Introducción (I)

- Secure SHell:
  - Permite crear conexiones seguras (cifradas) entre dos ordenadores, permitiendo reemplazar:
    - rlogin.
    - telnet.
    - rcp.
    - ftp.
    - ...

Introducción (II)

- SSH proporciona:
  - Verificación de la identidad del servidor a partir de la primera conexión.
  - Transmisión de toda la información cifrada con encriptación fuerte.
    - Dificultad para descifrar la misma por los no autorizados.
  - Posibilidad de reenviar aplicaciones inseguras, como X11, POP3, etc., mediante el reenvío de puerto.
- Versiones de SSH:
  - Versión 1:
    - Algoritmos de encriptación patentados.
    - Agujero de seguridad que podría permitir insertar datos falsos.
  - Versión 2.

Establecimiento de una conexión (I)

- Una conexión SSH se establece en tres pasos:
  - Creación de una capa de transporte segura (TLS).
  - Autenticación del cliente contra el servidor.
  - Uso de la conexión establecida por los servicios del cliente.

Establecimiento de una conexión (II)

- Creación de una capa de transporte segura:
  - Verifica la identidad del servidor.
  - Cifra y descifra la información.
  - Asegura la integridad de la información.
  - Permite opcionalmente comprimir la información.
- Se produce una negociación con los pasos:
  - Intercambio inicial de claves.
  - Selección del algoritmo de clave pública.
  - Selección del algoritmo de clave privada.
  - Selección del algoritmo de autenticación de mensajes.
  - Selección del algoritmo de hash utilizado.

Establecimiento de una conexión (III)

- En la creación de la capa de transporte segura:
  - El cliente puede verificar (a partir de la primera vez) la identidad del servidor.
  - Se crean dos valores:
    - Un valor de hash para intercambio.
    - Un valor de secreto compartido.
  - Estos valores permiten enviar la información de forma segura.
  - Cada cierta cantidad de datos se cambian los dos valores.

Establecimiento de una conexión (IV)

- Autenticación del cliente contra el servidor:
  - Inicialmente el servidor informa al cliente de los métodos disponibles.
  - El cliente selecciona uno de ellos y se autentica ante el servidor.
    - Usuario/contraseña.
    - Intercambio de claves pública/privada.
    - ...
  - Métodos a priori inseguros pueden usarse al ir cifrados por TLS.

Establecimiento de una conexión (V)

- Uso de la conexión establecida:
  - La conexión entre cliente y servidor se multiplexa en canales para:
    - Enviar múltiples sesiones entre terminales diferentes.
    - Reenviar conexiones X11.
    - ...
  - Cada canal:
    - Posee su propio control de flujo.
    - Permite un tamaño de paquete diferente.
    - Permite enviar diferente tipo de datos.

Configuración del servidor (I)

- El servidor de SSH:
  - Es el programa /usr/sbin/sshd.
  - Su fichero de configuración por defecto es /etc/ssh/sshd_config.
    - Puede modificarse utilizando la opción -f en el arranque.
  - Si no existe el fichero de configuración el servidor:
    - Muestra un mensaje de error.
    - Finaliza su ejecución (no arranca).

Configuración del servidor (II)

- Las opciones de configuración del servidor se dividen en:
  - Opciones generales.
  - Opciones de configuración de acceso.
  - Opciones de usuarios y grupos.
  - Opciones de reenvío de conexiones X11.
  - Otras opciones de configuración.
- Existen opciones solo validas para la versión 2 del protocolo.

Opciones generales

Opción	Descripción	Valor por defecto
AcceptEnv*	Indica las variables de ambiente enviadas por el cliente que serán aceptadas por el servidor.	Ninguna variable es aceptada.
AddressFamily	Especifica la familia de direcciones IP aceptadas por el servidor, los valores pueden ser *any*, *inet* ó *inet6*.	any
AllowTcpForwarding	Autoriza el reenvío de puertos.	Yes
GatewayPorts	Especifica si ordenadores remotos están autorizados a utilizar puertos reenviados a otros clientes. Los valores posibles son *no*, *yes* y *clientspecified*.	No
ListenAddress	Dirección IP local que escucha las conexiones entrantes. Pueden especificarse varias entradas para indicar varias direcciones de red.	Todas las direcciones.
Port	Puerto en que permanece a la escucha el servidor en espera de conexiones. Pueden especificarse varias entradas para especificar varios puertos distintos.	22 TCP.
Protocol	Versión de los protocolos SSH soportados por el servidor y orden de preferencia.	Versión 2.
TCPKeepAlive	Indica si deben enviarse paquetes para comprobar si la conexión con el cliente se encuentra activa.	Yes
UseDNS	Indica si se debe realizar una comprobación inversa de la identidad del cliente.	Yes
UsePrivilegeSeparation	Indica si SSH creará un proceso hijo sin privilegios una vez el usuario ha accedido al sistema.	Yes

Opciones de configuración de acceso (I)

Opción	Descripción	Valor por defecto
AuthorizedKeysFile	Fichero con las claves públicas usadas para autenticación.	~/.ssh/authorized_keys.
ChallengeResponseAuthentication	Indica si el intercambio de respuestas de autenticación es permitido.	Yes
Ciphers*	Indica los cifrados permitidos por el protocolo.	Todos.
GSSAPIAuthentication*	Especifica si la autenticación basada en GSSAPI es permitida.	No
GSSAPICleanupCredentials*	Especifica si las credenciales son automáticamente destruidas cuando termina la sesión.	Yes
HostbasedAuthentication*	Autoriza el acceso mediante clave pública de usuarios de los ordenadores indicados en *rhosts* o en */etc/hosts.equiv*.	No
HostKey	Especifica el fichero que contiene la clave privada del servidor. Sus valores por defecto son */etc/ssh/ssh_host_key* para la version 1 y */etc/ssh/ssh_host_rsa_key* y */etc/ssh/ssh_host_dsa_key* para la versión 2.	Ver descripción.
IgnoreRhosts	Deniega el uso de los ficheros *.rhosts* y *.shosts* en el acceso remoto.	Yes
IgnoreUserKnowHosts	Deniega el uso del fichero *~/.ssh/know_hosts* para encontrar los ordenadores conocidos.	No
LoginGraceTime	Tiempo, en segundos, antes de que se cierre la sesión de autenticación.	120 segundos.
LogLevel	Información que se escribirá en los accesos. Sus valores posibles son, de menor a mayor información QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2 y DEBUG3.	INFO

Opciones de configuración de acceso (II)

Opción	Descripción	Valor por defecto
MaxAuthTries	Número máximo de intentos de autenticación por conexión.	6
MaxStartups	Número máximo de conexiones simultaneas en estado de autenticación.	10
PasswordAuthentication	Permite la autenticación mediante contraseña.	Yes
PermitEmptyPasswords	Permite el acceso a usuarios sin contraseña.	No
PermitRootLogin	Permite el acceso de root mediante SSH.	Yes
PermitUserEnvironment	Especifica si las variables de ambiente del usuario serán procesadas por SSH.	No
PubkeyAuthentication*	Permite la autenticación mediante clave pública.	Yes
RhostsRSAAuthentication	Indica si se permite el uso de *rhost* o */etc/hosts.equiv* en la autenticación mediante RSA. Solo aplicable a la versión 1 del protocolo.	No
RSAAuthentication	Permite la autenticación mediante RSA. Solo aplicable a la versión 1 del protocolo.	Yes
UseLogin	Indica si se utiliza login para comprobar el acceso de los usuarios.	No
UsePAM	Indica si se utiliza PAM para comprobar el acceso de los usuarios.	No

Opciones de usuarios y grupos

Opción	Descripción	Valor por defecto
AllowGroups	Lista de nombres de grupos, separados por espacios, cuyos miembros, sea como grupo primario o grupo suplementario, tienen permitido el acceso al sistema mediante SSH. Pueden utilizarse los caracteres comodín * e ?.	Todos los grupos.
AllowUsers	Lista de nombres de usuarios, separados por espacios, cuyo acceso al sistema esta permitido por SSH. Puede tomar la forma usuario@ordenador, comprobando entonces tanto el nombre del usuario como el nombre del ordenador desde el que intenta el acceso. Pueden utilizarse los caracteres comodín * e ?.	Todos los usuarios.
DenyGroups	Lista de nombres de grupos, separados por espacios, cuyos miembros, sea como grupo primario o grupo suplementario, no tienen permitido el acceso al sistema mediante SSH. Pueden utilizarse los caracteres comodín * e ?.	Ningún grupo.
DenyUsers	Lista de nombres de usuarios, separados por espacios, cuyo acceso al sistema no esta permitido por SSH. Puede tomar la forma usuario@ordenador, comprobando entonces tanto el nombre del usuario como el nombre del ordenador desde el que intenta el acceso. Pueden utilizarse los caracteres comodín * e ?.	Ningún usuario.

Opciones de reenvío de conexiones X11

Opción	Descripción	Valor por defecto
X11DisplayOffset	Indica el primer identificador de pantalla que utilizará SSH en sus conexiones X11 para no interferir con los identificadores locales X11.	10
X11Forwarding	Permite el reenvío de conexiones X11.	No
X11UseLocalhost	Indica si SSH escucha las conexiones X11 en el interfaz de loopback o en los otros interfaz de red existentes.	Yes
XAuthLocation	Indica la localización del programa de autorización de acceso mediante X11.	/usr/bin/xauth

Otras opciones de configuración

Opción	Descripción	Valor por defecto
Banner*	Muestra un mensaje antes de acceder al servidor de SSH.	Sin ningún mensaje.
ClientAliveCountMax*	Número de paquetes de comprobación sin responder que se espera antes de cerrar la conexión por no obtener respuesta del cliente.	3
ClientAliveInterval*	Intervalo de inactividad, en segundos, que el servidor espera antes de enviar un mensaje al cliente solicitando una respuesta.	No activado (valor 0).
Compression	Especifica si la compresión es permitida o retrasada hasta que el usuario se ha autenticado correctamente. Sus valores son yes, no o delayed.	Delayed.
ForceCommand	Fuerza la ejecución del comando especificado.	Ninguno.
PrintLastLog	Especifica si al acceder mediante SSH se mostrará la información del último acceso sucedido.	Yes
PrintMotd	Especifica si SSH mostrará el mensaje del día indicado en */etc/motd*.	Yes
StrictModes	Especifica si SSH debe chequear el modo y propietario de los ficheros en el directorio raíz del usuario antes de permitir su acceso.	Yes
Subsystem*	Configura un subsistema externo, por ejemplo el *sftp-server*.	Ninguno.

Otros ficheros del servidor

- Existen en /etc/ssh otros ficheros usados por el servidor:
  - moduli (grupo Diffie-Hellman para intercambio de claves).
  - ssh_host_key (Clave privada RSA para SSHv1).
  - ssh_host_key.pub (Clave pública RSA para SSHv1).
  - ssh_host_dsa_key (Clave privada DSA para SSHv2).
  - ssh_host_dsa_key.pub (Clave pública DSA para SSHv2).
  - ssh_host_rsa_key (Clave privada RSA para SSHv2).
  - ssh_host_rsa_key.pub (Clave pública RSA para SSHv2).

Creación de claves para acceso remoto (I)

- El servidor puede permitir la autenticación mediante el uso de un par de claves pública/privada.
- Las claves se crean mediante:

```
ssh-keygen -t <tipo>
```

- Donde <tipo>
  - rsa1 para RSA y SSHv1.
  - dsa para DSA y SSHv2.
  - rsa para RSA y SSHv2.

Creación de claves para acceso remoto (II)

- Los ficheros se crean con los nombres:

Fichero	Descripción
~/.ssh/identity	Contiene la clave privada RSA para la versión 1 del protocolo SSH.
~/.ssh/identity.pub	Contiene la clave pública RSA para la versión 1 del protocolo SSH.
~/.ssh/id_dsa	Contiene la clave privada DSA para la versión 2 del protocolo SSH.
~/.ssh/id_dsa.pub	Contiene la clave pública DSA para la versión 2 del protocolo SSH.
~/.ssh/id_rsa	Contiene la clave privada RSA para la versión 2 del protocolo SSH.
~/.ssh/id_rsa.pub	Contiene la clave pública RSA para la versión 2 del protocolo SSH.

- La clave pública que deseamos utilizar debe añadirse en el fichero ~/.ssh/authorized_keys del usuario en el servidor remoto.

Configuración del cliente (I)

- El cliente de SSH:
  - Es el programa /usr/bin/ssh.
  - Su fichero de configuración por defecto es /etc/ssh/ssh_config.
  - Puede modificarse si el usuario posee un fichero ~/.ssh/config.
  - Los ordenadores cuya identidad conoce el cliente para el usuario (y puede verificar) se encuentran en
  - ~/.ssh/known_hosts.

Configuración del cliente (II)

Opción	Descripción	Valor por defecto
Host	Restringe las declaraciones que se hagan a continuación a los ordenadores identificados hasta la siguiente aparición de Host. Pueden usarse los caracteres comodín * e ?.	Ninguno.
AddressFamily	Especifica la familia de direcciones IP aceptadas por el servidor, los valores pueden ser *any*, *inet* ó *inet6*.	any
BindAddress	Dirección IP a enviar en ordenadores con múltiples interfaces de red.	Ninguno.
CheckHostIP	Chequea el nombre del ordenador en la lista de ordenadores conocidos.	Yes
EscapeChar	Asigna el carácter de escape de la conexión	~
ForwardAgent	Permite o no el redireccionamiento de la autenticación a un ordenador remoto.	No
ForwardX11	Permite el redireccionamiento de la conexión X11 por la conexión SSH.	No
GatewayPorts	Permite la conexión de ordenadores remotos a los puertos reasignados a una conexión segura.	No.
LocalForward	Especifica el puerto local que puede ser redireccionado a una conexión segura de otro ordenador y puerto.	Ninguno.
LogLevel	Información que se escribirá en los accesos. Sus valores posibles son, de menor a mayor información QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2 y DEBUG3.	INFO
NumberOfPasswordPrompts	Número de veces que se solicita la contraseña antes de cerrar la comunicación.	3
Protocol	Versión de los protocolos SSH soportados por el servidor que será aceptada y orden de preferencia.	Versión 2.
RemoteForward	Especifica que el ordenador y puerto remoto serán redireccionados a una conexión segura en un puerto del ordenador.	Ninguno.

Uso del cliente

- Uso:

```
ssh {[-l usuario] ,[usuario@]}<servidor> [comando]
```

- Donde:
  - <servidor> es el servidor donde conectarnos.
  - usuario es el usuario como el que queremos conectarnos.
    - El mismo del ordenador si no se especifica.
  - comando es el comando a ejecutar.
    - Se obtiene una shell si no se especifica.

Transferencia de archivos

- Dos posibilidades:
  - scp (sustituye a rcp).
  - sftp (sustituye a ftp).
- Uso de scp:

```
scp fichero_local usuario@ordenador_destino:/fichero_remoto
scp usuario@ordenador_origen:/fichero_remoto fichero_local
scp /descargar/* usuario@robotica.uv.es:/descargados/
```

- Uso de sftp:

```
sftp usuario@ordenador
```

Reenvío de X11

- El reenvío de X11:
  - Requiere un ancho de banda elevado.
  - Necesita que cliente y servidor tengan habilitada la opción.
  - Requiere que el cliente tenga un servidor X para poder ejecutar las ordenes que se transfieran desde el servidor.
- El reenvío es tan sencillo como ejecutar el comando en la shell remota:

```
xclock &
```

- Para no tener que modificar ficheros de configuración del servidor X debe ejecutarse como:

```
ssh -Y root@robotica.uv.es
```

Reenvío de un puerto (I)

- El comando de reenvío de un puerto es:

```
ssh -f -N -L puerto_local:ordenador_remoto:puerto_remoto
   usuario@ordenador_servidor
```

- Donde:
  - puerto_local es el puerto de nuestro ordenador que deseamos reenviar a través de SSH.
  - ordenador_remoto:puerto_remoto son el ordenador y puerto al que deseamos conectarnos mediante el reenvío de SSH.
  - usuario@ordenador_servidor es el ordenador a través del cual realizamos el reenvío del puerto.

Reenvío de un puerto (II)

- Ejemplos:

```
ssh -f -N -L 1100:robotica.uv.es:110 robotica.uv.es
ssh -f -N -L 1100:robotica.uv.es:110 amparo.uv.es
```

- El reenvío de puertos:
  - Es útil pues permite asegurar servicios entre clientes y servidores, utilizando incluso otros servidores.
  - Puede ser un problema de seguridad por:
    - Los cortafuegos suelen permitir conexiones por el puerto 22 (SSH).
    - Si un cliente que utiliza el reenvío de puertos se ve comprometido, los servicios reenviados estarán comprometidos en el servidor.