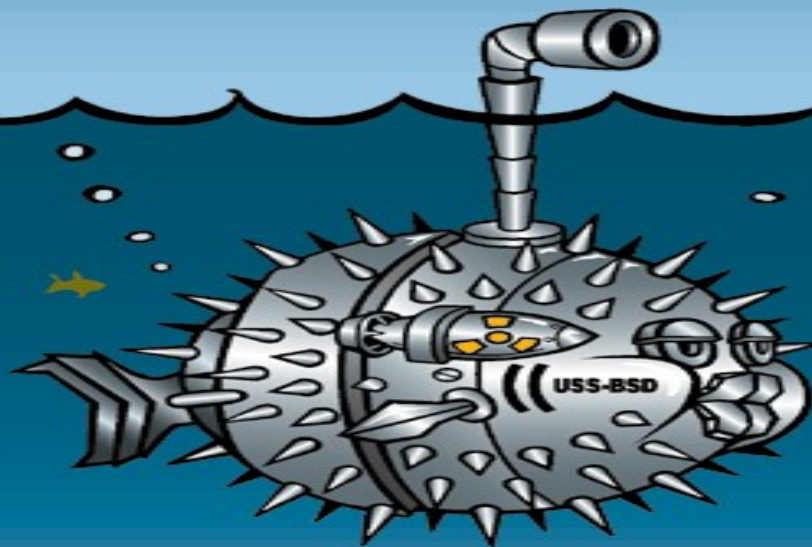


OpenSSH

Putting an end to unencrypted network logins



RLOGIN
1982-99
LIVED LIFE
WITH JOY

TELNET
1971-99
WONT CRYPT

RSH
1982-99
++



www.OpenSSH.com



OPENSSSH LE
ENSEÑA LAS
BRAGAS AL MUNDO
:O

NECESIDAD

una necesidad => **UNA SOLUCIÓN**

necesidad de privacidad!!!

por qué necesito la privacidad si no me persigue el FBI??

CRIPTOGRAFIA SIMETRICA

Misma clave para encriptar y desencriptar.

PROBLEMA: transmisión de clave en claro

Diferentes tipos:

bloque

flujo

CRIPTOGRAFIA ASIMETRICA

Dos claves (pública y privada):

privada => pública

pública !=>! privada

Operaciones:

encriptar (clave pública)

firmar (clave privada)

PROBLEMA: coste computacional (se utilizan hash)

MAC

FUNCIONES HASH

- garantiza la integridad de datos
- características

MAC (Message Code Authentication)

integridad de funciones hash

MAC = hash (datos + clave_simétrica)

CARACTERISTICAS SSH

- integridad
- confidencialidad
- autenticación
- autorización

AUTENTICACIÓN SSH-2

SSH-2 (autenticación):

contraseña

clau pública

máquinas de confianza

GSSAPI

keyboard-interactive

CONTRASEÑA vs PUBKEY

Deficiencias contraseña:

MITM se podría capturar

ataques de fuerza bruta

conociendo la contraseña tenemos acceso

PREREQUISITOS OPENSSSH

Prerequisitos:

OpenSSL

zlib

PAM (opcional)

USO BÁSICO

Para conectar a un servidor SSH:

```
ssh servidor_SSH
```

```
ssh -l login servidor_SSH  
ssh login@servidor_SSH
```

GENERACION CLAVES

Podemos generar claves RSA o DSA:

```
ssh-keygen -t rsa -b 4096
```

NOTA: con DSA se limita la máxima longitud a 1024 bits.

GENERACION CLAVES II

IMPORTANTE: establecer una frase de paso!!!

TEOREMA DE LA CAGADA

++++
OLVIDAR CLAVE PASO = CAGADA GORDA Y PELUDA
++++

INSTALAR CLAVE PUBLICA

Copiar nuestra clave pública en servidores SSH:

```
ssh-copy-id -i .ssh/id_dsa.pub login@servidor_SSH
```

Otra forma (**only frikis!!!**):

```
ssh servidor_SSH 'umask 077; cat >> .ssh/authorized_keys' < .ssh/id_dsa.pub
```

CUIDADIN

Peligro con el primer contacto con un servidor SSH!!!

Conveniente tener previamente el fingerprint

CUIDADIN II

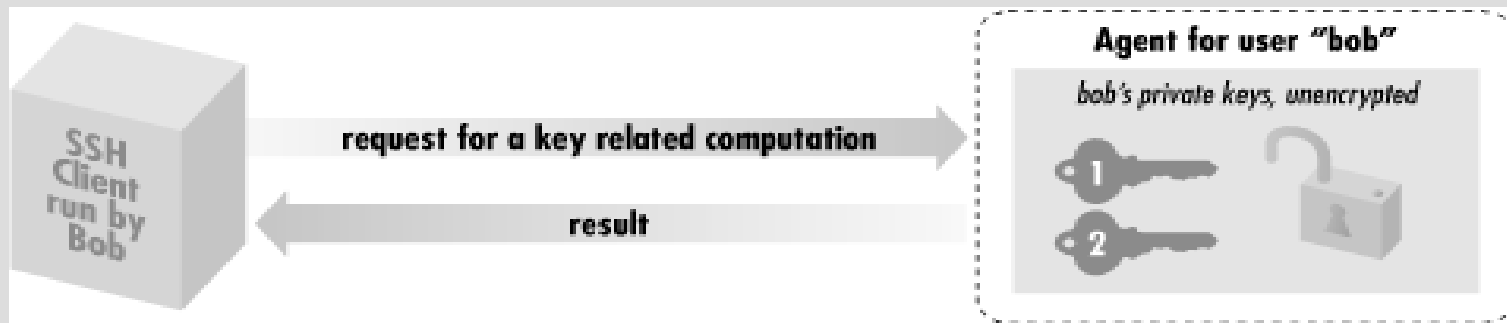
```
user@host:~$ ssh futura.disca.upv.es
The authenticity of host 'futura.disca.upv.es (158.42.180.173)' can't be
established.
RSA key fingerprint is a9:d0:bc:7d:2e:02:ba:9f:ff:f3:b7:cf:e6:cc:75:00.
Are you sure you want to continue connecting (yes/no)?
```

Es un momento de MUCHA TENSION, y nos podríamos quedar así...

AGENT

Se encarga de:

- almacena claves privadas en memoria.
- responde peticiones.



UTIL PARA GENTE MUY MUY VAGA

FUNCIONAMIENTO AGENT

Creación de un directorio en /tmp que contiene un socket unix domain.

ssh-add añade claves privadas en el agent.

Para visualizar las claves privadas:

```
ssh-add -l  
ssh-add -L
```

AUTHORIZED_KEYS

Fichero que donde cada línea contiene:

- opciones (opcionales).
- tipo de clave (RSA o DSA).
- clave pública.
- comentario (opcional).

FORCED COMMANDS

No se sirve un shell en bandeja!!

Fuerza a ejecutar un comando.

IMPORTANTE: el **forced command** no debería ser:

- shell_escape
- compiladores, intérpretes, ...
- programas setuidados/setgeidados.

CONTROL DE ACCESO

Restricción de acceso por IP o nombre de máquina:

```
from="192.168.1.45" ssh-dss .....
```

```
from="pepito.lospepes.com" ssh-dss .....
```

Se pueden utilizar caracteres comodín (* ?):

```
from="192.168.1.*" ssh-dss .....
```

```
from="*.lospepe.com" ssh-dss .....
```

IMPORTANTE: más seguridad restringiendo por IP.

OTRAS OPCIONES

DESACTIVAR FORWARDING

```
no-port-forwarding  ssh-dss .....  
no-agent-forwarding ssh-dss .....  
no-x11-forwarding   ssh-dss .....
```

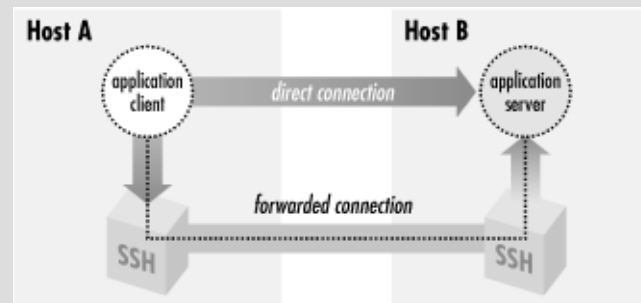
DESACTIVAR TTY

```
no-pty ssh-dss .....
```

NOTA: no se puede forzar la asignación de un pseudo-terminal.

QUE COÑO ES EL FORWARDING?

Forwarding (tunneling): encapsulación de un protocolo en otro.



Transparente una vez configurado.

Añade seguridad en protocolos inseguros.

QUE COÑO ES EL FORWARDING? II

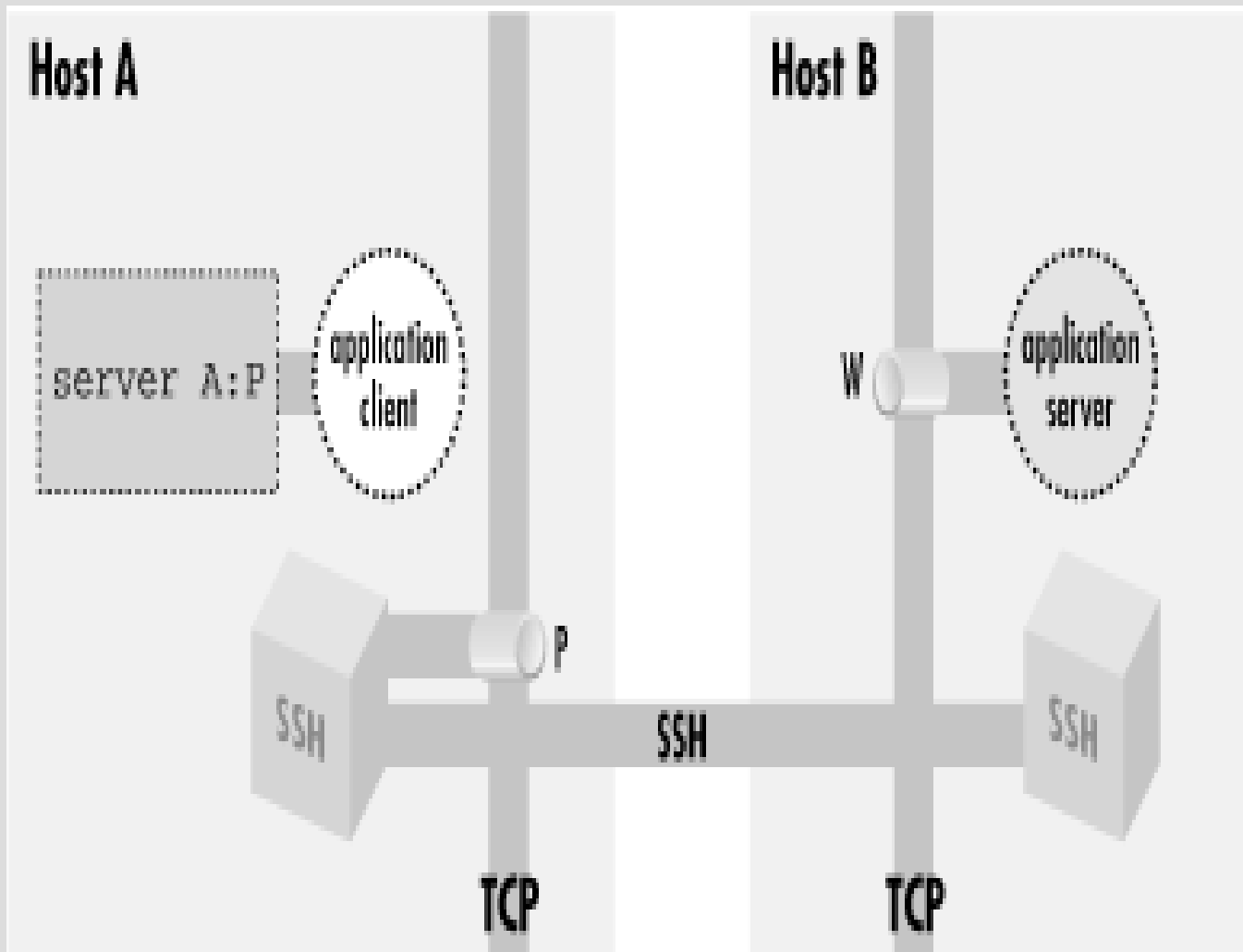
Tres tipos:

port forwarding

X11 forwarding

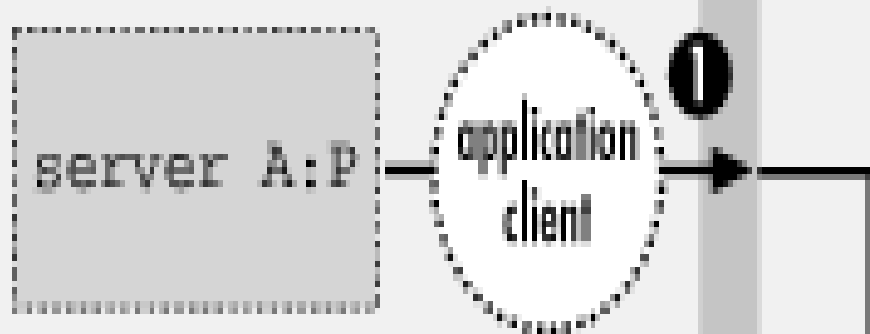
agent forwarding

PORT FORWARDING

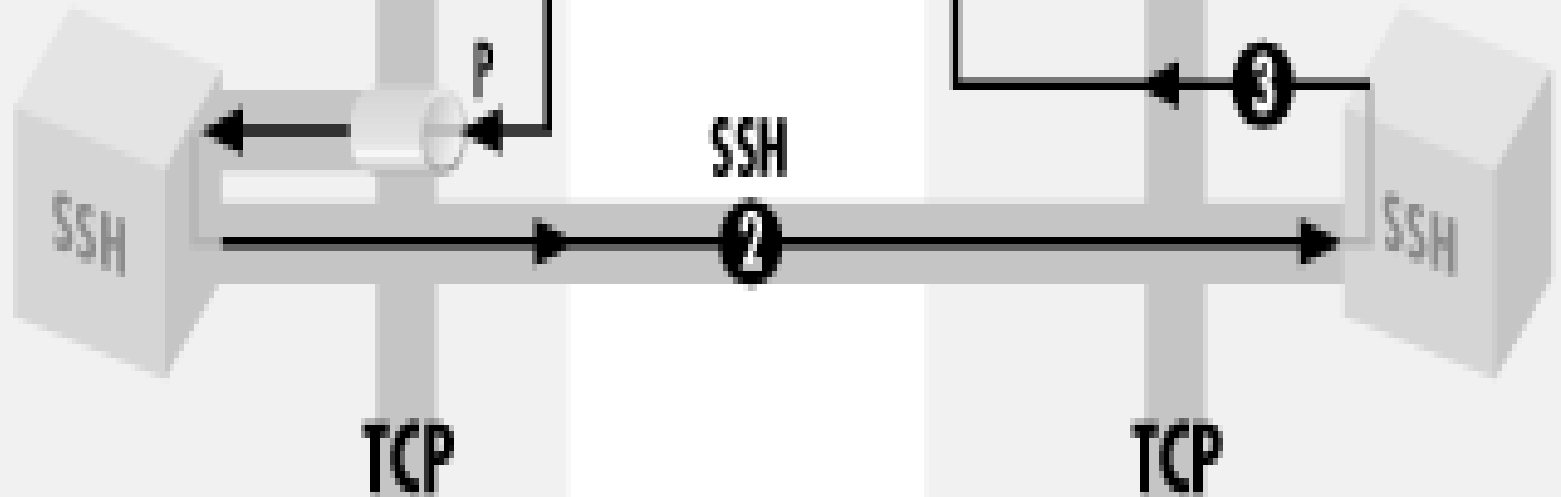
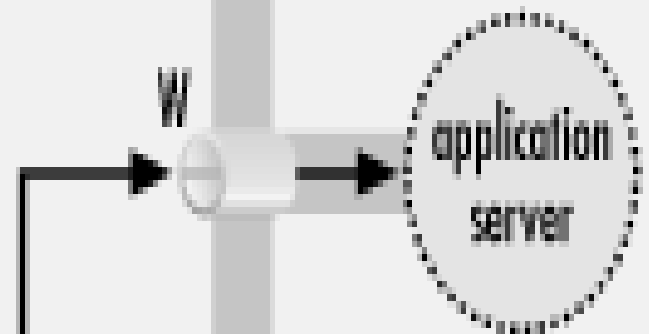


PORT FORWARDING II

Host A



Host B



PORT FORWARDING III

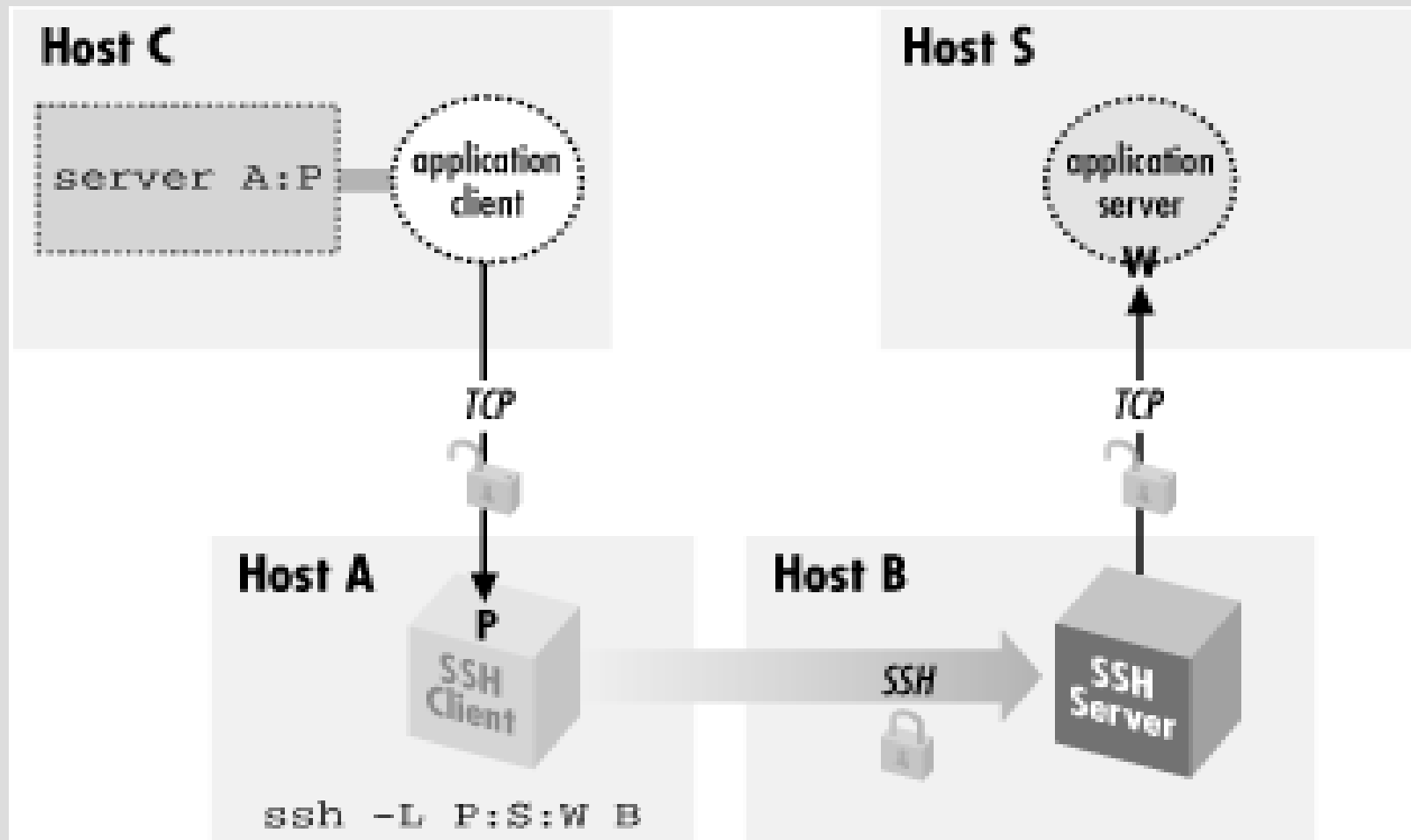
Dos tipos de port forwarding:

- local forwarding

- remote forwarding

LOCAL FORWARDING

```
ssh -fN -L8080:serverWeb:80 servidorWeb
```



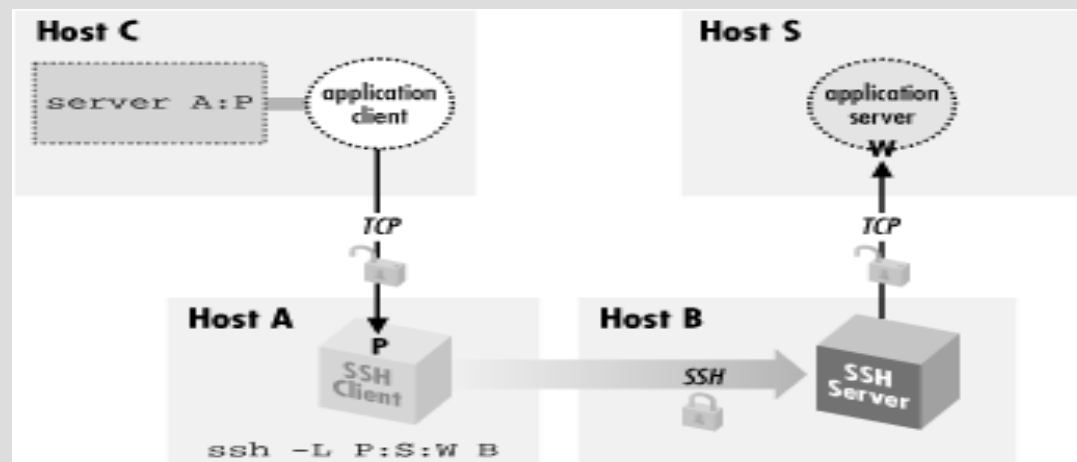
LOCAL FORWARDING II

OFF HOST:

aplicación cliente y cliente SSH en diferentes máquinas.

aplicación servidora y servidor SSH en diferentes máquinas.

NOTA: caso extremo de off host si se produce a la vez.



SEGURIDAD: viajan paquetes en claro por la red.

REMOTE FORWARDING

Se abren un puerto en remoto:

```
ssh -fN -R8080:localhost:80 servidorSSH
```

off-host en el siguiente caso:

```
ssh -fN -R8080:www.upv.es:80 servidorSSH
```

BURLAR CORTAFUEGOS

LOCAL FORWARDING -> si el cortafuegos permite acceso al puerto 22.

REMOTE FORWARDING -> conectar desde casa al trabajo.

AGENT FORWARDING

Ventajas:

un agent funcionando

mantener la clave privada en una máquina

autenticación transparente en diferentes servidores

PREGUNTAS?

Por favor NO

ya he trabajado bastante, no creéis?

AGRADECIMIENTOS

ColdWind
Zeros
germen
hdx303
slack
rafeta
TuXeD
galidor
juanki
okahei

-a SeT y Belén por mostrar de que trabaja realmente Galidor.

-a mis padres por pagarme la carrera y otras cosas que no saben :)

-a los pijos por darme la oportunidad de burlarme de ellos y hacer mi vida más divertida

-y a vosotros por estar aquí (hay que hacer la pelota...)