ULPGC Universidad de Las Palmas de Gran Canaria | ESCUELA DE INGENIERÍA INFORMÁTICA

Administración de Sistemas Operativos

Tema 4.1
Administración de usuarios y grupos
RESUMEN

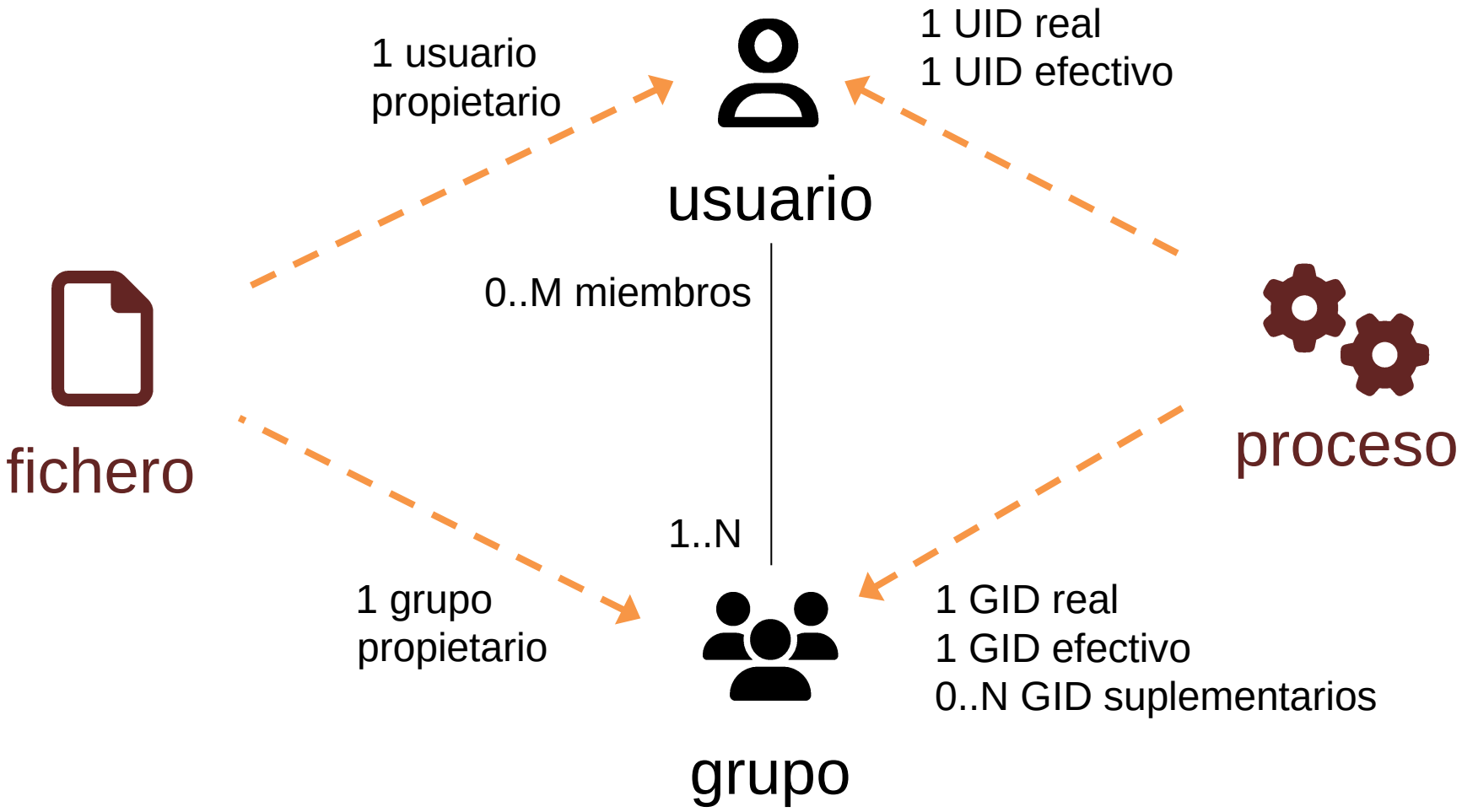
Esquema general

- Usuarios y grupos
- Cuenta, contraseña, UID, GID
- El superusuario (root)
- Usuario/grupo propietario de un recurso
- Caducidad de contraseñas (*password aging*)
- Ficheros administrativos: /etc/passwd, /etc/group…
- Utilidades: useradd, chage, newgrp, passwd...

Usuarios y grupos en UNIX

- UNIX articula su política de permisos de acceso en torno a los conceptos de **usuarios** y **grupos** de usuarios.
- Se pueden definir múltiples **cuentas de usuario** (*user accounts*).
- Una cuenta de usuario tiene un nombre (ej. «jomis») y un **UID** (ej. 1413).
- Para abrir sesión (*login*), hay que proporcionar un nombre de cuenta y su **contraseña** (*user password*).
- Un usuario puede pertenecer a uno o más grupos. Cada grupo tiene un nombre y un **GID**.
- Existe un usuario administrador (**root, UID=0**) con privilegios completos sobre todo el sistema. A veces se le llama **«superusuario»** (*super-user*).

Arquitectura de permisos en UNIX



ULPGC

Permisos de acceso a los recursos: reglas básicas

- Todo **fichero** (o directorio) tiene un **usuario propietario** y un **grupo propietario**.
- Un fichero (o directorio) permite establecer permisos de lectura, escritura, ejecución y otros. Según qué usuario esté accediendo, se comprueba si tiene permiso para realizar la operación. Sólo el usuario propietario puede cambiar los permisos de acceso (**chmod**).
- Un **proceso** pertenece a un usuario y al menos a un grupo (se llaman **UID real** y **GID real**) y se ejecuta a nombre de un par **UID/GID efectivos**. El proceso también puede pertenecer a varios **grupos suplementarios**.
- Sólo el usuario propietario de un proceso puede matarlo o realizarle modificaciones.
- Algunas operaciones del núcleo son **privilegiadas** (sólo puede realizarlas el superusuario). Ej. **chown**, **chroot**, etc.

ULPGC

Archivos para gestión de cuentas

usuarios

grupos

/etc/passwd

/etc/group

login:passwd:uid:gid:GECOS:homedir:shell

group_name:passwd:gid:userlist

/etc/shadow

/etc/gshadow

login:passwd:
creation_date:
min_change:
max_change:
grace_period:
days_expire:
time_expire:
reserved

name:passwd:adminlist:memberlist

ULPGC

Órdenes para gestión de cuentas

	crear	**borrar**	**modificar**	**acceder**	**salir**
usuarios	useradd	userdel	usermod chfn chsh	login su sudo	logout
grupos	groupadd	groupdel	groupmod	newgrp sg	---

	Fichero principal	**Fichero de contraseñas**	**Cambiar contraseña**	**Política de contraseñas**
usuarios	/etc/passwd	/etc/shadow	passwd	chage
grupos	/etc/group	/etc/gshadow	gpasswd	---

ULPGC

/etc/passwd

pepe:x:503:666:Usuario pepe,+34666111555:/Users/pepe:/bin/bash

7 campos separados por «:»

1. **login name**
2. **password** (una «x» si está en uso /etc/shadow)
3. **UID** → entero identificador de usuario (no repetir)
4. **GID** → entero identificador de grupo primario (idem)
5. **GECOS field** (nombre, teléfono, …)
6. **home directory** (directorio del usuario)
7. **login shell** (listados en /etc/shells)

ULPGC

Alta de usuarios: procedimiento manual

1. Editar el fichero ***/etc/passwd***.
2. Editar el fichero ***/etc/shadow.***
3. Editar los ficheros ***/etc/group*** y ***/etc/gshadow***.
4. Crear el directorio de usuario.
5. Dar los permisos adecuados al directorio.
6. Copiar los ficheros típicos de configuración del shell. Están en ***/etc/skel***.
7. Asignar una clave de acceso (`passwd` *`cuenta`*).

*NOTA: los programas **vipw** y **vigr** permiten editar los ficheros de usuarios y grupos con seguridad (pasos 1-3).*

ULPGC

Alta de usuarios: utilidades

- **`useradd`**: automatiza muchas tareas del proceso de alta
  - Multitud de opciones permiten controlar el proceso de alta
- Ficheros/directorios implicados:
  - /etc/defaults/useradd
  - /etc/skel
- ejemplo:

```
# useradd perico
perico:x:502:503::/home/perico:/bin/bash
perico:!!:15285:0:99999:7:::
```

ULPGC

```
useradd -c “Pedro Pi” -g grupo -G
g_secundario -m -s /bin/zsh perico
```

/etc/passwd:

```
perico:x:502:504:Pedro Pi:/home/perico:/bin/zsh
```

/etc/shadow:

```
perico:!!:15285:0:99999:7:::
```

Poner una clave: **`passwd perico`**

ULPGC

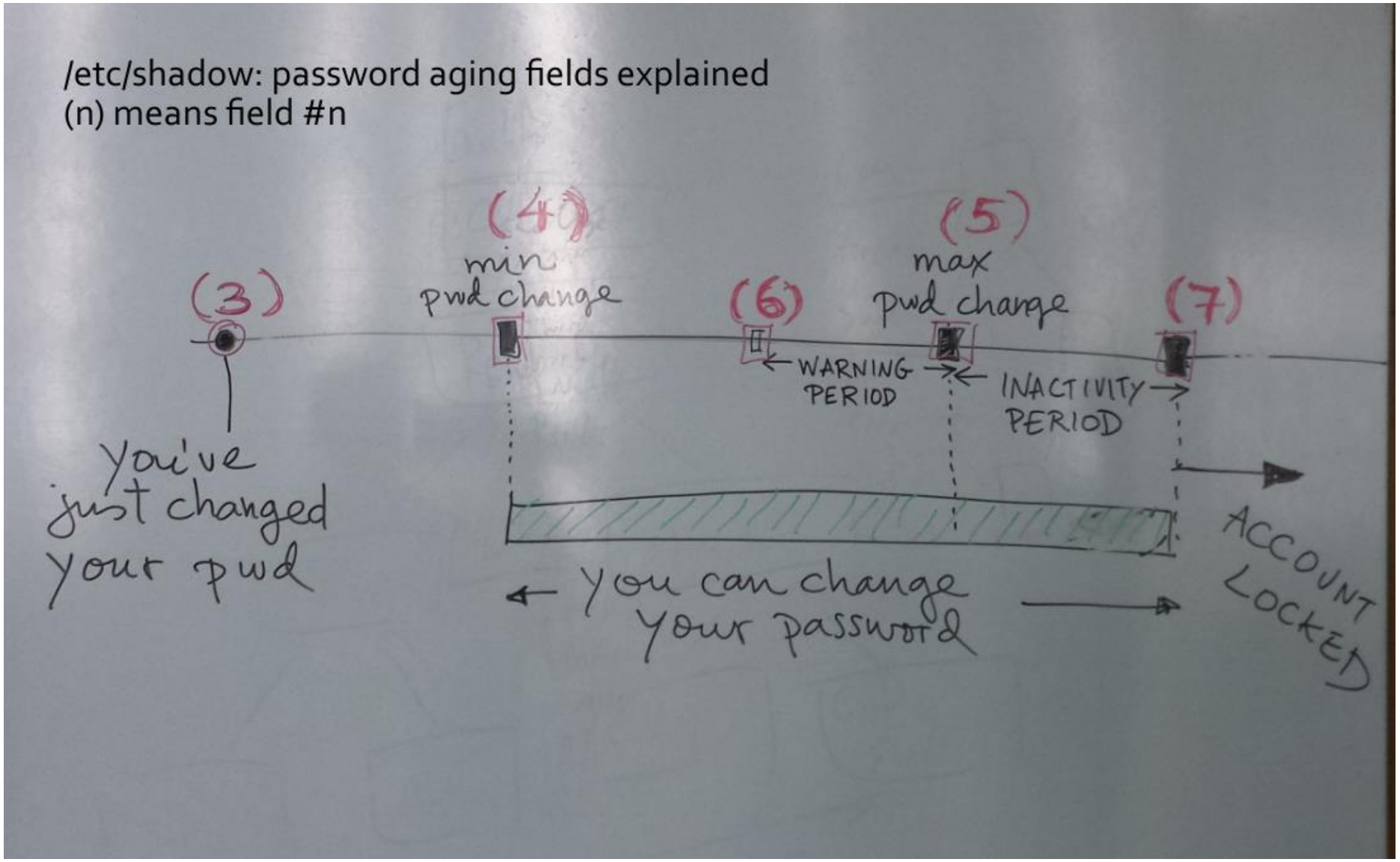
/etc/shadow

pepe:1EmN3ie2s$VPv/wGp68qnHO4LLv.0Ki0:15285:0:99999:7:::

- claves encriptadas + política de contraseñas (*password aging)*
  1. login name (ídem que /etc/passwd)
  2. clave encriptada
  3. fecha del último cambio de clave
  4. nº mínimo de días entre cambios de clave
  5. nº máximo de días entre cambios de clave
  6. nº de días de preaviso de caducidad de la clave
  7. nº de días permitidos antes de bloquear la cuenta por no cambiar la clave
  8. fecha de caducidad de la cuenta
  9. reservado para uso futuro

ULPGC

/etc/shadow: password aging fields explained
(n) means field #n



ULPGC

Administrar /etc/shadow

- **`chage`**: orden específica para manejar la caducidad de contraseñas
- También **`passwd`**, **`useradd`** y **`usermod`** tienen opciones para manejar la caducidad
- **`pwconv`**: concilia los ficheros /etc/passwd y /etc/shadow
- **/etc/login.defs**: opciones por defecto para la política de caducidad de contraseñas

/etc/group

```
chagewheel:x:10:trent,ned,evi,garth,lynda,millert
csstaff:*:100:lloyd,evi
student:*:200:dotty
```

Campos:

1. **Nombre del grupo**
2. **Contraseña encriptada:** una **«x»** cuando se usa gshadow
3. **GID:** número identificador de grupo
4. **Lista de usuarios** pertenecientes al grupo, separados por comas y sin espacios

/etc/gshadow

```
barrera:!!::barrera
cluster:$1$gfMdBPZP$NVOUnFjNaOSip27TBJeSl/::chema,cris
```

Campos:

1. nombre del grupo
2. contraseña (**`gpasswd`**)
3. lista de **administradores de grupo**
4. lista de miembros de grupo

ULPGC

Gestión de grupos: herramientas

- **`vigr`** : edita de forma segura los ficheros de grupos (/etc/groups y /etc/gshadow)
- **`groupadd`** : creación de nuevos grupos
- **`groupmod`** : modificación de grupos existentes

ULPGC

Gestión de grupos: herramientas

- **`usermod:`** permite modificar los atributos de la cuenta de un usuario:
  - cambiar el nombre de usuario
  - cambiar el grupo primario
  - agregar el usuario a un nuevo grupo secundario
  - establecer un nuevo shell
  - establecer el directorio de usuario (*home*)
  - bloquear/desbloquear la clave del usuario
  - …y alguna cosa más (ver el manual)

Gestión de grupos: herramientas

- **`groupmod:`** permite modificar grupos
  - cambiar el nombre de grupo
  - cambiar el identificador de grupo (gid)
- **`newgrp`** *grupo* : cambia el grupo primario del usuario actual a *grupo*
  - Si el usuario ya pertenece al grupo, **newgrp** realiza el cambio inmediatamente. Si no pertenece y el grupo tiene definida contraseña, el usuario debe introducir la contraseña.
- **`gpasswd:`**poner claves a grupos y administrar a los administradores de grupos

Otras utilidades

- **`userdel` :** eliminación de usuarios y (algunos) de sus ficheros y directorios
  - No elimina todos los ficheros del usuario
  - Tener en cuenta consideraciones de seguridad antes de eliminar usuarios/ficheros
- **`groupdel`** : eliminación de grupos

Algunas URL de interés

- http://tldp.org/HOWTO/Shadow-Password-HOWTO-7.html
- http://linux.die.net/man/5/gshadow