



UNIVERSIDAD
DE MÁLAGA

ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

TEMA 3.3

Servidores SSH



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Grado en Ingeniería Informática

Protocolo SSH (Secure SHell)



UNIVERSIDAD
DE MÁLAGA

Es una forma de controlar una máquina remota desde una terminal o computadora local

Trata de sustituir a telnet, que transmite la información entre ambos equipos sin ningún tipo de cifrado

La principal ventaja de SSH es que la información enviada entre cliente-servidor está cifrada.

Tenemos 3 alternativas:

- **Cifrado simétrico**
- **Cifrado asimétrico**
- **Hashing**



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Objetivos de la encriptación o cifrado



UNIVERSIDAD
DE MÁLAGA

- **Confidencialidad**
Solo puede acceder al contenido real su legítimo destinatario y ninguno otro
- **Integridad**
La información no puede ser alternada por un tercero sin ser esto detectado
- **No repudio**
El emisor de la información no puede dejar de reconocer su autoría
- **Autenticación**
Tanto emisor como receptor pueden estar seguros de la identidad del otro



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Cifrado simétrico

Se utiliza la misma clave secreta por tanto por parte del **cliente** como por parte del **servidor** ...

... tanto para **cifrar** como para **descifrar**

La clave nunca se revela a terceros

No se debe transmitir a pelo (solo con otro cifrado)

La clave se genera por un algoritmo de intercambio

VENTAJAS: sencillo y eficiente

Una vez generada... todo el tráfico es encriptado...

...incluidos **el login y password del usuario**



Te amo

ALGORITMO
DE
CIFRADO

&%&2"1

ALGORITMO
DE
DESCIFRADO

Te amo



Cifrado simétrico

Hay varias variantes (algoritmos):

PROCESO DE BLOQUES

La información se divide en bloques de tamaño fijo y a cada uno se le aplica la clave de tamaño fijo

- **DES** = Data Encryption Standard
- **3DES** = Triple Data Encryption Standard
- **AES** = Advanced Encryption Standard
- **CAST** = Carlisle Adams, Stafford Tavares
- **Blowfish**

PROCESO DE FLUJO

La clave se usa para generar un flujo pseudo-aleatorio que se le aplica al flujo de información

- **RC2** = Ron Rivest Cipher, ver 2
- **RC3** = Ron Rivest Cipher, ver 3
- **RC4** = Ron Rivest Cipher, ver 4



Cifrado asimétrico para confidencialidad

Se utilizan dos claves distintas ...

una para **cifrar** y otra para **descifrar**

El emisor cifra el mensaje usando la clave pública del receptor

El receptor descifra el mensaje usando su clave privada

La clave pública del receptor es por todos conocida

La clave privada del receptor solo la conoce el mismo

No es posible calcular una clave a partir de otra



Te amo

ALGORITMO
DE
CIFRADO

&%&2"1

ALGORITMO
DE
DESCIFRADO

Te amo



clave pública
de cifrado
Albert Rivera



clave privada
de cifrado
Albert Rivera



No es posible determinar
una clave a partir de la otra



Cifrado asimétrico para autenticidad



UNIVERSIDAD
DE MÁLAGA

También se puede usar para estar seguros de la autenticidad del emisor ...

**Si el emisor cifra el mensaje con su clave privada ...
... solo descifrando con su clave pública se obtiene el original**

Así se garantiza AUTENTICIDAD y NO REPUDIO
Se una a modo de firma



Ídem

ALGORITMO
DE
VALIDACIÓN

)6@ñv

ALGORITMO
DE
FIRMA

Ídem



clave pública
de firma
Albert Rivera



clave privada
de firma
Albert Rivera



No es posible determinar
una clave a partir de la otra



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA



Cifrado asimétrico

DESVENTAJA: lento, muy ineficiente

Solo se usa para intercambiar la clave simétrica al inicio de la sesión ... luego se usa cifrado simétrico

Alternativas (algoritmos) más usadas:

- **DH** (Diffie – Hellman / logaritmos)
- **RSA** (Rivest – Shamir – Adleman / primos)
- **DSA** (Digital Standard Algorithm)



Hashing

Asegura que un mensaje entre un emisor y un receptor no ha sido modificado por un tercero

La función de hash no tiene inversa $H(x)=h$ $h > x$ (inviabile)
Aunque el mensaje tiene longitud variable,
el resultado de la función de hash tiene longitud fija

Alternativas (algoritmos) más usadas:

- MD5 (Message Digest, v5)
- SHA-1 (Secure Hash Algorithm, v1)
- SHA-2 (Secure Hash Algorithm, v2)

El receptor comparará el HASH original con el que se produce al recibir y descifrar la información:

- Si son iguales el mensaje no ha sido alterado
- Si son distintos el mensaje ha sido modificado



Pasos en la apertura de sesión SSH



UNIVERSIDAD
DE MÁLAGA

- 1) El cliente SSH abre conexión con el servidor SSH
- 2) **Cliente y servidor negocian la versión del protocolo**
- 3) El servidor envía al cliente su clave pública RSA
- 4) **El cliente mira que la clave coincida con la almacenada**
- 5) Si no tenemos la clave pública del servidor, se pide confirmación al usuario (riesgo) y se almacena clave
- 6) **El cliente decide un algoritmo de cifrado simétrico y genera aleatoriamente una clave para dicho algoritmo**
- 7) El cliente cifra la clave anterior usando RSA y la clave pública del servidor. Envía el mensaje al servidor
- 8) **El servidor descifra el mensaje anterior con su clave RSA privada y ...**

a partir de entonces toda comunicación es encriptada usando la clave compartida



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Pasos en la autenticación del cliente



UNIVERSIDAD
DE MÁLAGA

... lo siguiente es ver si el cliente tiene acceso permitido

NOTA: todo lo siguiente está además codificado con un mecanismo de clave simétrica

Método Básico:

El cliente manda login + password y el servidor comprobará sus credenciales como si fuera usuari local

Método con clave pública :

- 1) El servidor genera un número aleatorio (desafío) y cifra el número con la clave pública RSA/DSA del cliente
(el servidor debe tener previamente dicha clave pública)
- 2) El servidor envía el desafío cifrado al cliente y este lo descifra usando su clave privada.
- 3) El cliente envía el desafío descifrado al servidor que comprueba que sea el generado inicialmente



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Instalación de OpenSSH Server



UNIVERSIDAD
DE MÁLAGA

Primero obtenemos los permisos de root:

```
# sudo -i
```

Actualizamos la base de datos de paquetes

```
# apt-get update
```

Y finalmente instalamos el OpenSSH server

```
# apt-get install openssh-server
```

Comprobamos el estado del demonio SSH:

```
# service ssh status
```

● ssh.service - OpenBSD Secure Shell server

Loaded: loaded (/lib/systemd/system/ssh.service;
enabled; vendor preset: enabled)

Active: **active (running)** since Sun 2018-12-16
13:19:23 UTC; 1h 21min ago

Conectando con OpenSSH Server



UNIVERSIDAD
DE MÁLAGA

Tenemos que abrir el puerto 22 en el ufw:

```
# ufw app info
```

```
OpenSSH 22/tcp
```

```
# ufw allow in OpenSSH
```

```
# ufw status
```

```
Status: active
```

```
OpenSSH                ALLOW          Anywhere
```

Para conectarnos a la máquina remota desde una local:

```
# ssh <usuario remoto>@<nombre o IP>
```

```
# ssh pyromikel@172.16.195.137
```

```
pyromikel@172.16.195.137's password: *****
```

```
pyromikel@ubuntu:~#
```

Para salir **quit** o bien **Ctrl+D**



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Conectando con OpenSSH Server

Opciones adicionales del cliente ssh:



UNIVERSIDAD
DE MÁLAGA

```
# ssh -[1|2] -l <usuario remoto> <nombre o IP>
```

```
# ssh -p <puerto> -C -c <tipoCifrado> <user>@<host>
```

-1 Fuerza a usar SSH1

-2 Fuerza a usar SSH2

(si no se pone nada se negocia con el servidor)

-l nos permite especificar el usuario remoto

-p puerto de escucha del servidor (22 por defecto)

-C ... las comunicaciones son comprimidas (gzip)

-c <tipoCifrado> ... para configurar el cifrado

En SSH1: des | 3des | blowfish (seleccionar uno)

En SSH2: se pone un listado de preferidos

(separados por ,) 3des,aes128,aes192,aes256

arcfour, blowfish, cast128,chacha20



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Cambiando el puerto de SSH / capar root



UNIVERSIDAD
DE MÁLAGA

Tenemos que editar el fichero de configuración:

vi /etc/ssh/sshd_config

Buscamos la línea ... **#Port 22**

... y ponemos otro puerto (quitando #): **Port 9568**

Otra medida es capar el acceso remoto de root

Buscamos la línea ... **#PermitRootLogin ...**

... y ponemos (quitando #): **PermitRootLogin no**

También tenemos que cambiar el puerto en el ufw

- Primero modificamos el perfil OpenSSH

vi /etc/ufw/applications.d/openssh-server

... y cambiamos **ports=22/tcp** por **ports=9568/tcp**



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Cambiando el puerto de SSH (cont)

Actualizamos el perfil de ufw:

```
# ufw app update OpenSSH
```

Comprobamos que se ha hecho el cambio:

```
# ufw app info OpenSSH
```

Y que las reglas están activas:

```
# ufw app status
```

Finalmente reiniciamos los demonios ufw y ssh

```
#service ufw restart
```

```
#service ssh restart
```

Para volver a entrar:

```
#ssh -p 9568 pyromikel@servidor
```



Otras opciones de sshd_config



UNIVERSIDAD
DE MÁLAGA

HostKey /etc/ssh/ssh_host_rsa_key

HostKey /etc/ssh/ssh_host_dsa_key

Ficheros con las claves privadas del servidor (RSA, DSA...)

PubKeyAuthentication no|yes

Permite autenticación con clave pública de cada usuario

PasswordAuthentication no|yes

Permite autenticación básica con login y password

AuthorizedKeyFiles %h/.ssh/authorized_keys

Para cada usuario hay que indicar la localización de un fichero que contendrá las claves públicas de dicho usuario



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA



Otras opciones de sshd_config (cont)

PermitRootLogin prohibit-password

Solo permite conectarse a root con autenticación RSA/DSA

AllowUsers pyromikel juan@150.214.57.12

Especificamos qué usuarios pueden conectarse y desde qué máquinas pueden hacerlo (separados por espacios)

DenyUsers pcasado@pp.es piglesias@podemos.es

Especificamos qué usuarios NO pueden conectarse

AllowUsers informatica teleco industriales

Todos los usuarios de estos grupos pueden conectarse

DenyGroups peperos sociatas podemitas naranjas

Los usuarios de estos grupos tienen el acceso prohibido

DenyUsers pcasado@pp.es piglesias@podemos.es

Especificamos qué usuarios NO pueden conectarse



Otras opciones de sshd_config (cont)

X11Forwarding no|yes

Para permitir que aplicaciones gráficas se ejecuten en el servidor y se visualicen en el cliente remoto

LoginGraceTime 60s | 1m

Tiempo en el que se permite introducir la password

MaxConnections 100

Número máximo de clientes que pueden conectarse

MaxAuthTries 5

Número de veces en el que puedo fallar al meter password

MaxSessions 3

Máximo número de sesiones desde una misma terminal

MaxStartups valor | mín:tasa:máx

Máximo núm de clientes sin autenticar (op1) rechazar a partir de valor (op2) a partir de min y hasta max rechazaremos una petición con una probabilidad tasa% (a partir de máx se rechazan todas)

Opciones de ssh_config

Host <nombre máquina>|<dirección IP>| * (todos)

Funciona a modo de separador de sección y su valor indica a qué máquinas remotas se aplican los siguientes parámetros

Port XXXX (por defecto 22)

Indica el puerto por el que escucha el servidor anterior

PasswordAuthentication no|yes

Permite autenticación básica con login y password

PubKeyAuthentication no|yes (se recomienda yes)

Permite autenticación clave pública

IdentityFile ~/.ssh/id_rsa

Archivo que contiene la clave pública del usuario

StrictHostKeyChecking no|yes

Indica qué hacer cuando nos intentamos conectarnos a una máquina de la que no tenemos la clave pública. **NO: nos pregunta**

YES: no lo permite



Copiado remoto con scp (secure copy)



UNIVERSIDAD
DE MÁLAGA

“scp” permite copiar ficheros de forma segura entre dos máquinas: local a remota/remota a local/remota a remota

```
#scp -p user@host:/usr/fich.c /home/michel
```

Copia /usr//fich.c del servidor a /home/michel de la computadora local/ **-p** conserva las propiedades originales

```
#scp -P 9568 -p user@host:/usr/fich.c /bin
```

Si queremos especificar un puerto de la máquina remota distinto de 22, usaremos la opción **-P**

```
#scp user1@host1:/path1/file1 user2@host2:/path2
```

Copia de una máquina remota a otra

```
#scp -R /local_folder user@host:/path
```

Con **-R** copia de forma recursiva una carpeta a otra



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Secure File Transfer Protocol (SFTP)



UNIVERSIDAD
DE MÁLAGA

“sftp” es la versión segura del clásico ftp

Extensión del protocolo SSH que proporciona funcionalidades de transferencia y administración de ficheros

- Capacidad de reanudar transferencias interrumpidas
- Listado, copiado y borrado de ficheros y carpetas
- Independiente del sistema operativo
-
-

Para abrir una consola sftp:

#sftp -P <port> <usuario>@<nombre o IP remoto>



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Secure File Transfer Protocol (SFTP)



UNIVERSIDAD
DE MÁLAGA

Comandos básicos:

- **ls** : lista el contenido del directorio de trabajo remoto
- **lls**: lista el contenido del directorio de trabajo local
- **pwd**: imprime el nombre del directorio de trabajo remoto
- **lpwd**: imprime el nombre del directorio de trabajo local
- **cd**: cambia el directorio de trabajo remoto
- **lcd**: cambia el directorio de trabajo local
- **mkdir / lmkdir** : para crear directorios remoto/local
- **rmdir / lrmkdir**: para borrar un directorios remoto/local
- **get**: copia un fichero del directorio remoto al local
- **put**: copia un fichero del directorio local al remoto
- **mget**: copia varios ficheros del directorio remoto al local
- **mput**: copia varios ficheros del directorio local al remoto



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Ficheros de clave a tener en cuenta



UNIVERSIDAD
DE MÁLAGA

En la máquina que se conecta como cliente:

`/etc/ssh/ssh_known_hosts2`

Claves públicas de los host conocidos por el cliente
(todos los hosts a los que me puedo conectar)

Cada usuario tiene en la máquina local:

`$HOME/.ssh/id_rsa`

Clave privada del usuario, visible solo por cada usuario

`$HOME/.ssh/id_rsa.pub`

Clave pública del usuario, visible por todo el mundo



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA



Ficheros de clave a tener en cuenta

En la máquina que actúa como servidor SSH:

/etc/ssh/ssh_host_rsa_key

Clave privada RSA del servidor – solo visible por root

Este fichero se crea automáticamente al instalar OpenSSH

/etc/ssh/ssh_host_rsa_key.pub

Clave pública RSA del servidor, visible por todos los usuarios

Este fichero se crea automáticamente al instalar OpenSSH

Para cada usuario:

\$HOME/.ssh/authorized_keys

Claves públicas que puede usar el usuario para

Autenticarse como cliente en esta máquina remota



Ficheros de clave a tener en cuenta

En la máquina que se conecta como cliente:



UNIVERSIDAD
DE MÁLAGA

/etc/ssh/ssh_known_hosts2

Claves públicas de los host conocidos por el cliente
(*todos los hosts a los que me puedo conectar*)

O lo agrega el cliente a mano... o se agrega al conectar la primera vez a cierta máquina remot

Cada usuario tiene en la máquina local:

\$HOME/.ssh/id_rsa

Clave privada del usuario, visible solo por cada usuario

\$HOME/.ssh/id_rsa.pub

Clave pública del usuario, visible por todo el mundo

**Estos 2 ficheros los debe generar
cada usuario que quiere conectar
con una máquina remota**



LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA



Generación de claves pública+privada

Cada usuario que quiera conectarse de forma remota con un servidor SSH por RSA:

```
# ssh-keygen -t rsa1|rsa|dsa|ecdsa -b 1024|2048
```

Así generamos un par de claves, pública y privada para conectarnos como cliente (por defecto RSA de 2048 bits)

Generating public/private rsa key pair.

*Enter file in which to save the key: ~/.ssh/id_rsa (privada
... y la pública ~/.ssh/id_rsa.pub*

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Private key saved in /home/pyromikel/.ssh/id_rsa.

Public key saved in /home/pyromikel/.ssh/id_rsa.pub.

The key fingerprint is:

SHA256:U2lXjNIQqltyEal1v3gvyDjyl5uK2SnmU1...



Proteger clave privada



UNIVERSIDAD
DE MÁLAGA

Es recomendable proteger la clave privada mediante una palabra de paso (clave) ...

Si no lo hicimos al generarla... podemos hacerlo después:

```
# ssh-keygen -p -f ~/.ssh/id_rsa
```

Nos pide una clave que tendremos que usar siempre que queramos utilizar la clave privada



Gracias por su atención