UNIDAD 6

Seguridad en sistemas informáticos

Sistemas Informáticos
1º de DAM/DAW Semipresencial
IES San Vicente 2020/2021

Index

Seguridad en un sistema informático

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, por ejemplo).

Los 3 elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos.

- Por hardware entendemos el conjunto de todos los elementos físicos de un sistema informático como CPU, terminales, cableados, medios de almacenamiento secundarios, tarjeta de red, etc.

- Por software entendemos el conjunto de programas lógicos que hacen funcionar el hardware tanto sistemas operativos como aplicaciones.

- Por datos el conjunto de información lógica que maneja el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos.

Debemos ser conscientes de que las medidas de seguridad que deberán establecerse comprenden el hardware el sistema operativo, las comunicaciones, medidas de seguridad física, controles organizativos y legales.

La seguridad absoluta no es posible y en adelante entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a proteger nuestros sistemas informáticos (sobre todo los datos que almacenan).

La seguridad es un problema integral, los problemas de seguridad informática no pueden ser tratados aisladamente ya que la seguridad de todo el sistema es igual a su punto más débil. El uso de sofisticados algoritmos y métodos es inútil si no garantizamos la confidencialidad de las estaciones de trabajo, por otra parte, existe algo que los *hackers* llaman ingeniería asociada que consiste simplemente en conseguir mediante un engaño que los usuarios autorizados revelen sus contraseñas, por lo tanto la educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar.

Objetivos a mantener en un sistema informático

- **Confidencialidad:**

  - Confidencialidad de los datos: Garantiza que los datos privados o confidenciales no se pone a disposición ni se divulgan a personas no autorizadas.

  - Privacidad: Asegura que las personas que controlan o influyen en la información relacionada con ellos puede ser recogida y almacenada y por quién y a quién puede ser revelada dicha información.

- **Integridad**:
    - De los datos: Es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.
    - Del sistema: Es la cualidad que asegura que el sistema realiza la función deseada de forma intacta, que está libre de una manipulación no autorizada del sistema.
- **Disponibilidad:**
    - Se trata de la capacidad de un servicio de unos datos o de un sistema a ser accesible y utilizable por los usuarios o procesos autorizados cuando lo requieran. También se refiere a la capacidad de que la información pueda ser recuperada en el momento que se necesite.

Tipos de amenazas

Las amenazas de un sistema informático pueden provenir desde un programa descargando de forma gratuita que nos ayuda a gestionar nuestras fotos pero que supone una puerta trasera a nuestro sistema, hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad. Se pueden clasificar por tanto en amenazas provocadas por personas, lógicas y físicas.

A continuación se presenta a una relación de los elementos que potencialmente pueden amenazar a nuestro sistema:

Personas

- **Personal**: se pasa por alto el hecho de que una persona de la propia organización, incluso alguien ajeno a la estructura informática, puede comprometer la seguridad de los equipos.
- **Ex-empleados**: generalmente se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema del que conocen perfectamente, pueden insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema como si aún trabajaran en la organización.
- **Curiosos**: son los atacantes juntos con los crakers, que más se dan.
- **Hackers**: una persona que intenta tener acceso no autorizado a los recursos de la red (con intención maliciosa o no).
    - **Crackers**: es un término más preciso para describir una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
- **Intrusos remunerados**: se trata de personas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema que son pagados por una tercera parte generalmente para robar secretos o simplemente para

dañar la imagen de la organización)

Amenazas lógicas

- **Software incorrecto**: a los errores de programación se les llama Bugs y a los programas para aprovechar uno de estos fallos y vulnerar la seguridad se les llama Exploits.

- **Bugs de hardware**: Errores en el diseño de ciertas CPUs o GPUs pueden llevar a la ejecución de instrucciones no permitidas por parte de atacantes. Ejemplos recientes conocidos son Spectre o Meltdown (y sus variantes) que afectan casi en exclusiva a CPUs del fabricante Intel. Estos fallos se pueden "parchear" mediante software (sistema operativo), firmware de la CPU, o hardware (en futuras arquitecturas).

- **Herramientas de seguridad**: cualquier herramienta de seguridad representa un arma de doble filo. De la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o la subred completa, un intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Herramientas como NESUS, SAINT o SATAN pasa de ser útiles a peligrosas cuando la utilizan Crakers.

- **Puertas traseras**: durante el desarrollo de aplicaciones grandes o sistemas operativos es habitual que entre los programadores insertar atajos en los sistemas habituales de autenticación del programa o núcleo de sistema que se está diseñando. Son parte de código de ciertos programas que permanecen sin hacer ninguna función hasta que son activadas para realizar alguna acción no permitida.

- **Canales cubiertos**: son canales de comunicación que permiten a un proceso trasferir información de forma que viole la política de seguridad del sistema.

- **Virus**: un virus es una secuencia de código que se inserta en un fichero ejecutable denominado huésped, de forma que cuando el archivo se ejecuta el virus también lo hace insertándose a sí mismo en otros programas.

- **Gusanos:** es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes en ocasiones portando virus, o aprovechando bugs de los sistemas a los que se conecta para dañarlos.

- **Caballos de Troya**: son instrucciones escondidas en un programa de forma que este parezca realizar las tareas que un usuario espera del pero que realmente ejecuta funciones ocultas. Programas conejo o bacterias (bajo este nombre se conoce a este programa que no hace nada útil si no que simplemente se delimitan a reproducirse hasta que el número de copias acaba con los recursos del sistema produciendo una negación del servicio.

Amenazas Físicas

Robos, sabotajes, destrucción de sistemas. Suministro eléctrico. Condiciones atmosféricas. Catástrofes naturales. Etc.

Protección del sistema

Para proteger nuestros sistemas hemos de realizar una análisis de las amenazas potenciales, las pérdidas que podrían generar, y la probabilidad de que ocurran. A partir de este análisis hemos de diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. A esto se le llama mecanismos de seguridad. Estos mecanismos se pueden clasificar en activos o pasivos.

Protección activa

La protección activa evita daños en los sistemas informáticos mediante empleo de contraseñas adecuadas en el acceso a sistemas y aplicaciones, encriptación de los datos en las comunicaciones, filtrado de conexiones en redes y el uso de software específico en seguridad informática.

Control de acceso

El control de acceso no solo requiere la capacidad de identificación, sino también asociar la apertura o cierre de puertas, permitir o negar acceso, basado en restricciones de tiempo, área o sector dentro de una organización.

El servicio de vigilancia es el encargado del control de acceso, de todas las personas al edificio, este servicio es el encargado de colocar a los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal. A cualquier personal ajeno a la planta se le solicitara completar un formulario de datos personales, los motivos de la visita, hora de ingreso y salida, etc.

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz de ingreso y salida del personal a los distintos sectores de la empresa, en este caso la persona se identifica por algo que posee por ejemplo una llave, una tarjeta de identificación o una tarjeta inteligente, etc. Su mayor desventaja es que estas tarjetas pueden ser robadas, copiadas, etc.

Sistemas biométricos.

Definimos la biometría como la parte de la biología que estudia de forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos. La biometría es una tecnología que realiza mediciones de forma electrónica, y compara características únicas para la identificación de personas.

La forma de identificación consiste en la comparación de características físicas de cada persona, por un patrón conocido y almacenado en una base de datos. Los lectores biométricos que identifican a la persona por lo que es manos, ojos, huellas digitales y voz.

Beneficios de una tecnología biométrica:

- Pueden eliminar la necesidad de poseer una tarjeta para acceder y de

una contraseña difícil de recordar o que finalmente acabe escrita en una papel y visible para cualquier persona.

- Los costes de administración son más pequeños se realizan un mantenimiento del lector y una persona se encarga de mantener una base de datos. Además las características biométricas son intransferibles a otra persona.

Protección electrónica.

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectado los elementos de señalización que son los encargados de hacer saber al personal de una situación de emergencia.

Las barreras infrarrojas y de microondas.

Transmiten y reciben haces de luces infrarrojas y de microondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Estas barreras están compuesta por un emisor y un receptor de igual tamaño y apariencia externa. Cuando el haz es interrumpido se activa el sistema de alarma y luego vuelve al estado de alerta, estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc.

Detector ultrasónico.

Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera cualquier movimiento, que realice un cuerpo dentro del espacio protegido generara una perturbación en dicho campo que accionara la alarma, este sistema posee un circuito refinado que elimina las falsas alarmas, la cobertura puede llegar a un máximo de 40 metros cuadrados.

Circuitos cerrados de televisión (CCTV).

Permite el control de todo lo que sucede en la planta según se capta por la cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista para ser utilizadas como medidas disuasivas u ocultas para evitar que el intruso sepa que está siendo captado.

Protección contra condiciones ambientales.

Normalmente se recibe por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

La frecuencia y severidad de su ocurrencia debe ser tenida en cuenta al decidir la construcción de un edificio. La comprobación de los informes meteorológicos o la existencia de un servicio de una tormenta severa permiten que se tomen precauciones adicionales tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

Protección contra incendios.

Son causados por el uso inadecuado de combustible, fallo en instalación eléctrica o por defecto en la misma, por el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad es considerado el enemigo número uno de las computadoras. Desgraciadamente los sistemas contra fuego dejan mucho que desear causando casi igual daño que el propio fuego. El dióxido de carbono actual alternativa al agua resulta peligroso para los empleados si quedan atrapados.

Protección pasiva

La protección pasiva minimiza el impacto y los efectos causados por accidentes mediante uso de hardware adecuado, protección física, eléctrica y ambiental, realización de copias de seguridad.

Sistemas de alimentación interrumpida.

Trabajar con computadoras indica trabajar con electricidad por lo tanto estas es una de las principales asear a considerar en la seguridad física, además es una problemática que abarca desde un usuario hogareño hasta la gran empresa.

Un SAI es un dispositivo que gracias a sus baterías puede proporcionarte energía eléctrica tras un apagón a todos los dispositivos que tengas conectados durante un tiempo limitado permitiendo poder apagar los equipos no necesarios manteniendo aquellos que se consideren vitales. Los dispositivos hardware no irán enchufados a las tomas de corriente directamente se enchufaran al SAI que estará conectado al enchufe, asiendo de este modo el intermediario entre la red eléctrica y los dispositivos hardware.

Otra de las funciones de los SAI es mejorar la calidad de la energía eléctrica que llega a los aparatos filtrando subidas y bajadas de tensión y eliminando armónicos en caso de usar corriente alterna. Los SAI dan energía eléctrica a equipos llamados cargar criticas como pueden ser aparatos médicos, industriales o informáticos que requieren tener siempre alimentación y que esta sea de calidad

Copias de Seguridad y Restauración.

Las copias de seguridad (backup) son réplicas de datos que nos permiten recuperar la información original en caso de ser necesario es un archivo digital, un conjunto de archivos o la totalidad de los datos considerados lo suficientemente importantes para ser conservados.

Estas copias se pueden almacenar en soportes extraíbles en otros directorios o particiones de datos de nuestra máquina en unidades compartidas de otros discos, discos de red o servidores remotos. La copia de seguridad es útil por varias razones: Para restaurar un ordenador a un estado operacional después de un desastre (copia de seguridad del sistema).

Para restaurar un pequeño número de ficheros después de que hayan sido borrados o dañados accidentalmente (copias de seguridad de datos). En el mundo de la empresa además es útil y obligatorio para evitar ser sancionado por los órganos de control y materias de protección de datos (en España, la Agencia Española de Protección de Datos).

Normalmente las copias de seguridad se suelen hacer en cintas magnéticas si bien dependiendo de lo que se trate podrían usarse CD, DVD, discos ZIP, magnetoópticos, pen drive o pueden realizarse en un centro de respaldo remoto propio o vía internet.

Las copias de seguridad en un sistema informático tienen por objetivo, mantener cierta capacidad de recuperación de la información ante posibles pérdidas, esta capacidad puede llegar a ser muy importante, incluso crítico para las empresas.

RAID

En informática el acrónimo RAID hace referencia a un sistema de almacenamiento que usa múltiples discos duros entre los que distribuye o replica datos dependiendo de su configuración a la que suele llamarse nivel. Los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor rendimiento y mayor capacidad.

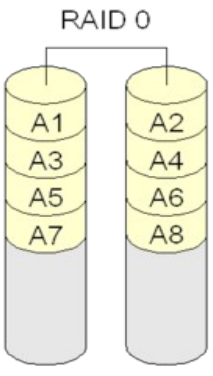
Las configuraciones RAID más usadas comúnmente son:

- RAID 0 (conjunto dividido).
- RAID 1 (conjunto en espejo)
- RAID 5 (conjunto dividido con paridad distribuida)

Sistemas RAID

RAID 0 (DATA STRIPING)

Un RAID 0 también llamado conjunto dividido o volumen dividido, distribuye los datos equitativamente entre dos o más discos.



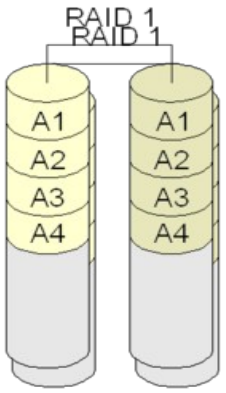
Se usa normalmente para incrementar el rendimiento aunque también puede utilizarse como forma de crear un disco virtual de más capacidad a partir de discos físicos más pequeños.

No tiene tolerancia a fallos. Si un disco falla, se pierden todos los datos.

Un RAID 0 puede ser creado con discos de diferentes tamaños, pero el espacio de almacenamiento añadido al conjunto estará limitado por el tamaño de discos más pequeño, por ejemplo si un disco de 300 Gigas se divide con uno de 100 Gigas el tamaño del conjunto será solo de 200 Gigas ya que cada disco aporta solo 100 gigas.

Se multiplica (velocidad x nº discos) la velocidad teórica de lectura/escritura, ya que los fragmentos de datos se reparten y se escriben de forma simultánea en todos los discos.

RAID 1 (DATA MIRRORING)



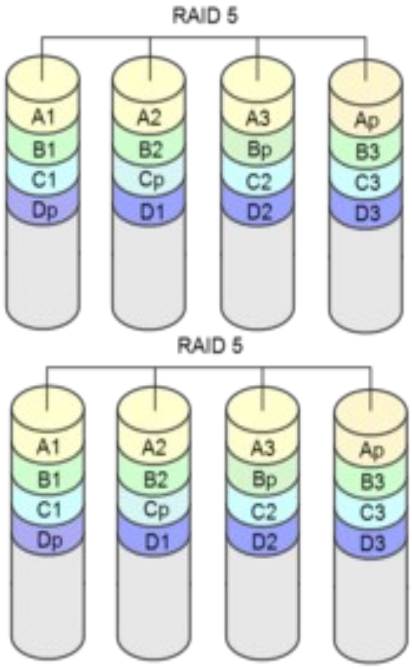
Consiste en utilizar 2 o más discos que contendrán una copia exacta de los mismos datos. A esta configuración también se le llama discos en espejo.

La capacidad total del RAID 1 es la misma que la un solo disco. Un conjunto RAID 1 solo puede ser tan grande como el más pequeño de sus discos.

Es el método más tolerante a fallos (deberían fallar todos los discos a la vez para perder algún dato). El rendimiento de lectura aumenta (leer de varios discos al mismo tiempo), pero no el de escritura (escribe el mismo dato en todos los discos a la vez, y no varios datos simultáneamente como antes).

El RAID 1 tiene muchas ventajas de administración por ejemplo, es posible dividir el espejo, marcar disco duro como inactivo, hacer una copia de seguridad de dicho disco y luego reconstruir el espejo.

RAID 5



Un RAID 5 usa división de datos a nivel de bloques distribuyendo la información de paridad entre todos los discos miembros del conjunto.

Se utiliza un bloque de paridad para el control de errores por cada bloque que se escribe en la misma posición en el resto de discos duros. Es una solución intermedia entre RAID 0 y 1, y solo tiene sentido usarlo a partir de 3 discos duros.

Se pierde la capacidad de 1 disco duro (para almacenar el bloque de paridad), por lo que tendremos una capacidad de n – 1 discos. Puede fallar 1 disco máximo sin perder nada de información.

La velocidad de escritura se ve un poco afectada por el cálculo de la paridad pero sigue siendo mejor que la de un RAID 1. La velocidad de lectura es casi tan rápida como la de un RAID 0.

Un **RAID 6** amplia el nivel del RAID 5 añadiendo otro bloque de paridad, por lo que distribuye dos bloques de paridad entre todos los miembros del conjunto.

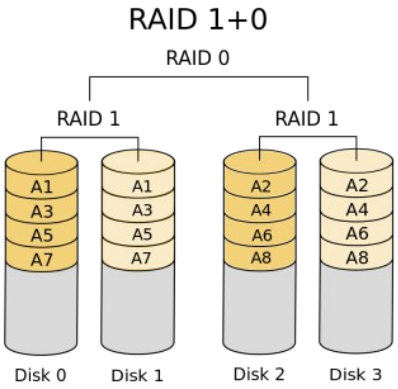
Niveles RAID anidados

Muchas controladoras permiten anidar niveles RAID, es decir que un RAID

pueda usarse como elemento básico de otro en lugar de discos, resulta instructivo pensar en estos conjuntos como capas dispuestas unas sobre otras, con los discos físicos en la inferior, los RAID anidados se indican normalmente, uniendo en un solo número, los correspondientes a los niveles RAID usados, añadiendo un símbolo +, entre ellos, por ejemplo el RAID 10 O RAID 1+0, consiste conceptualmente en múltiples conjuntos de nivel uno, almacenados en discos físicos con un nivel 0 encima, agrupando los anteriores niveles 1.

RAID 10

RAID 10 o 1+0 es una combinación de RAID 0 y RAID 1. Se establecen 2 o más grupos de RAID 1 (en espejo), y dichos grupos se unen a su vez en un RAID 0.



Esto implica tener altas velocidades de lectura y unas velocidades de escritura intermedias entre el RAID 0 y RAID 1. Sobre la tolerancia a fallos, para que se pierda la información, deben fallar al menos todos los discos de un grupo (RAID 1), de esa manera el RAID 0 principal perdería parte de la información repartida. Mientras quede al menos 1 disco por grupo funcionando, el sitema seguirá en pie.

Se pueden hacer grupos de 2 o más discos modo en RAID 1, y juntar 2 o más grupos en un RAID 0, todo depende de si se busca más seguridad (grupos con más discos) o más rendimiento (más cantidad de grupos). La configuración más básica se hace con 4 discos (2 grupos de 2 discos).

SSH

SSH (Secure Shell) es un protocolo para acceder a una máquina remota de forma segura (los datos de la comunicación se cifran). Podemos usar este protocolo como base para que otros, por ejemplo, una sesión gráfica remota con VNC, se comuniquen de forma segura utilizando las medidas de seguridad y el cifrado de que dispone SSH.

Un sistema básico e inseguro de conexión (cifrada) sería algo así:

1. Se establece una conexión cliente/servidor
2. El servidor genera una clave aleatoria simétrica. Se llama simétrica porque se utilizará la misma clave para cifrar y descifrar la información.
3. A partir de ese momento el intercambio de información se cifra con esa clave (incluyendo la contraseña de inicio de sesión por ejemplo).

Problema → El intercambio inicial de la clave no es cifrado, alguien podría capturar el paquete con esa clave.

Cifrado asimétrico

La mejora de seguridad se produce utilizando lo que se llaman claves asimétricas, formadas por una clave llamada pública y otra privada. Estas claves, son suficientemente largas (2048 bits por defecto) para ser adivinadas por fuerza bruta. Se generan mediante una función matemática.

Lo que una clave cifra, sólo la otra lo puede descifrar y viceversa. Los algoritmos de clave asimétrica más usados son RSA (versión 2, la primera tiene fallos) y DSA.

Este sistema puede funcionar aunque una clave (la pública) sea conocida por todos, siempre que la privada sea conocida por solo un equipo en la conexión. De esta manera, la clave simétrica aleatoria para el intercambio de datos se puede enviar cifrada con la clave pública, de forma que solo el equipo que tiene la clave privada puede llegar a conocerla.

Autenticación del servidor

Cuando se instala el servidor SSH por primera vez, se generan pares de claves públicas/privadas dentro de **/etc/ssh** para cada algoritmo (por defecto se usará RSA). Las claves públicas tienen la extensión **.pub**.

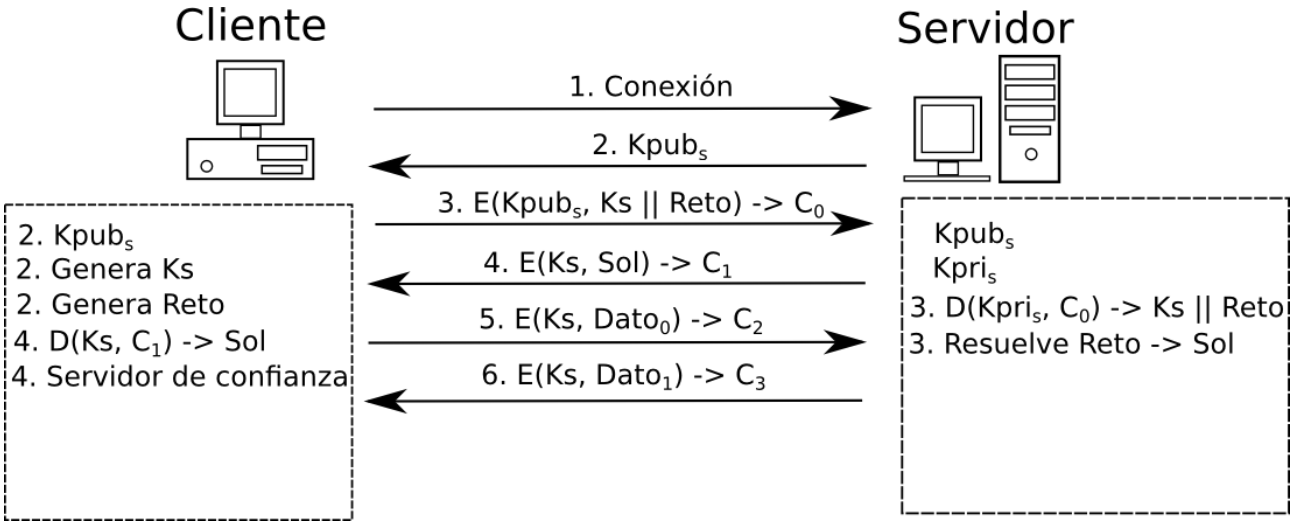
Se genera una huella o fingerprint (con una función MD5 generalmente) de la clave pública que servirá para identificar al servidor. Este resumen debería ser conocido por todo aquel que quiera conectar al servidor. Se puede volver a generar la huella con este comando (la clave rsa sería ssh_host_rsa_key.pub):

ssh-keygen -lf /etc/ssh/ssh_host_ecdsa_key.pub

Cuando alguien se conecta al servidor, este le envía su clave pública. Puedes comprobar que es el servidor correcto porque la máquina cliente genera el resumen y debes confirmar que se trata de la clave pública correcta. En las sucesivas veces ya estará guardado en un archivo **$HOME/.ssh/known_hosts**.

Para comprobar que la clave pública la ha generado el servidor y no ha sido copiada, el cliente podría enviarle una prueba cifrada con la clave pública, junto con una clave simétrica para el posterior envío de información también cifrada con dicha clave. Sólo el servidor original dispone de la clave privada para poder descifrar el mensaje y devolver la prueba resuelta (cifrada con la privada). Esta prueba podría ser simplemente un texto plano que tiene que devolver cifrado con su clave privada.

El cifrado asimétrico se usa únicamente para autenticar a las partes en las conexiones (los certificados digitales y firma electrónica son un buen ejemplo de esto), ya que es muy costoso computacionalmente. Para el envío posterior de datos, se usa un algoritmo de cifrado simétrico.



Kpub$_S$ → Clave pública del servidor
Kpri$_S$ → Clave privada del servidor
Ks → Clave simétrica
E(K,Dato) → Cifrar dato con dicha clave
D(K,Mensaje) → Descifrar mensaje con dicha clave

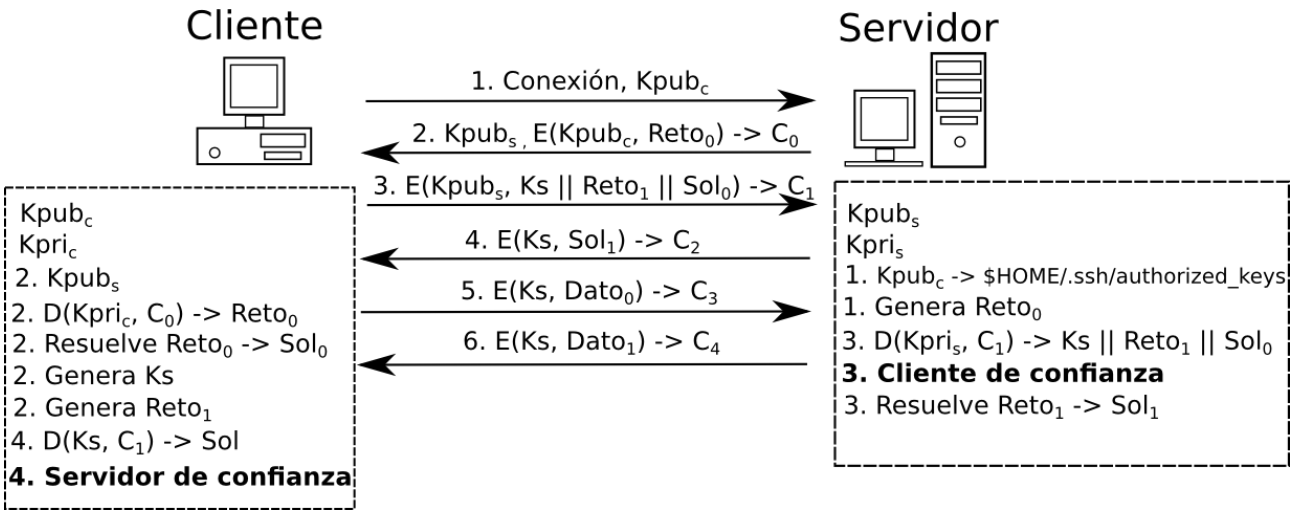
Autenticación del cliente

Por defecto, el servidor SSH sólo requiere la contraseña del usuario con el que se conecta el cliente para iniciar la sesión. Este sistema es relativamente seguro pero mejorable si no quieres depender de una contraseña simplemente.

Para mejorar la seguridad generaremos un par de claves privada/pública en el cliente de tal forma que en el servidor se registre la clave pública y que sea el usuario el encargado de guardar de forma segura la clave privada (que además, por si la pierde, se puede proteger con contraseña).

De esta forma, además, se comprobará la identidad del usuario (el servidor envía una prueba, y sólo quien posea la clave privada puede conocerla y resolverla) siendo innecesaria la contraseña de inicio de sesión.

La clave simétrica se intercambia justo después. El cliente la genera y envía cifrada al servidor (con la pública del servidor). Después de autenticarse, se usa un sistema de clave simétrico.



Instalación de un servidor SSH (Linux)

Instalamos el paquete **openssh-server** (con el comando apt).

Podemos controlar el servicio con el comando systemctl:

sudo systemctl [start|stop|restart|status] ssh

Probar la conexión desde otra máquina al servidor (el usuario debe existir en la máquina donde se ejecuta el servidor:

ssh usuario@ip_servidor (ejemplo → ssh pedro@192.168.2.13)

Al conectarnos por primera vez, nos mostrará la huella de la clave pública del servidor para validarla y confirmar que nos estamos conectando al servidor correcto. Podremos cerrar la sesión remota en cualquier momento ejecutando **exit**.

Ejecución de un comando en la máquina remota (casi igual que lo anterior, pero no mantiene la conexion. Ejecuta el comando y cierra la sesión):

ssh usuario@IP_remota "comando"

Ejemplo → ssh pepe@192.168.2.3 "ls -l"

Copiar archivos entre una máquina remota y el ordenador local (desde sesión local) → Útil para pasar la clave pública al servidor más adelante.

- Del ordenador local al remoto:

  scp ruta_archivo_local usuario@IP_remota:ruta_archivo_remoto
- Del remoto al local →

  scp usuario@IP_remota:ruta_archivo_remoto ruta_archivo_local

Ejemplo: scp img/foto1.jpg pepito2@192.168.1.12:/home/juan/img/foto1.jpg

Autenticar cliente con clave privada

Generamos un par de claves asimétricas en el ordenador cliente.

ssh-keygen -t rsa

Esto genera una clave de 1024 bits (si queremos más seguridad utilizaremos la opción -b seguido del número de bits que deseamos → 2048 o 4096).

Nos preguntará por el nombre del archivo a guardar (la clave privada no tendrá extensión y la pública tendrá la exntesión .pub) y una contraseña para proteger la clave privada (para el caso de que algún posible intruso se pudiera hacer con el archivo).

```
Generating public/private rsa key pair
Enter file in which to save the key (/home/b/.ssh/id_rsa):clave
Enter passphrase (empty for no passphrase): password
Enter same passphrase again: password
Your identification has been saved in /home/guest/clave
Your public key has been saved in /home/guest/clave.pub
```

La clave introducida protegerá nuestro archivo de clave privada. Solo se podrá utilizar conociendo la clave introducida al crearla (más seguridad).

Ahora vamos a guardar la clave pública en el servidor en un archivo llamado **authorized_keys** y está dentro del directorio **.ssh** (dentro de la carpeta home de cada usuario al que nos queramos conectar remotamente con la clave generada):

Copiamos la clave pública al servidor con el comando **scp** (ver arriba). A continuación desde el servidor, con la cuenta de usuario remota, copiamos la clave pública en el archivo de claves autorizadas.

cat clave.pub >> ~/.ssh/authorized_keys (~ es un alias del directorio home del usuario actual).

Por si acaso (el servidor OpenSSH lo suele pedir por seguridad), vamos a dejar que sólo el usuario propietario pueda leer o escribir el archivo.

chmod 600 .ssh/authorized_keys

El archivo con la clave privada (clave) nos lo guardaremos en un lugar seguro donde sólo nosotros tengamos acceso (es nuestra llave).

Importante: Para que este método de seguridad tenga sentido, vamos a deshabilitar la opción de que se pueda conectar alguien utilizando sólo la contraseña del usuario remoto (opción por defecto cuando el cliente no se autentica con clave privada o esta falla). Abrimos en el servidor el archivo **/etc/ssh/sshd_config** y comprobamos que la línea PasswordAuthentication está descomentada (sin '#') y

tenga el siguiente valor:

PasswordAuthentication no

Reiniciamos el servidor SSH para que los cambios tengan efecto

sudo systemctl restart ssh

A partir de ahora sólo podremos acceder a la máquina remotamente utilizando la clave privada.

Como conectarse a un servidor utilizando la clave privada

De la misma forma que lo hacíamos antes, pero teniendo en cuenta alguna cosa más. Lo primero es asegurarnos que los permisos del archivo con la clave privada son lo suficientemente seguros:

chmod 600 clave

A continuación utilizando la opción **-i** en la conexión, e indicándole a continuación cual es el archivo con la clave privada.

ssh -i clave pepe@192.168.2.3

Si todo ha ido de forma correcta, nos pedirá la contraseña que protege la clave privada (password). Si la introducimos correctamente, ya estaremos dentro del otro sistema.

Conectarse con Putty desde Windows (con clave privada)

Descargar los programas Putty y Puttygen:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Utilizar Puttygen primero para convertir la clave privada generada en Linux a un formato soportado por Putty. Después, en la sección Connection → SSH → Auth, seleccionar el archivo de clave privada que se ha creado en formato Putty.

En el campo de servidor (Host name) introduciremos usuario y la IP del servidor (usuario@IP) y nos conectaremos.