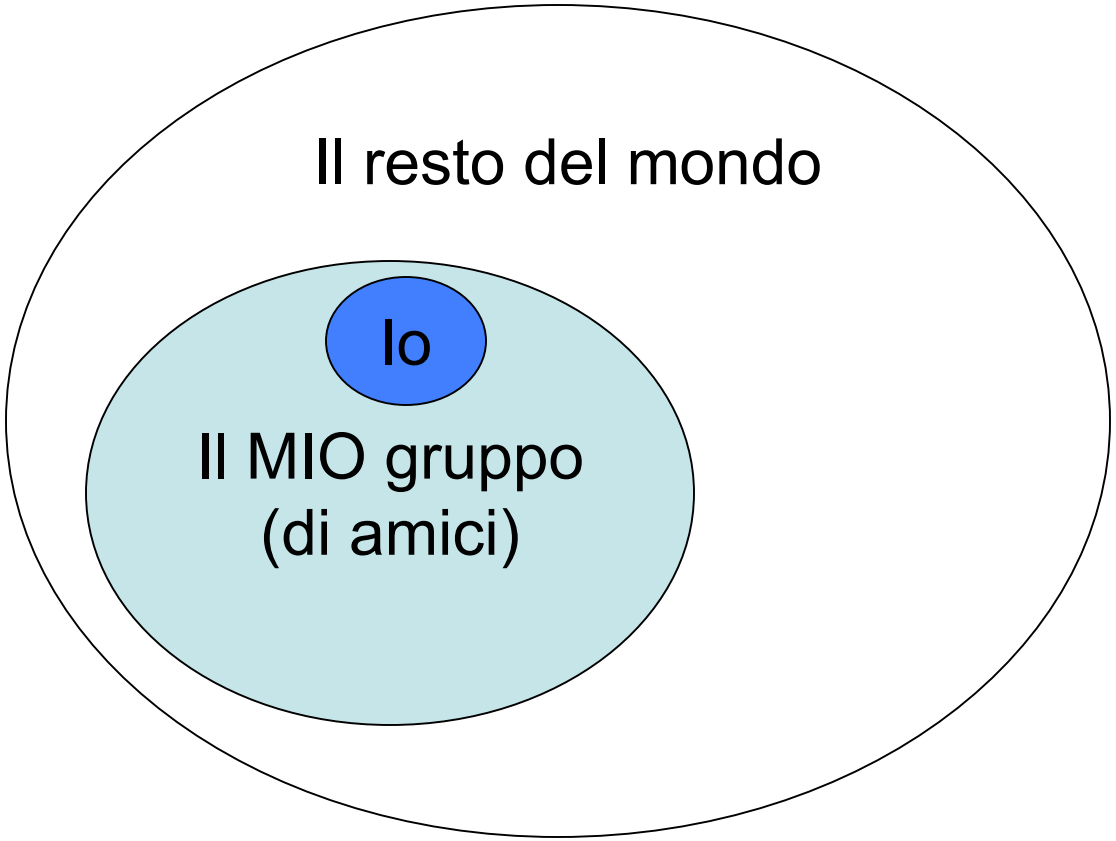
Modello sociale



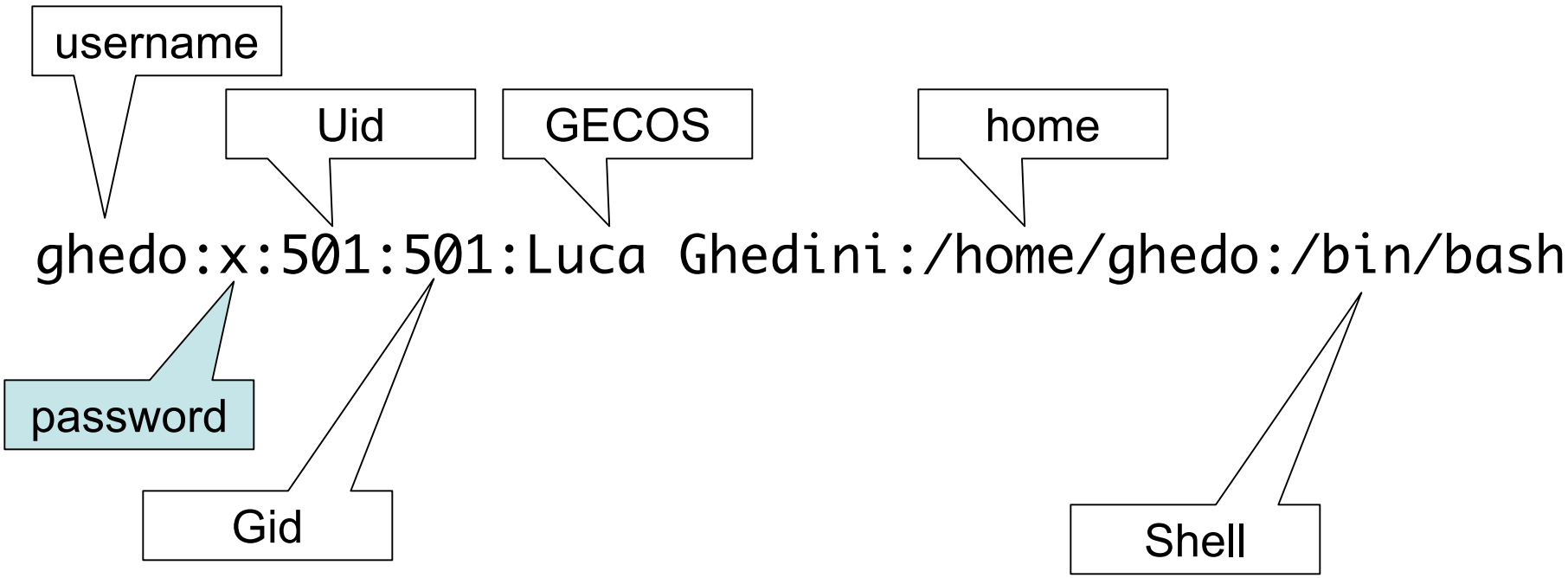
Utenti in locale

In unix tutto è file: Le protezioni si applicano ai file.
Ogni file ha 1 SOLO proprietario.

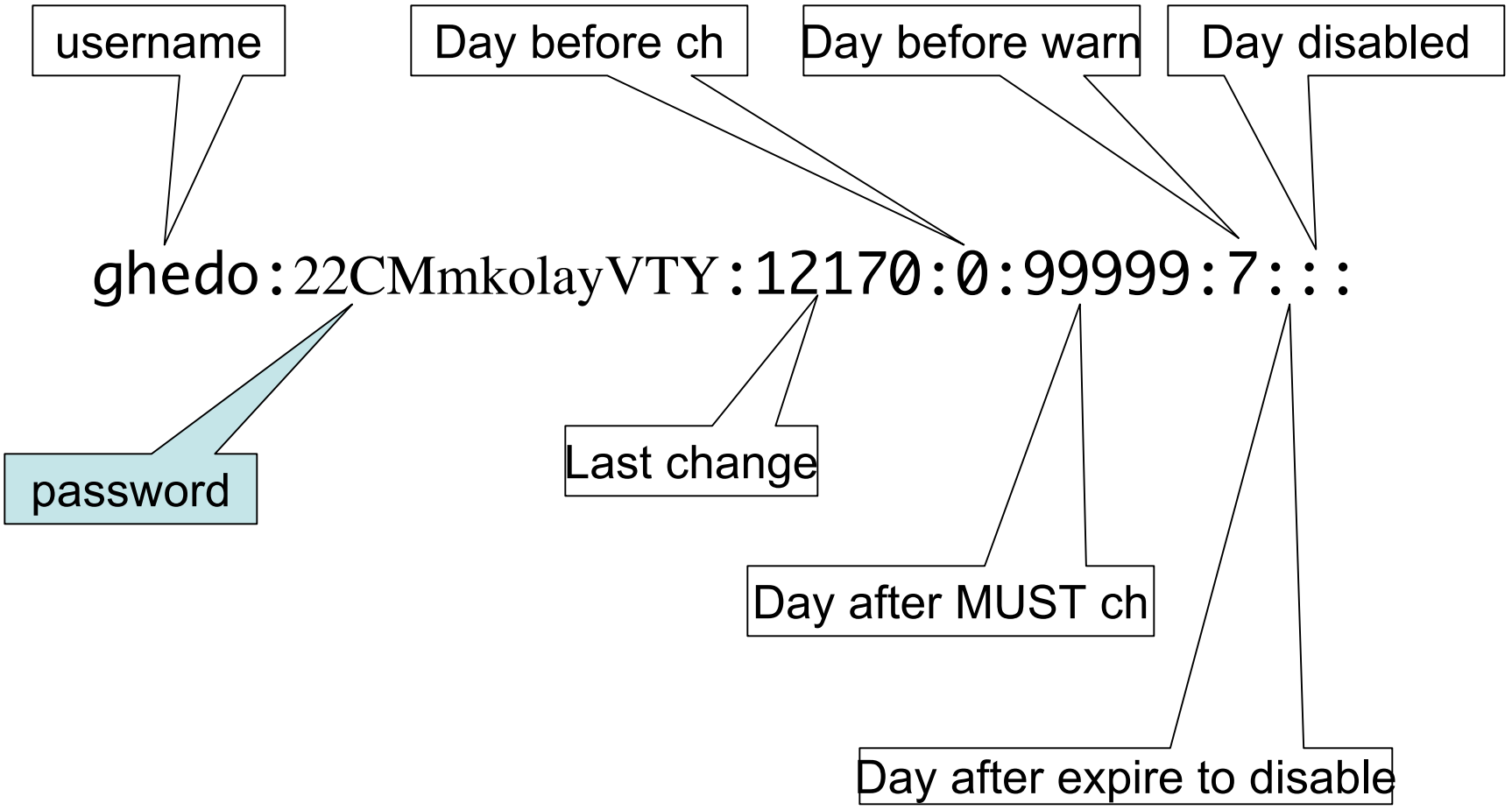
File di dati fondamentali:

- /etc/passwd (informazioni sugli utenti)
- /etc/shadow (password utenti)
- /etc/group (informazioni sui gruppi)

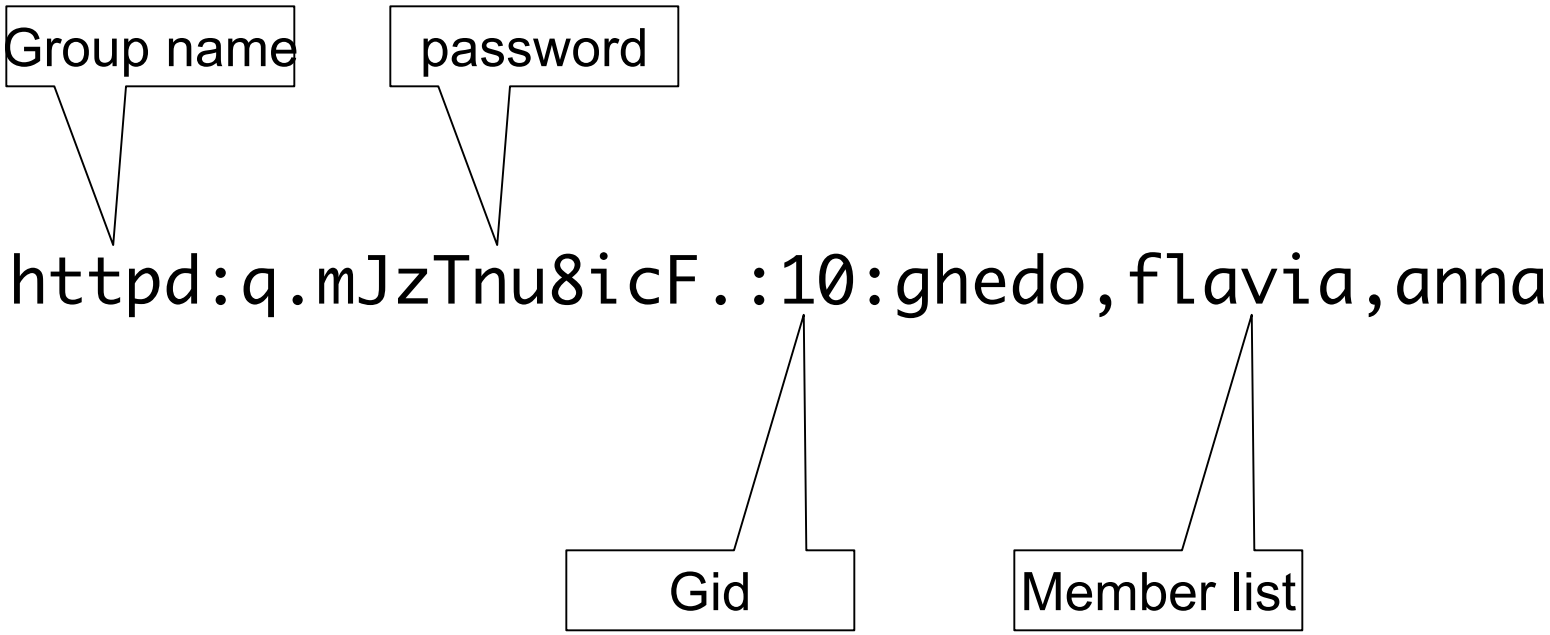
/etc/passwd


username
Uid
GECOS
home
ghedo:x:501:501:Luca Ghedini:/home/ghedo:/bin/bash
password
Gid
Shell

/etc/shadow

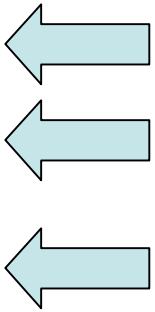

username
Day before ch
Day before warn
Day disabled
ghedo:22CMmkolayVTY:12170:0:99999:7:::
password
Last change
Day after MUST ch
Day after expire to disable

/etc/group

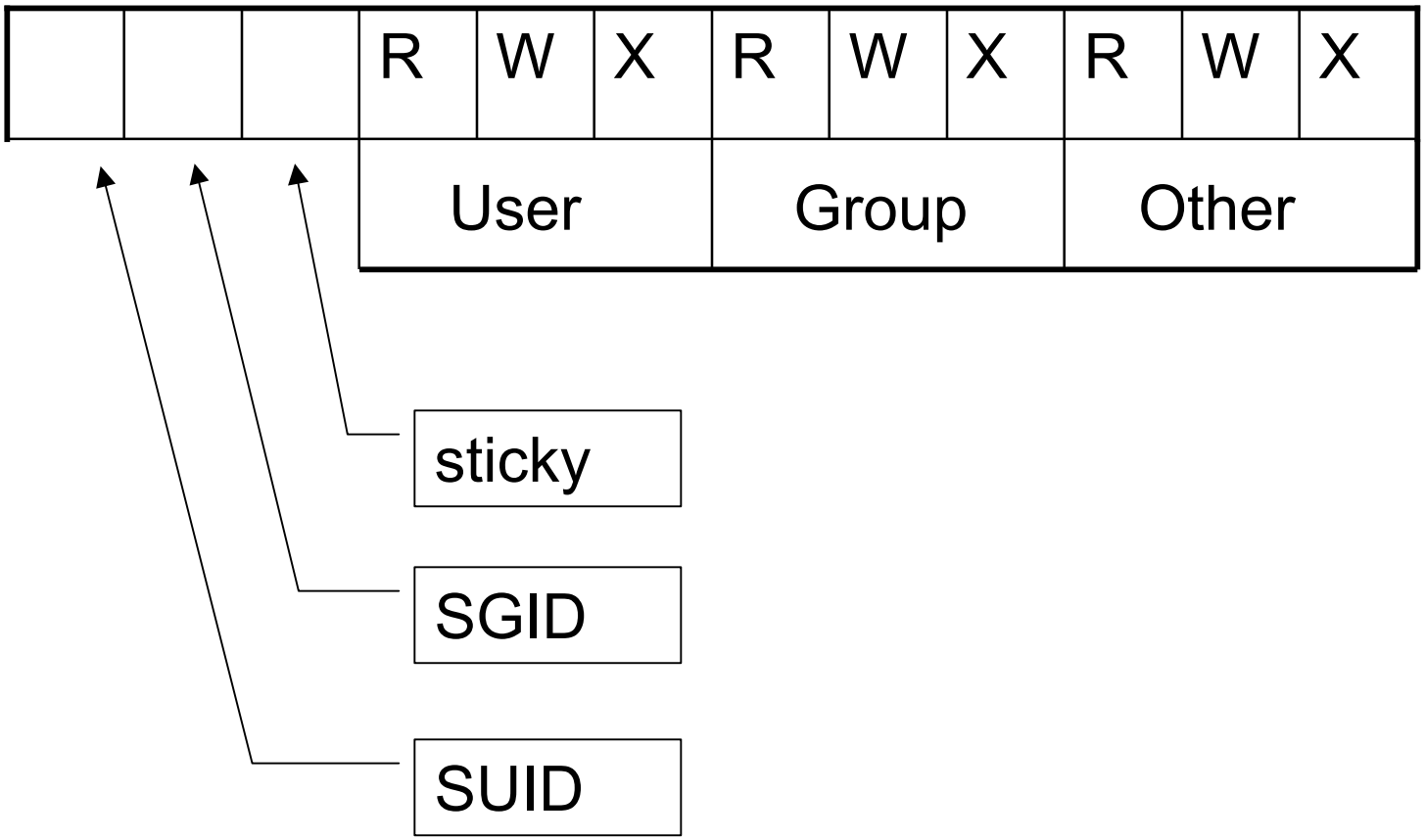

Group name
password
httpd:q.mJzTnu8icF.:10:ghedo,flavia,anna
Gid
Member list

Comandi utenti

useradd
passwd
chown
chfn
id
groupadd
groupdel
usermod



UGO!



Bit File Dir

	`file`	`directory`
R	Il file è leggibile da [U|G|O]	Consente di listare la dir
W	Il file è scrivibile da [U|G|O]	Rimozioni / aggiunte di entry dalla dir
X	Il file è eseguibile da [U|G|O]	cd nella dir

SUID SGID STICKY

	file	directory
Sticky	Suggerise al SO di conservare copia del programma nella swap (obsoleto)	Solo il propritario può cancellare un file Sticky anche se la dir è scrivibile da tutti
SGID	Il gid dell'utente che esegue un file SGID è assimilato al proprietario del file	I file creati dentro la dir sono asseganti al gruppo della dir ($file_{GID}$:=dir_{GID})
SUID	Il uid dell'utente che esegue un file SUID è assimilato al proprietario del file	

Note per le dir

“Le directory sono file che conservano l’elenco dei file contenuti in esse”

- il diritto di lettura su una directory è necessario per poter elencare i file contenuti
- il diritto di scrittura su una directory è necessario e **sufficiente** per poter **creare** e **cancellare** file al suo interno (non importa avere diritti sul file)
- il diritto di “esecuzione” va interpretato come possibilità di entrare nella directory (è sufficiente questo, ad esempio, per poter lanciare un programma che sta dentro una directory, anche se non si ha il diritto di lettura, a patto di conoscerne il nome)

Real & effective

Ogni utente è caratterizzato da una coppia UID GID (presa dal file passwd)

Se l'utente esegue programmi con SUID/SGID impostati, dell'ambito di quella esecuzione assume i UID/GID del programma.

Questi valori di UID/GID sono detti **effective**

Il sistema utilizza gli effective per ogni controllo a run time

La collaborazione

In un sistema unix la collaborazione fra utenti diversi avviene tramite la appartenenza ad un gruppo comune.

Due approcci

1. Creare più utenti con lo stesso Gid
2. Creare utenti con Gid differente ma assegnarli ad un gruppo comune (con Gid differente da entrambi)

1 più semplice ma meno sicuro: se utenti diversi partecipano a progetti diversi?

2 più complesso ma più sicuro (1 gruppo per progetto)

In the large…

- Quando gli utenti diventano migliaia ?
- Quando gli utenti operano su più elaboratori?

L’approccio a file diventa inefficiente

database di validazione degli utenti
servizi centralizzati di autenticazione

nis
pam
ldap