEP.

Posteriormente, se introdujo el protocolo WPA (Wifi Protected Access), que utilizaba el sistema TKIP para generar claves dinámicas de 128 bits para cada paquete, lo que aumentó la seguridad y utilizaba el algoritmo MIC en lugar de CRC. Aunque más seguro que WEP, WPA también presentaba vulnerabilidades.

Finalmente, se creó el protocolo WPA2, que utiliza el cifrado AES y es obligatorio en todos los dispositivos wifi. El WPA2 empresarial cuenta con varias ventajas:

- Cada usuario cuenta con su propia contraseña, por lo que no es necesario que las contraseñas wifi sean públicas.
- Las contraseñas no se necesitan ni memorizar ni actualizar, puesto que son renovadas siguiendo la política de contraseñas de la empresa.
- La red almacena los datos y las actividades del usuario, por lo que la seguridad aumenta.
- Para acceder a la wifi, necesitas ser un miembro autorizado, por lo que los usuarios bloqueados o deshabilitados no pueden acceder.
- Para autenticar los accesos, se puede usar Windows Server como servidor RADIUS.

WPA3

El protocolo WPA3 es el más reciente, contando con un cifrado de 192 bits, mejorando las vulnerabilidades de WPA2. Igualmente, se presentan las versiones personal y empresarial. Siempre que este protocolo esté disponible, se usará frente a otros.

WPS

El protocolo WPS (Wifi Protected Setup) permite que un dispositivo se conecte a una red inalámbrica de forma sencilla sin necesidad de ingresar una contraseña. Esto se logra a través de un botón WPS en el punto de acceso o mediante la introducción de un PIN de 8 dígitos preestablecido en el dispositivo que se quiere conectar. Sin embargo, el uso de WPS con el botón y con PIN es considerado inseguro debido a que es vulnerable a ataques de fuerza bruta que intentan adivinar el PIN. Por esta razón, se recomienda que los usuarios desactiven la función WPS en su red inalámbrica para mejorar la seguridad.

Imagen 11. Botón WPS

Hotspots

El término Hotspot se refiere a un punto de acceso inalámbrico público que permite a los usuarios conectarse a internet de forma inalámbrica. Por lo general, no se necesita una autorización previa para conectarse a un hotspot, aunque es común que los usuarios deban aceptar los términos y condiciones de uso.

Un hotspot no requiere un firmware especial y cualquier dispositivo con capacidad wifi puede conectarse a él. Los puntos de acceso inalámbricos pueden configurarse como hotspots mediante la creación de una red independiente y aislada, por lo que se recomienda la instalación de redes separadas para la red inalámbrica y la red cableada empresarial.

Algunas de las características comunes de un hotspot pueden incluir:

- Una ventana de condiciones de uso que el usuario debe aceptar antes de acceder.
- Publicidad para la empresa del servicio hotspot.
- Limita el acceso a ciertas URL (proxy web), a elección de la empresa.
- Limita el tiempo de utilización de la wifi para evitar un uso abusivo.
- Establece un sistema de pago según el tiempo límite.

La instalación de un hotspot puede requerir la contratación de una línea de acceso a Internet dedicada y la implementación de un cortafuegos para separar la red inalámbrica del resto de la red empresarial.

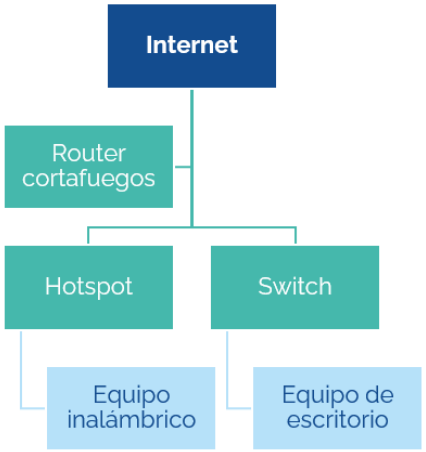


Imagen 12. Separación de redes en Hotspot.

Ataques a redes wifi

1. **Obtención de contraseña mediante suplantación de SSID**

   Cualquier atacante es capaz de montar un punto de acceso con el mismo SSID que la red a la que intenta atacar. Si el usuario, sin percatarse, se conecta a dicho punto, se ve comprometido. Es lo que se llama punto de acceso "furtivo" (*rogue access point*).

Determinados dispositivos inalámbricos de gama profesional tienen un *software* especial capaz de avisar en caso de detectar puntos de acceso con el propio SSID.

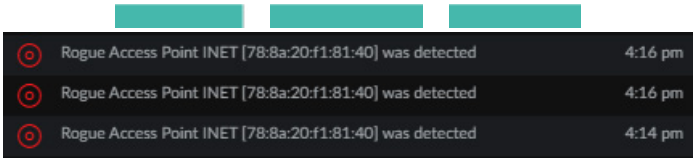


Imagen 4. Alertas de detección desde un punto de acceso.

Es cierto que un atacante puede crear un punto de acceso furtivo con el mismo SSID que la red original para obtener las contraseñas de los usuarios que se conectan a él. Sin embargo, es importante mencionar que este ataque es menos efectivo si la red utiliza cifrado de tipo WPA2 con una contraseña segura, ya que es difícil de romper mediante ataques de fuerza bruta o diccionario.

2. **Denegación de servicio (DoS, Denial of Service)**

   Un atacante puede emitir una señal de ruido para interferir en la comunicación de la red wifi y enviar paquetes falsos para expulsar a los usuarios legítimos. Pero también es importante mencionar que, en general, este tipo de ataque requiere de una gran cantidad de recursos y es menos efectivo en redes wifi modernas que utilizan protocolos de seguridad como WPA2..

   Por otra parte, no toda la comunicación inalámbrica se cifra: existen diversos paquetes de gestión que no viajan cifrados los cuales se convierten en objeto de ataques.

3. **Secuestro de sesión**

   Cuando un usuario permitido, conectado a una red wifi, navega a través de páginas web donde inicia sesión, cabe la posibilidad de que sus credenciales sean atacadas y utilizadas posteriormente para suplantar la identidad del usuario en la web. En cualquier caso, la mejor medida de seguridad es que los usuarios jamás introduzcan datos comprometidos en internet, y siempre lo hagan en páginas web HTTPS (cifradas). Por ello:

   - Nunca hay que navegar con HTTP.
   - HTTPS no está exento de ataques si se utilizan protocolos wifi poco seguros.

2.11.3. Monitorización del tráfico de red

Para detectar accesos de atacantes ilegítimos a una red wifi, se puede monitorear el tráfico de la red capturando los paquetes de datos y analizándolos para encontrar evidencias. Esta tarea es complicada por los protocolos de red que se necesitan, por lo que se suele hacer uso de esta medida cuando ya ha surgido el problema y no como medida preventiva.

Las herramientas que permiten monitorizar este tráfico de red son conocidas como *sniffers* o analizadores de paquetes (*packet analyzers*). Los más importantes son:

- Tcpdump.
- Netsniff-ng.
- Wireshark.
- Firmware en dispositivos red.

NOTA

La monitorización del tráfico de red también se puede usar como medida preventiva para detectar vulnerabilidades en la red y corregirlas antes de que sean explotadas por atacantes. Además, es importante destacar que el uso de estas herramientas debe ser ético y legal, y se debe obtener el consentimiento previo de los usuarios de la red antes de monitorear su tráfico.

www.universae.com