

Cursul #8

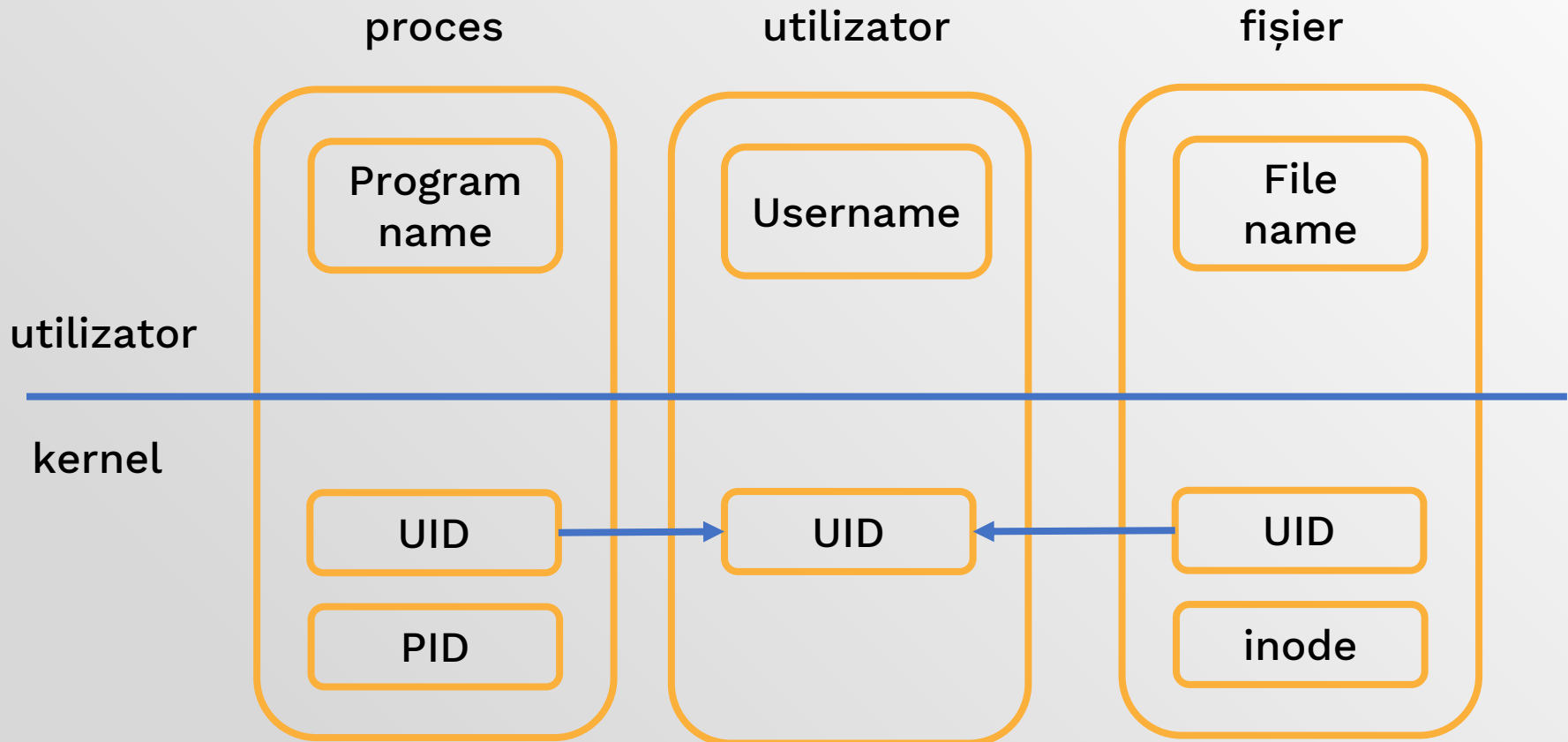
Utilizatori



*Treat your password like your toothbrush.
Don't let anybody else use it, and
get a new one every six months.*

Clifford Stoll

SF – utilizatori – procese



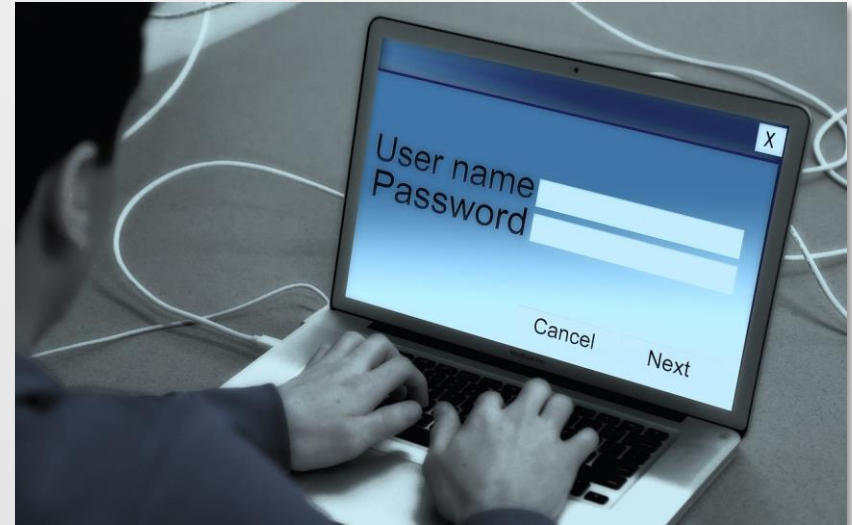
Utilizator =?

- Perspectiva umană
 - Persoană care folosește un sistem de calcul



Utilizator =?

- Perspectiva SO
 - Cont pe un sistem
 - Agent: execută acțiuni
 - Acces, drepturi, acțiuni, proprietate
 - Identificat prin username și UID
 - Procesele sunt create în cadrul unui utilizator



Separare

- Sisteme multi-utilizator
- Mai mulți utilizatori rulează simultan
- **Utilizatorii** separă:
 - Procesele
 - Fișierele
 - Alte resurse



Utilizator de ...

Sistem

- Cont care permite
 - Crearea de procese
 - Deținerea fișierelor
 - Crearea altor conturi

Aplicație

- Ex: conturi în aplicații web
- Acces la resurse gestionate de aplicație
- Nu permit accesul la resursele sistemului

La ce bun?

- Securizarea sistemului
- Depanarea problemelor de autentificare
- Identificarea acțiunilor ostile / abuzive



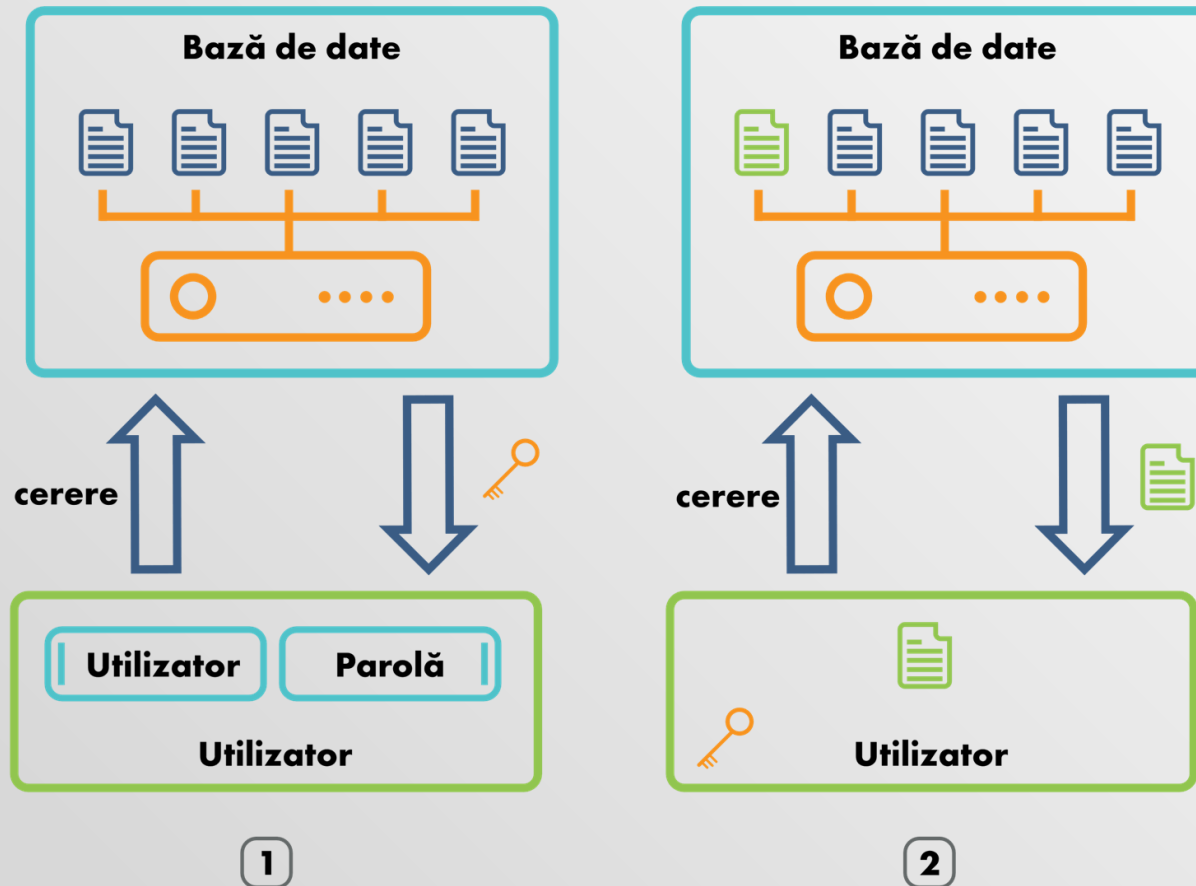
Operații

- Autentificare (*login*)
 - Furnizarea credențialelor
 - Parolă, semnătură digitală, amprentă
- Deconectare (*logout*)
- Schimbare parolă, detalii acces
- Schimbare utilizator curent (*switch user*)
- Rulare de procese cu permisiunile utilizatorului

Autentificare & permisiuni

- **Bază de date** cu toate username și forma de autentificare
- După autentificare, un utilizator are anumite **permisiuni**/drepturi
 - Conturi de aplicație: **roluri**
 - Moodle: student/profesor
 - Bloguri: admin/editor/cititor

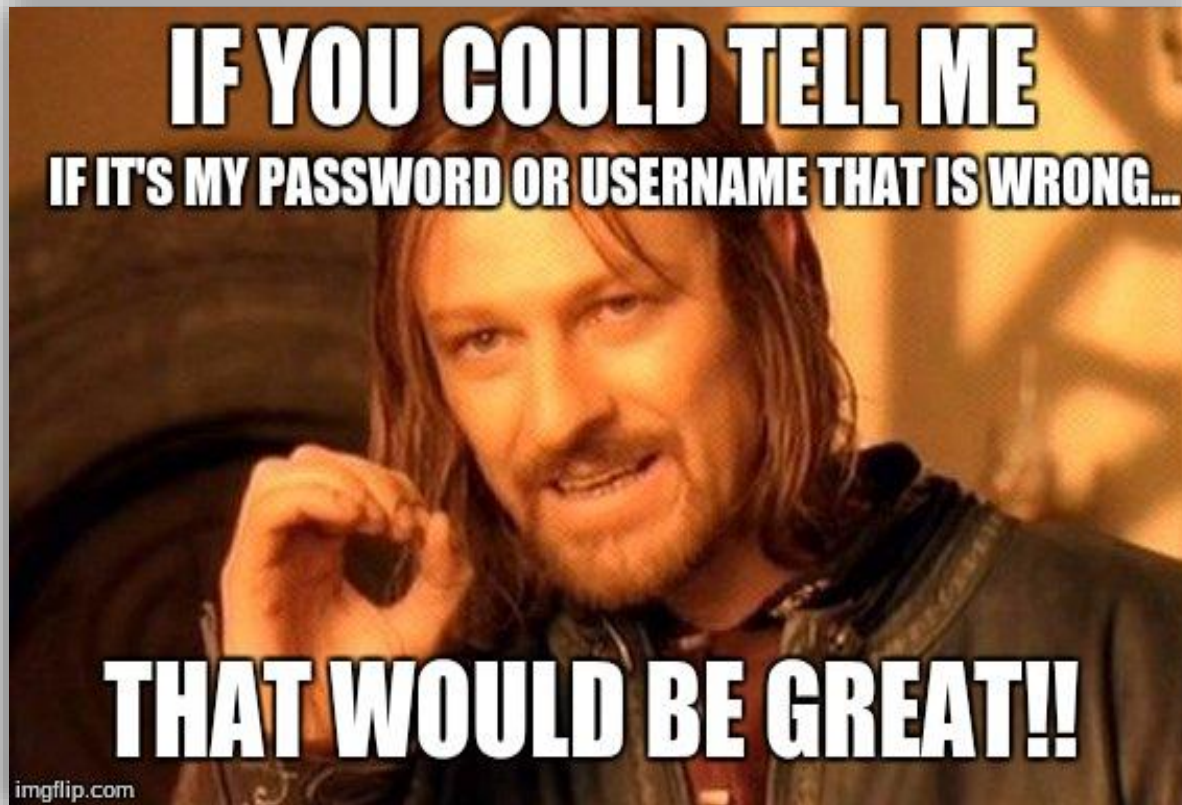
Acces bază de date



Parolă

- Formă tipică de obținere a accesului (login)
- Șir de caractere tipăribile





<https://imgflip.com/i/105mbt>

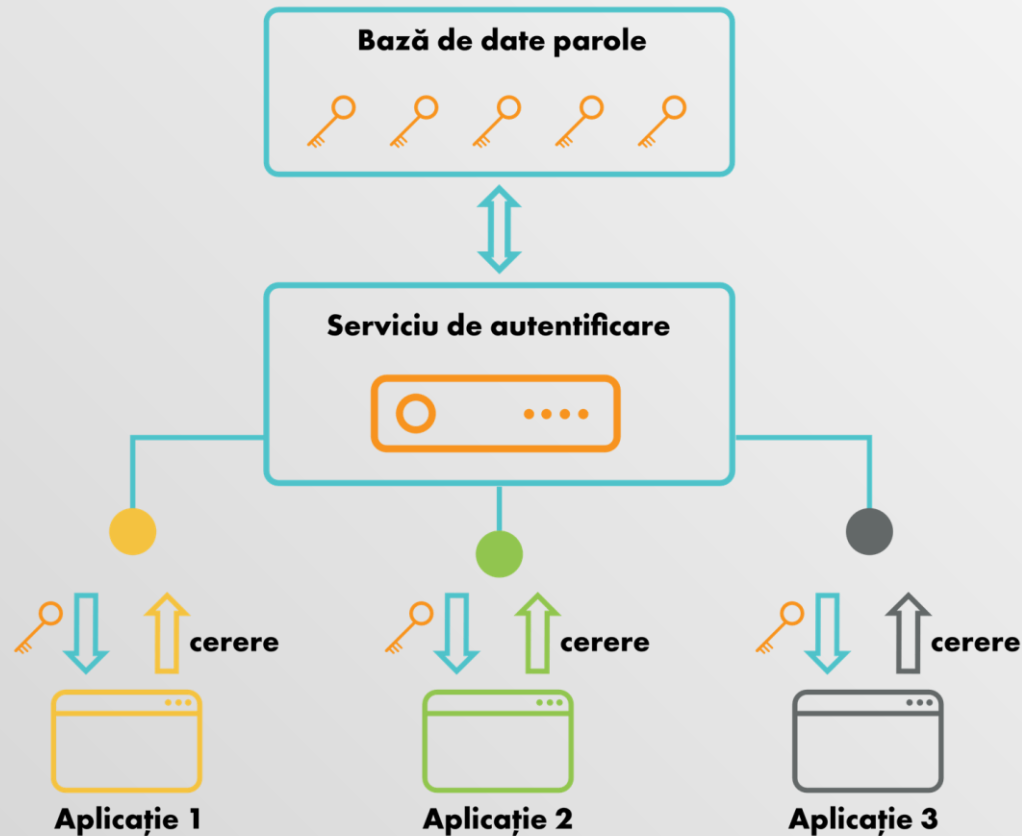
Parolă sigură

- fără cuvinte comune (din dicționar)
- fără date de naștere
- dacă o notați, aveți grijă unde
- înlocuire periodică
- caractere, speciale, numere, majuscule
- fiecare cont cu parola lui

Autentificare centralizată

- Este complicat să ai un cont și o parolă diferită pentru fiecare tip de aplicație
- Autentificare centralizată
 - Serviciu care gestionează baza de date de parole
 - Nume de utilizator și parolă unică pentru toate aplicațiile
 - **Windows:** serviciul AD – Active Directory
 - **Linux:** serviciul LDAP – Lightweight Directory Access Protocol

Autentificare centralizată



Autentificare multi-factor

- Autentificare prin...
 - **Ceva ce știi:** parolă
 - **Ceva ce ai:** token, device, mobil
 - **Ceva ce ești:** biometric



Gestiunea utilizatorilor

Privilegiat

- Access complet la resursele sistemului
- Poate schimba parolele altor utilizatori
- Nu poate afla parolele inițiale
- Accesul trebuie securizat

Neprivilegiat

- Acces complet la un director tip Home
- Acces de execuție sau read-only la alte părți ale sistemului de fișiere
- Poate obține privilegii administrative

Acțiuni

Acțiuni privilegiate:

- gestiunea utilizatorilor (adăugare, ștergere utilizatori)
- gestiunea pachetelor
- configurarea rețelei
- configurarea parametrilor de boot
- configurarea nucleului

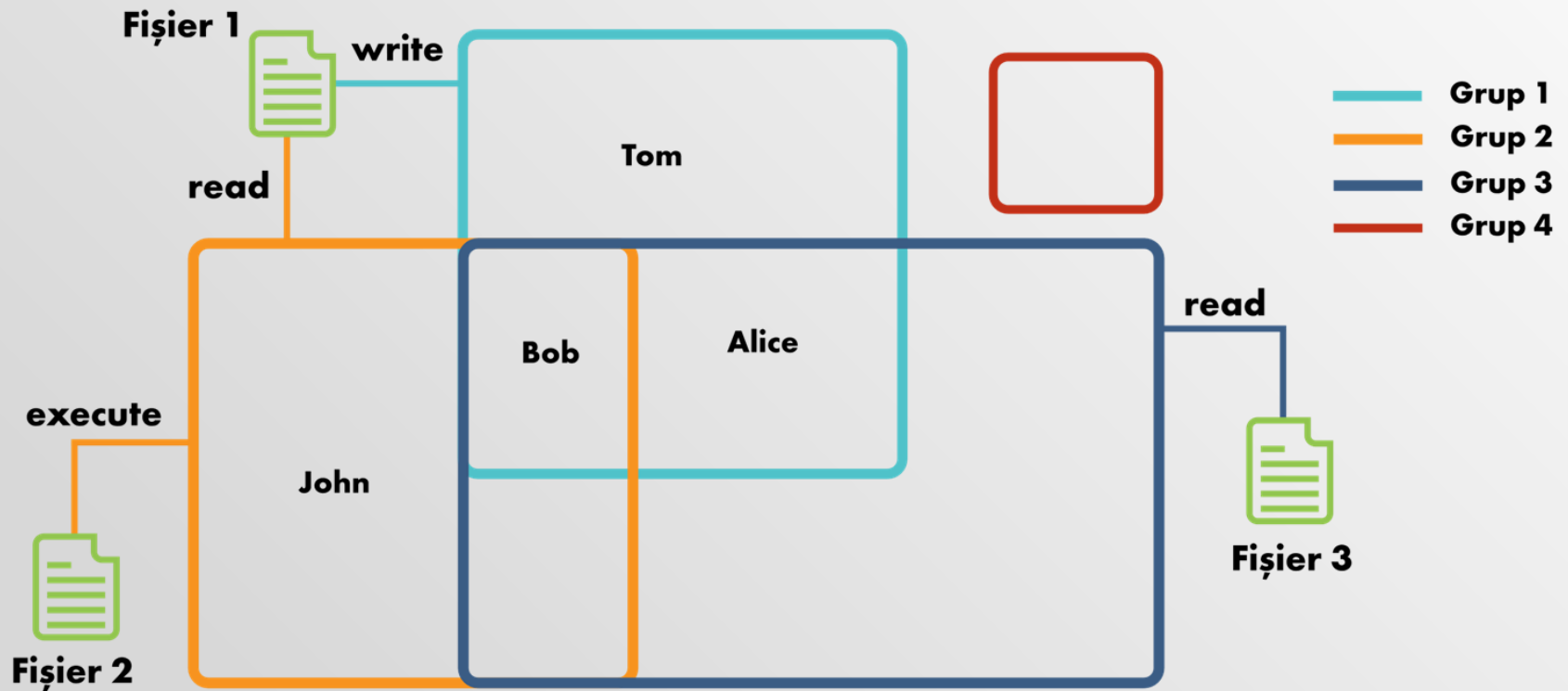
Acțiuni neprivilegiate:

- parcurgerea ierarhiei de fișiere
- rularea de programe
- conexiuni de rețea

Grupuri

- Utilizatorii sunt grupați
 - Un utilizator face parte dintr-unul sau mai multe grupuri
 - Un grup poate conține 0 sau mai mulți utilizatori
- Grupul definește accesul la resurse
- Atributele grupului sunt definite în fișiere de configurare sau baze de date
 - Vizibile pentru orice utilizator
 - Modificabile de utilizatori privilegiați

Asociere utilizatori-grupuri



Utilizator privilegiat

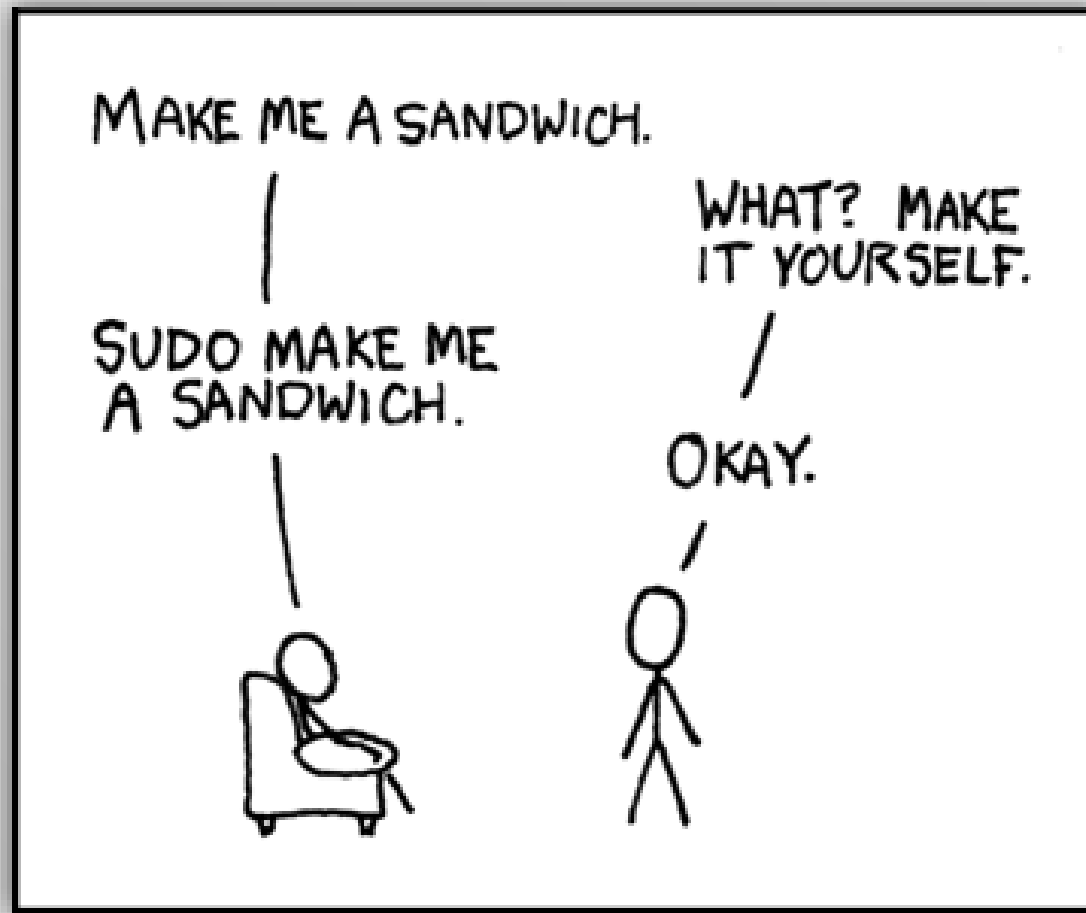
- Unix: utilizatorul root
 - prompt-ul începe cu #
 - su sau sudo
- Windows:
 - Utilizatorul *Administrator*
 - Grupul *Administrators*



SU

- Schimbarea utilizatorului
 - Implicit / fără parametru: în root
 - Cu parametru: în utilizatorul indicat
- Se cere parola noului utilizator
- Permite rularea unei comenzi fără a deschide un shell prin -c

sudo



sudo

- substitute user do
- rularea unor comenzi cu drepturile altui utilizator
- de obicei se rulează cu drepturi de root
- este solicitată parola utilizatorului **care rulează comanda**
- prin configurarea /etc/sudoers un utilizator poate rula comenzi ca root
- *cine are permisiuni de root?*

sudo

- configurat în /etc/sudoers
- putem configura granular privilegii: un utilizator poate rula privilegiat doar anumite comenzi

```
$ sudo apt-get install package-name  
                                # install package-name  
$ sudo su                      # open root  
shell  
$ sudo bash                    # open root shell
```

Operații cu utilizatori

Neprivilegiat

- Verificare informații
- `/etc/passwd`,
`/etc/group`
- Comenzi (`id`, `who`,
`whoami`, `users`,
`finger`, `pinky`,
`last`)

Privilegiat

- Adăugare/ ștergere
utilizatori (`adduser`,
`deluser`)
- Schimbare parolă
utilizatori (`passwd`)
- Oferire/revocare
privilegii

Gestiunea utilizatorilor

Utilizatori

- Crearea unui utilizator
- Ștergerea unui utilizator
- Schimbarea parolei
- Modificarea atributelor unui utilizator
 - Username, login shell, director

Grupuri

- Crearea unui grup
- Ștergerea unui grup
- Adăugarea / ștergerea unui utilizator din grup

Informații

Fișier	Rol	Informații
<code>/etc/passwd</code>	informații utilizatori	nume de utilizator, UID, director home, shell de login, GID
<code>/etc/shadow</code>	parole utilizatori	nume de utilizator, parolă criptată, informații expirare parolă
<code>/etc/group</code>	informații grupuri	nume grup, GID, utilizatori aferenți

Utilitare

Utilitar	Rol	Fișiere investigate
id	informații despre utilizator	/etc/passwd, /etc/group
groups	grupurile utilizatorului curent	/etc/group
users, w, who	utilizatorii autentificați în sistem acum	/var/run/utmp
whoami	numele utilizatorului curent	N/A
finger, pinky	informații complete despre un utilizator	/etc/passwd, /etc/group

Operații

Operație	Utilitare	Fișiere modificate
adăugare utilizator	useradd	/etc/passwd, /etc/shadow, /etc/group
ștergere utilizator	userdel	/etc/passwd, /etc/shadow, /etc/group
modificare utilizator	usermod	/etc/passwd, /etc/shadow, /etc/group
adăugare grup	groupadd	/etc/group
ștergere grup	groupdel	/etc/group
modificare grup	groupmod	/etc/group
modificare shell	chsh	/etc/passwd
modificare informații utilizator	chfn	/etc/passwd
schimbare parolă	passwd	/etc/shadow

Gestiunea parolelor

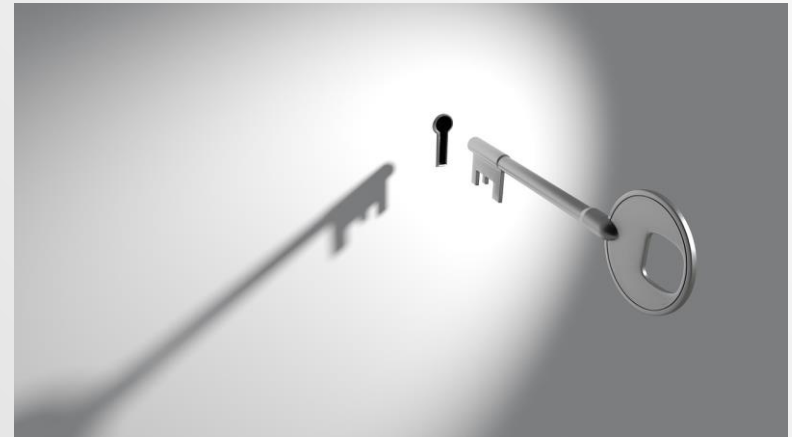
- Utilizator neprivilegiat: gestionarea proprie parole
- Utilizator privilegiat: gestionarea parolelor tuturor utilizatorilor
- Acțiuni
 - Schimbarea parolei
 - Stabilirea duratei de viață
 - Blocarea parolei

Permisiuni

- Drepturi de acces
- Definesc acțiunile posibile pentru utilizator
- Drepturi generice:
 - Citire: un fișier / o zonă de memorie poate fi vizualizat(ă)
 - Scriere: un fișier poate fi editat / se poate scrie în memorie
- Un utilizator poate configura drepturile pentru fișierele din proprietatea sa

Attribute

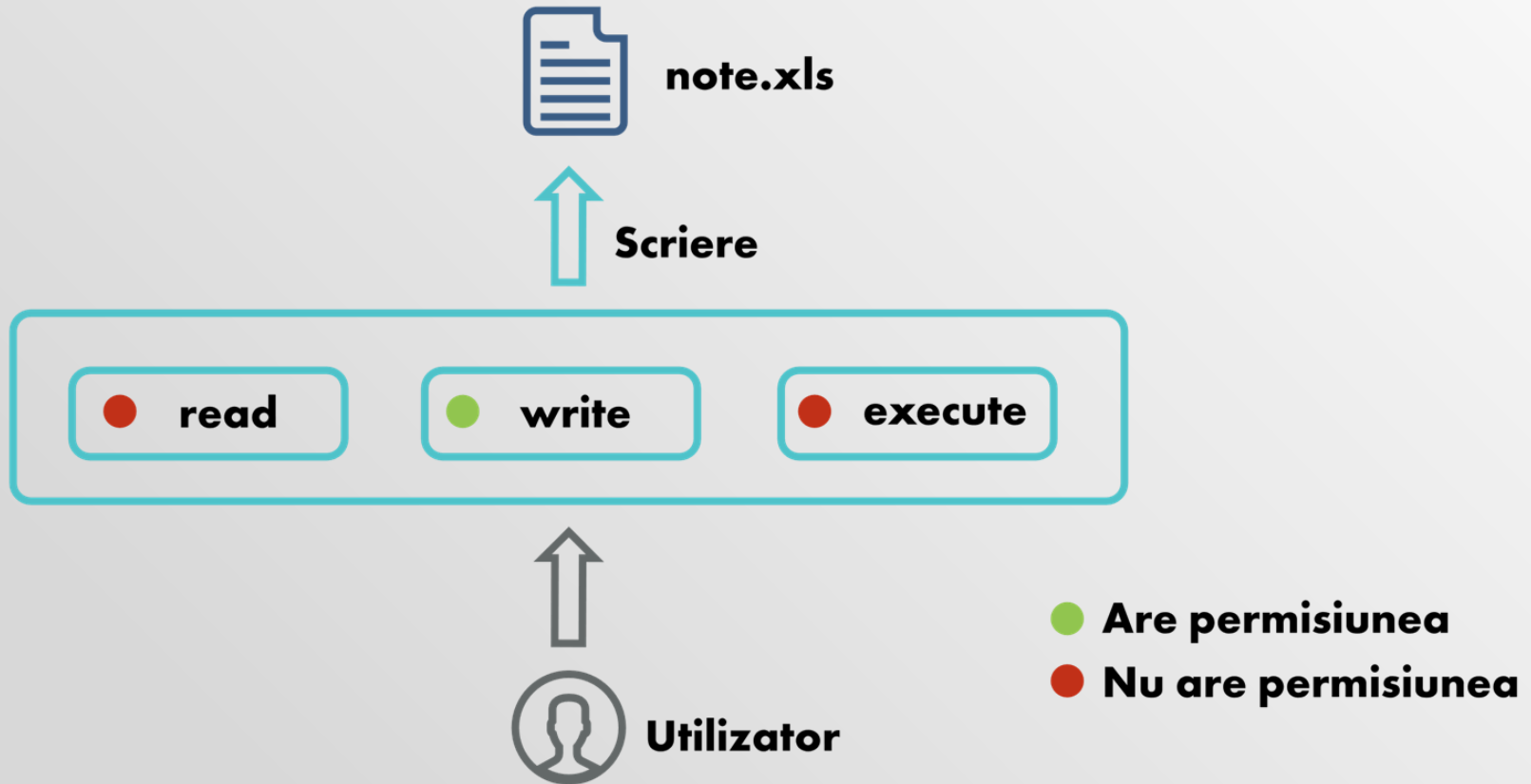
- Fiecare utilizator are
 - permisiuni complete pentru directorul **Home**
 - permisiuni specifice pentru o anumită resursă
- Informațiile despre permisiuni sunt reținute în **attributele** fiecărui fișier
 - attribute = metadata



Entități și permisiuni

- 3 tipuri de entități
 - Utilizator (user)
 - Grup (Group)
 - Ceilalți (Others)
- 3 tipuri de permisiuni
 - Citire (Read)
 - Scriere (Write)
 - Execuție (Execute)

Utilizatori și fișiere



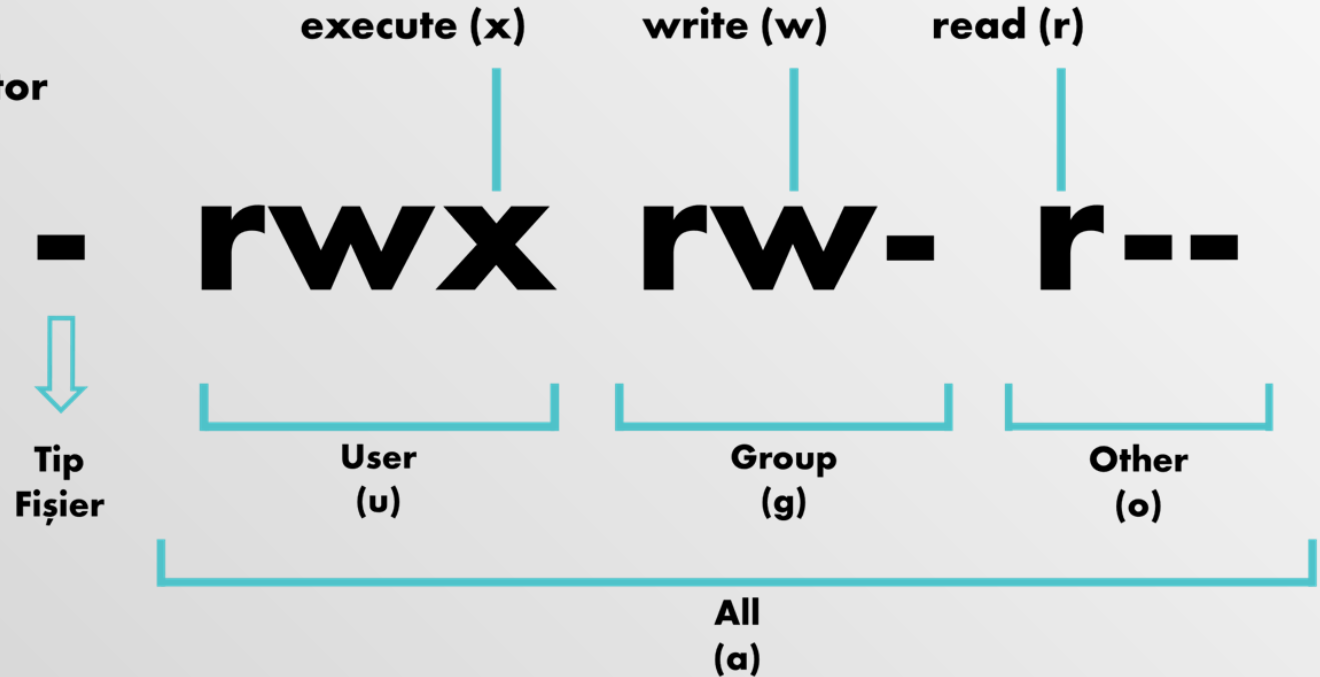
Permisuni în Linux

- Permisunile = șir de 9 caractere
 - 3 pentru utilizator
 - 3 pentru grup
 - 3 pentru ceilalți

Permisiuni în Linux

Tip fișier:

■ ➡ fișier
d ➡ director
l ➡ link



Format permisiuni

- Pe biți:
 - r w - r- - r - - corespunde 110100100
 - r w x r- x - - - corespunde 111101000
 - r w - rw- - - - corespunde 110110000

- Octal:
 - r w - r- - r - - corespunde 644
 - r w x r- x - - - corespunde 750
 - r w - rw- - - - corespunde 660

Gestiunea permisiunilor

- **Linux:** Fiecare fișier are metadate
 - Metadate: User, Group, Permisuni
 - Entități: User, Group, Others
 - Tipuri: Read, Write, Execute
- **Windows:** Liste de acces
 - ACL: access control lists
 - Permisuni prezente doar pe NTFS, nu și pe FAT32

Comenzi

- Afişare:
 - `ls -l`
 - `stat`
- Modificare:
 - `chown`: modifică utilizatorul și grupul
 - `chgrp`: modifică grupul
 - `chmod`: modifică permisiunile

Permisiuni de creare

- touch și mkdir creează fișiere / directoare cu metadata implicite
 - Definite în masca de creare a shell-ului
 - Fișiere: ȘI logic între 666 (octal) și masca inversată
 - Directoare: ȘI logic între 777 (octal) și masca inversată

Mască de creare	Mască inversată	Permisiuni de creare fișier	Permisiuni de creare director
022	755	644	755
002	775	664	775
077	700	600	700

umask

- Afișarea și modificarea măștii shell-ului
 - Fără parametru: afișează masca de creare
 - Cu parametru: modifică masca de creare

Operații privilegiate













Operații neprivilegiate:

- pwd
- cd
- ls
- cat
- touch, mkdir, ln
- rm, rmdir
- cp, mv
- tar, gzip
- chmod

Operații privilegiate:

- fdisk
- mkfs
- mount
- umount
- chown

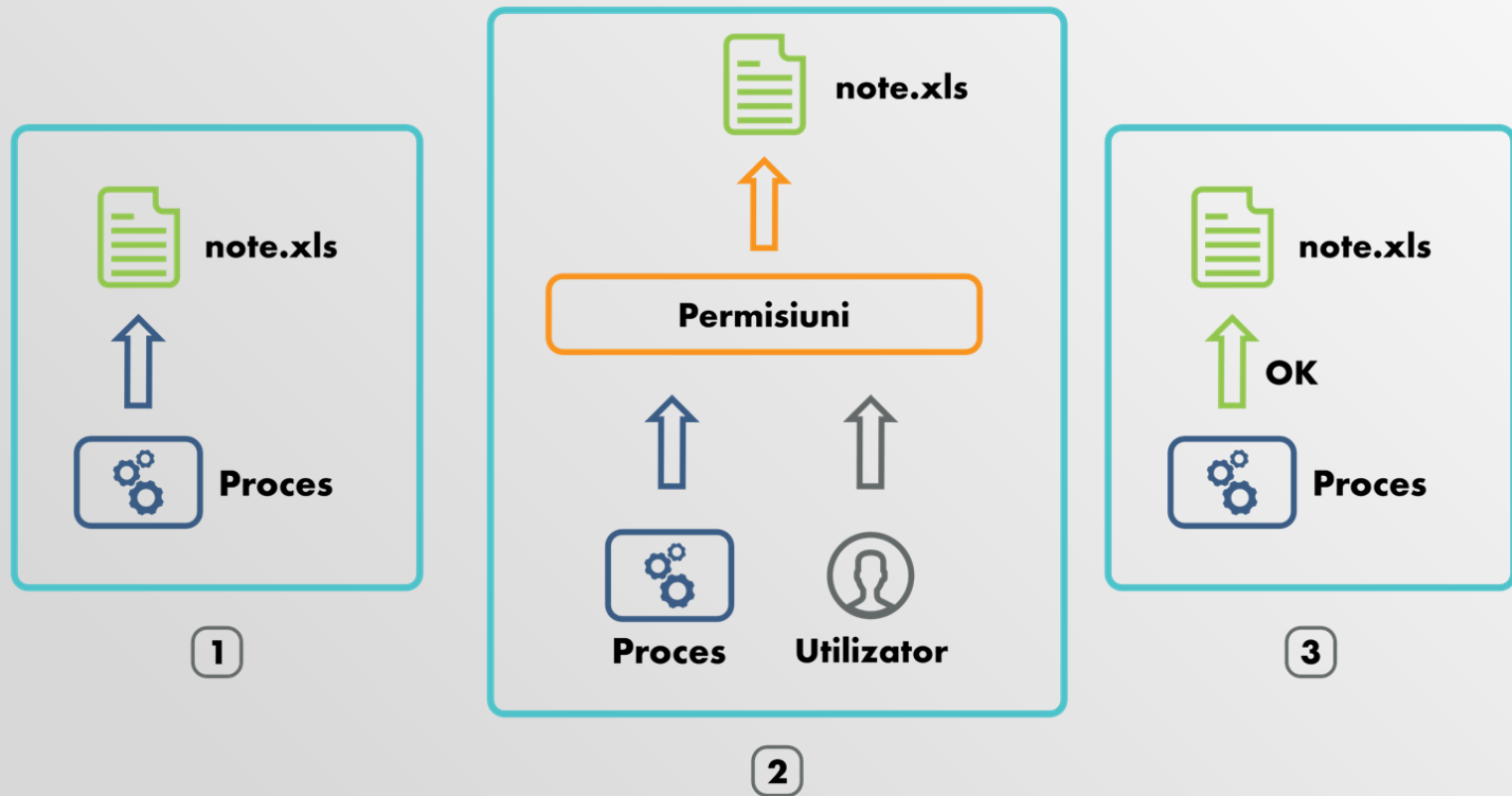
Liste de acces Windows

File Access Control List	
Utilizator / Grup	Permisiuni
 Bob	<div> read</div> <div> write</div> <div> execute</div>
 Grup 1	<div> read</div> <div> write</div> <div> execute</div>
 Alice	<div> read</div> <div> write</div> <div> execute</div>
...	...

 Are permisiunea

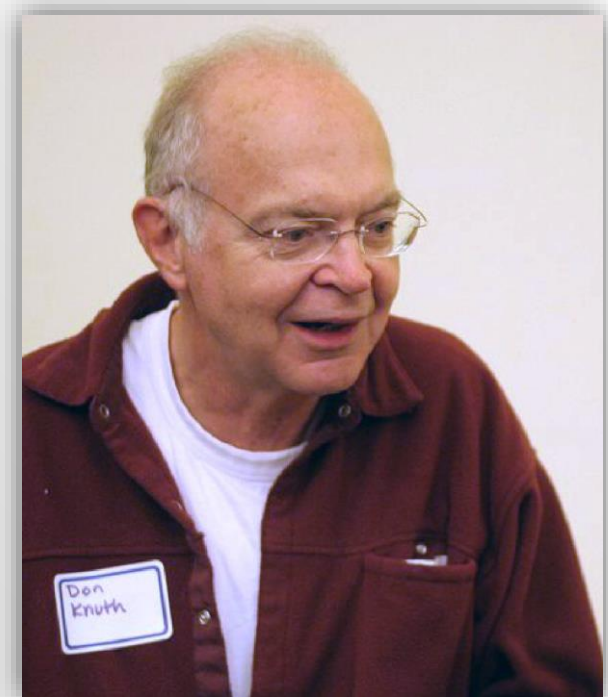
 Nu are permisiunea

Verificarea permisiunilor



Donald Knuth

- *The Art of Computer Programming*
- analiza algoritmulor
- autorul TEX, METAFONT
- umor profesional



Cuvinte cheie

- Permisuni
- Acces Informații
- Root
- Parole
- Privilegii
- Activități
- Operații
- Autentificare

Resurse utile

- Silberschatz, Galvin, Gagne - Operating System Concepts, 7th Edition (chapter 3: Processes)
- Tanenbaum - Modern Operating Systems, 2nd Edition (chapter 2: Processes and Threads)
- https://en.wikipedia.org/wiki/Multi-factor_authentication
- http://en.wikipedia.org/wiki/Category:Unix_signals
- <http://computer.howstuffworks.com/operating-system5.htm>