Introducción (I)

- Actualmente el control de acceso se realiza mediante:
  - Envolventes de acceso (tcpwrappers).
  - Servidor xinetd.
- Ambos son versiones mejoradas de:
  - Antiguos envolventes de acceso.
  - Servidor inetd.

El servidor inetd (I)

- Surgió en la versión de UNIX 4.3 de BSD.
  - Anteriormente cada servicio escuchaba su propio puerto.
  - A partir de esta versión, existe un servidor que escucha los puertos y lanza los servidores adecuados.
- El fichero de configuración del servidor es /etc/inetd.conf.
- Es leído:
  - Al arrancar el servidor.
  - Al recibir el servidor la señal de SIGHUP.

El servidor inetd (II)

- Cuando recibe una petición genera un nuevo proceso.
  - Si la petición es a un puerto TCP:
    - Este proceso lanza el servidor que atiende el puerto.
    - Le comunica la dirección IP/puerto del cliente.
  - Si la petición es a un puerto UDP:
    - Se libera el socket original para permitir a inetd seguir escuchando el puerto.
    - inetd permanece a la espera de que termine la solicitud.

El servidor inetd (III)

- Ejemplo:

```
ftp       stream   tcp   nowait   root   /usr/etc/ftpd      ftpd –l
telnet    stream   tcp   nowait   root   /usr/etc/telnetd   telnetd
daytime   dgram    udp   wait     root   internal
```

- Descripción de los campos:
  - Nombre del servicio.
  - Tipo de socket.
  - Protocolo de transporte.
  - Esperar (wait) o no (nowait) a que el servidor termine su ejecución.
  - Usuario como el que ejecutar el servidor.
  - Servidor a ejecutar (internal -> servicio soportado por inetd).
  - Argumentos del servidor.

Los envolventes de acceso (I)

- Permiten controlar y limitar los servicios ofrecidos.
- Sus ventajas son:
  - Un único programa que controla el acceso.
  - Condiciones de acceso especificada en pocos ficheros.
  - Información de acceso almacenada en unos pocos ficheros de log.
- El más conocido es TCPWrapper.

Los envolventes de acceso (II)

- TCPWrapper permite:
  - Mostrar mensajes de acceso.
  - Realizar una búsqueda inversa doble de la IP del cliente.
  - Registrar información de los accesos permitidos y denegados.
  - Controlar el acceso en función del cliente:
    - Transferir el control al servidor en caso de ser aceptado.
    - Denegar el acceso.
    - Permitir el acceso a un falso servidor.

Los envolventes de acceso (III)

- Su introducción en el servidor de inetd es:
  - Sustituir el nombre del servidor por el del envolvente. Ejemplo:

```
telnet    stream   tcp   nowait   root   /usr/etc/tcpd   telnetd
```

  - Donde /usr/etc/tcpd es el envolvente de acceso.
- Las reglas de acceso se especifican en dos ficheros:
  - /etc/hosts.allow: Servicios permitidos y ordenadores a los que se les permite.
  - /etc/hosts.deny: Servicios denegados y ordenadores a los que se les deniega.

Los envolventes de acceso (IV)

- Los ficheros de examinan en el orden:
  - /etc/hosts.allow.
    - Si se encuentra un servicio para un ordenador este se permite.
  - /etc/hosts.deny.
    - Si se encuentra un servicio para un ordenador este se deniega
  - Si un servicio/ordenador no se encuentra en ninguno de los ficheros se permite por defecto.

El servidor xinetd (I)

- Se encuentra en /usr/sbin/xinetd.
- Su fichero de configuración por defecto es /etc/xinetd.conf.
  - Complejidad muy superior a la del fichero /etc/inetd.conf.
- Las entradas del fichero son de la forma:

```
service <nombre del servicio>
{
   <atributo> <operador> <valor>...
   ...
}
```

El servidor xinetd (II)

- Donde:
  - <nombre del servicio>: Servicio que configura esta entrada.
  - <atributo>: Atributo que se esta configurando.
  - <operador>: Operación que se realiza:
    - = Asignar valor al atributo.
    - += Añadir valor al atributo.
    - -= Eliminar valor del atributo.
    - La mayoría de atributos solo admiten el operador =.
  - <valor>: Valor a asignar, añadir o eliminar.

El servidor xinetd (III)

Atributo	Descripción
id	Identifica de forma univoca el servicio. Este atributo tiene por defecto el nombre del servicio y, de forma general, solo es necesario cuando un mismo servicio posee diferentes protocolos y necesita ser descrito con diferentes entradas en el fichero de configuración.
type	Identifica el tipo de servicio y puede ser una combinación de los valores RPC (servicio RPC), INTERNAL (servicio proporcionado por el propio *xinetd*), TCPMUX/TCPMUXPLUS (servicio que debe ser arrancado de acuerdo al protocolo descrito en el RFC 1078 en un puerto TCPMUX bien conocido) y UNLISTED (servicio no listado en los ficheros estándar de servicios del ordenador).
flags	Identifica el modo de funcionamiento del servicio y es una combinación de los valores INTERCEPT (interceptar los paquetes o aceptar conexiones para verificar que provienen de ordenadores validos), NORETRY (no reintentar en caso de que falle la llamada a la creación de un proceso hijo mediante *fork*), IDONLY (aceptar conexiones solo cuando el ordenador remoto identifique al usuario remoto), NAMEINARGS (colocar el nombre del servicio como argumento primero en la llamada al servidor, tal y como sucede con *inetd*), NODELAY (permite que si el servicio es de tipo TCP, pueda configurarse la opción TCP_NODELAY en el socket), KEEPALIVE (permite que si el servicio es de tipo TCP, pueda configurarse la opción SO_KEEPALIVE en el socket), NOLIBWRAP (desactiva la llamada interna al TCPWrapper, con lo cual la llamada debe ser realizada de forma explícita como sucedía con *inetd*), SENSOR (reemplaza el servicio con un sensor que detecta los accesos al puerto especificado), IPv4 (especifica que el servicio es de tipo IPv4, esto es, AF_INET) y por último IPv6 (especifica que el servicio es de tipo IPv6, esto es, AF_INET6).
include	Indica el nombre de un fichero que será tomado como nuevo fichero de configuración.
includedir	Indica el nombre de un directorio cuyos ficheros serán añadidos como configuración de *xinetd*. De estos ficheros se excluye todos aquellos que contienen un punto en su nombre o terminan con una tilde (~).
disable	Es un valor booleano (“yes” o “no”) que indica si el servicio esta habilitado o deshabilitado.
enabled	Toma como argumento la lista de los *id* que deben ser habilitados. Aquellos que no se encuentren en esta lista serán deshabilitados.
socket_type	Especifica el tipo de socket, sus valores son *stream*, *dgram*, *raw* y *seqpacket* (secuencia de datagramas).

El servidor xinetd (IV)

Atributo	Descripción
protocol	Especifica el protocolo que emplea el servicio. Sus valores posibles son cualquier protocolo de transporte especificado en */etc/protocols*.
wait	Sus valores posibles son “yes” o “no” e indica si *xinetd* debe esperar la finalización del servidor de ese servicio antes de lanzar otro servidor (valor “yes”) o no (valor “no”).
user	Determina el UID con el que se ejecutara el proceso. Dicho UID debe existir en el fichero */etc/password*.
group	Determina el GID del proceso servidor. Si el GID no existe se utiliza el GID del usuario.
server	Indica el nombre del programa que ejecuta este servicio.
server_args	Determina los argumentos que se pasaran al servidor.
rpc_versión	Determina la versión de RPC para un servicio RPC. La versión puede ser un número o un rango en el formato número-número.
rpc_number	Determina el número para un UNLISTED RPC.
env	Indica una lista de strings en formato ‘nombre=valor’. Esos strings serán añadidos a las variables de ambiente antes de arrancar el servidor.
passenv	Determina la lista de las variables de ambiente de *xinetd* que deben ser pasadas al proceso servidor.
port	Determina el puerto del servicio.
redirect	Permite a los servicios TCP ser redirigidos a otro ordenador. Cuando *xinetd* recibe una conexión TCP a ese puerto, establece una conexión con el ordenador y puerto especificado y envía todos los datos entre los dos ordenadores. La sintaxis es *redirect* = <*dirección IP*> <*puerto*>.

El servidor xinetd (V)

Atributo	Descripción
bind	Permite al servicio ser asignado a una determinada dirección IP o interface específico del ordenador, esto permite, por ejemplo, que el servicio este disponible para un interface de la intranet y no para el interface que da acceso a Internet, su sintaxis es *bind = <dirección IP o interface>*.
interface	Es un sinónimo de *bind*.
groups	Puede tomar los valores “yes” o “no” e indica si el servidor es ejecutado con los permisos de los grupos a los que el UID del servidor tiene acceso o no.
umask	Especifica la máscara del servicio en formato octal. La máscara por defecto es 022.

El servidor xinetd (VI)

Atributo	Descripción
only_from	Indica que ordenadores están autorizados a ejecutar este servicio en particular. Las formas más comunes de especificación son mediante una dirección IP concreta (147.156.222.65), un rango de direcciones IP especificado en formato dirección/rango de la mascara (147.156.222.0/23), el nombre de un ordenador (*glup.irobot.uv.es*) o el nombre de un dominio (*.irobot.uv.es*).
no_access	Determina que ordenadores no están autorizados a ejecutar este servicio en particular. El formato de especificación es igual al de *only_from*.
access_times	Indica el intervalo de horas en que el servicio esta disponible. El formato es hh:mm-hh:mm, donde hh va de 0 a 23 y mm de 0 a 59.
instances	Indica el número de servidores que pueden estar activos simultáneamente. El valor por defecto es sin límite.
per_source	Especifica el número de instancias permitidas de este servicio por dirección IP. Su valor es un entero o UNLIMITED si no se desea limitarlo.
cps	Especifica el número máximo de conexiones por segundo que pueden ser recibidas por este servicio. Sus argumentos son dos enteros, el primero indica el número máximo de conexiones que pueden ser recibidas y el segundo el intervalo en segundos en que el servicio estará deshabilitado si se sobrepasa el valor anterior.
deny_time	Especificá el tiempo de denegación de acceso a todos los servicios para una IP que ha sido indicada por el *flag* de SENSOR. Los valores posibles son FOREVER, NEVER y un valor numérico. FOREVER causa que la dirección IP no tenga acceso a los servicios hasta que *xinetd* sea restaurado, NEVER permite que la dirección IP continué teniendo acceso y el valor numérico indica el número de minutos en que le será denegado el acceso.

El servidor xinetd (VII)

Atributo	Descripción
nice	Determina la prioridad con la que se ejecuta el servidor.
max_load	Es un número en coma flotante que indica la carga (porcentaje de CPU) máxima para un servicio. En caso de que dicho valor se sobrepase el servicio dejará de aceptar conexiones.
rlimit_as	Determina el limite de memoria del servicio, el límite se especificá como un entero seguido de K (kilobytes) o M (megabytes) o UNLIMITED para indicar que no existe límite.
rlimit_cpu	Especifica el máximo número de segundos que el servidor puede utilizar de CPU. El límite se especifica como un entero o UNLIMITED si no existe.
rlimit_data	Especifica el tamaño máximo de los datos que el servidor puede utilizar. El límite se especifica como un entero indicando los bytes o UNLIMITED si no existe.
rlimit_rss	Especifica el tamaño máximo del programa que debe permanecer residente. Un tamaño pequeño hace a este servicio candidato a ser volcado a disco cuando la cantidad de memoria disponible es baja.. El tamaño se especificá como un entero que indica el número de bytes o UNLIMITED si no existe.
rlimit_stack	Especifica el tamaño máximo de la pila que el servidor puede utilizar. El límite se especifica como un entero indicando los bytes o UNLIMITED si no existe.

El servidor xinetd (VIII)

Atributo	Descripción
banner	Indica el nombre de un fichero que será mostrado en el ordenador remoto cuando una conexión a este servicio es solicitada.
banner_success	Indica el nombre de un fichero que será mostrado en el ordenador remoto cuando una conexión a este servicio es aceptada.
banner_fail	Indica el nombre de un fichero que será mostrado en el ordenador remoto cuanto una conexión a este servicio es rechazada.
log_type	Determina el tipo de log que utiliza el servicio, existen dos formas, SYSLOG y FILE. SYSLOG tiene la sintaxis SYSLOG syslog_facility [syslog_level] y especifica que el log será enviado al fichero de log del sistema con la facilidad especificada por syslog_facility (daemon, auth, authpriv, user, mail, lpr, new, uucp, ftp, local0-7) y el nivel especificado por syslog_level (emerg, alert, crit, err, warning, notice, info, debug), si el nivel no esta presente se asume info. Por su parte FILE tiene la sintaxis FILE file [soft_limit [hard_limit]] e indica que la salida será grabada en el fichero especificado por file, teniendo dicho fichero un limite soft y hard de forma similar a como sucede con los limites soft y hard en las cuotas de los usuarios.
log_on_success	Indica la información que será almacenada en el log cuando el servidor empieza y cuando termina. Puede ser cualquier combinación de los valores PID (identificador del proceso servidor), HOST (dirección del ordenador remoto), USERID (identificador del usuario), EXIT (código de terminación del servidor) y DURATION (duración del servicio).
log_on_failure	Indica la información que será almacenada cuando la petición es rechazada. Sus valores son una combinación de HOST (dirección del ordenador remoto), USERID (identificador del usuario) y ATTEMPT (guarda que ha sucedido un fallo, esta opción esta implícita en las dos anteriores).

El servidor xinetd (IX)

- Solamente las siguientes propiedades deben ser especificadas para cada servicio:
  - *socket_type*.
  - *user* (solo para servicios no internos).
  - *server* (solo para servicios no internos).
  - *wait*.
  - *protocol* (solo para servicios RPC o no listados).
  - *rpc_version* (solo para servicios RPC).
  - *rpc_number* (solo para servicios RPC no listados).
  - *port* (solo para servicios no listados).

El servidor xinetd (X)

- El fichero de configuración suele contener una entrada donde es posible especificar valores por defecto para algunos atributos.

```
defaults
{
   <atributo> = <valor>...
   ...
}
```

El servidor xinetd (XI)

- En la entrada defaults los atributos pueden ser:
  - *log_type*.
  - *bind*.
  - *per_source*.
  - *umask*.
  - *log_on_success*.
  - *log_on_failure*.
  - *only_from*.
  - *passenv*.
  - *instances*.
  - *disable*.
  - *enabled*.
  - *banner*.
  - *banner_success*.
  - *banner_fail*.
  - *per_source*.
  - *groups*.
  - *cps*.
  - *max_load*.

El servidor xinetd (XII)

- Ejemplo de fichero /etc/xinetd.conf:

```
defaults
{
 log_type    = SYSLOG daemon info
 log_on_failure  = HOST
 log_on_success  = PID HOST DURATION EXIT
 cps         = 50 10
 instances       = 50
    per_source      = 10
    v6_only     = no
    groups      = yes
    umask       = 002
}
includedir /etc/xinetd.d
```

El servidor xinetd (XIII)

- Ejemplos de ficheros en /etc/xinetd.d:
  - Fichero daytime-stream:

```
service daytime
{
   disable       = yes
   id            = daytime-stream
   type          = INTERNAL
   wait          = no
   socket_type   = stream
}
```

  - Fichero daytime-dgram:

```
service daytime
{
   disable       = yes
   id            = daytime-dgram
   type          = INTERNAL
   wait          = yes
   socket_type   = dgram
}
```

El servidor xinetd (XIV)

- Fichero rsync:

```
service rsync
{
   disable          = yes
   flags            = IPv6
   socket_type      = stream
   wait             = no
   user             = root
   server           = /usr/bin/rsync
   server_args      = --daemon
   log_on_failure   += USERID
}
```

- Fichero telnet:

```
service telnet
{
   flags            = REUSE
   socket_type      = stream
   wait             = no
   user             = root
   server           = /usr/sbin/in.telnetd
   log_on_failure   += USERID
   disable          = yes
}
```

El servidor xinetd (XV)

- Fichero tftp:

```
service tftp
{
   socket_type   = dgram
   protocol      = udp
   wait          = yes
   user          = root
   server        = /usr/sbin/in.tftpd
   server_args   = -s /var/lib/tftpboot
   disable       = yes
   per_source    = 11
   cps           = 100 2
   flags         = IPv4
}
```

El envolvente de acceso de Linux (I)

- El envolvente de acceso analiza las peticiones antes que el servidor xinetd.
  - Una petición de servicio rechazada por el envolvente no es analizada por xinetd.
- Su configuración se basa en los ficheros:
  - /etc/hosts.allow: Servicios/ordenadores permitidos.
  - /etc/hosts.deny: Servicios/ordenadores denegados.
- Los ficheros se analizan como se explico con anterioridad.

El envolvente de acceso de Linux (II)

- La sintaxis de las reglas de los ficheros es:

```
<lista de servicios>: <lista de clientes>
  [: spawn <comando de shell>]
```

  - <lista de servicios>: Uno o más servicios separados por espacios. Los servicios se identifican por:
    - El nombre del servidor que los proporciona (vsftpd, sshd, in.telnetd).
    - El nombre del servicio (daytime, echo) si es proporcionado por xinetd.
  - <lista de clientes>: Uno o más ordenadores (nombre ó IPs) o patrones separados por espacios.
  - <comando de shell>: Acción opcional a ejecutar si una regla se cumple.

El envolvente de acceso de Linux (III)

- Existen tres elementos para definir los patrones:
  - . : Indica todo un dominio o conjunto de direcciones IP:
    - Dominio: .irobot.uv.es
    - Conjunto de direcciones IP: 147.156.
  - * : Cero o más caracteres.
  - ? : Un carácter.
- Además, existen palabras clave:

Palabra	Descripción
ALL	Especifica todos los ordenadores.
LOCAL	Especifica todos los ordenadores de nuestra red local, esto es, que no contienen el carácter '.' en su nombre.
KNOWN	Especifica todos los ordenadores cuyo nombre o dirección IP son conocidos.
UNKNOW	Especifica todos los ordenadores cuyo nombre o dirección IP es desconocidos.
PARANOID	Especifica todos los ordenadores cuyo nombre no corresponde con su dirección IP.

El envolvente de acceso de Linux (IV)

- La lista de clientes puede contener el operador EXCEPT.
  - Permite combinar dos listas en la misma línea.
  - La lista de servicios se aplica a los clientes de la primera lista de clientes excepto los indicados en la segunda lista.
  - Ejemplo:

```
vsftpd: .irobot.uv.es EXCEPT amparo.irobot.uv.es glup.irobot.uv.es
```

- La lista de servicios puede contener el valor ALL para indicar todos los servicios.

```
ALL: ALL EXCEPT in.telnetd: amparo.irobot.uv.es
```

El envolvente de acceso de Linux (V)

- La opción spawn permite ejecutar el comando indicado a continuación.

```
in.telnetd: .irobot.uv.es : spawn (/bin/echo `date` %c >>
  /var/log/telnet.log) &
```

Carácter	Descripción
%a	La dirección IP del cliente.
%A	La dirección IP del servidor.
%c	Proporciona una variedad de información como el nombre del usuario y el nombre del ordenador, o el nombre del usuario y la dirección IP.
%d	El nombre del servicio solicitado.
%h	El nombre del cliente (o dirección IP si el nombre no existe).
%H	El nombre del servidor (o dirección IP si el nombre no existe).
%n	El nombre del cliente. Si no existe se escribe *unknow*. Si el nombre del cliente y su dirección IP no coinciden se escribe *paranoid*.
%N	El nombre del servidor. Si no existe se escribe *unknow*. Si el nombre del cliente y su dirección IP no coinciden se escribe *paranoid*.
%p	El identificador del proceso del servicio.
%s	Proporciona una variedad de información como el identificador del proceso y el nombre o dirección IP del servidor.
%u	El nombre del cliente. Si no existe se escribe *unknow*.

El envolvente de acceso de Linux (VI)

- Ejemplo:

```
# Fichero hosts.allow
# Servicio FTP (21/tcp) permitido a todo el mundo
vsftpd: ALL
# Servicio SSH (22/tcp) permitido a todo el mundo
sshd: ALL
# Servicio daytime (13/tcp) permitido solo a Robótica
daytime: .irobot.uv.es

# Fichero hosts.deny
ALL : ALL : spawn (/bin/echo `date` %h %d >>
  /var/log/deny.log) &
```