Sécurisation physique du BIOS

Faille

Accès aux options du BIOS comme le choix de la source du boot (disque, disquette, réseau, etc.) ;
Possibilité à une personne physique de couper l'alimentation et de **redémarrer votre ordinateur avec une disquette, et d'accéder ainsi après quelques manipulations au contenu du disque**

Protection

Activer la protection par **mot de passe du BIOS**

En pratique

Se rendre dans les paramètres de configuration de votre BIOS par l'action d'une touche au démarrage, puis configurer. (Suivant la machine : *DEL, SUPPR, INS, F8, ALT+F1... for SETUP*)

/etc/passwd et /etc/shadow

Faille

Un fichier unique pour des informations plus ou moins critiques

`/etc/passwd`, informations sur comptes des utilisateurs (`login:passwd:uid:gid:fullname:/home/dir/:shell`) : **utiles dans plusieurs applications mais accès ouvert au passwd même chiffré**

Protection

Dissociation en deux fichiers : ajout de `/etc/shadow` qui sert uniquement lorsque l'on a besoin d'accéder au passwd

En pratique

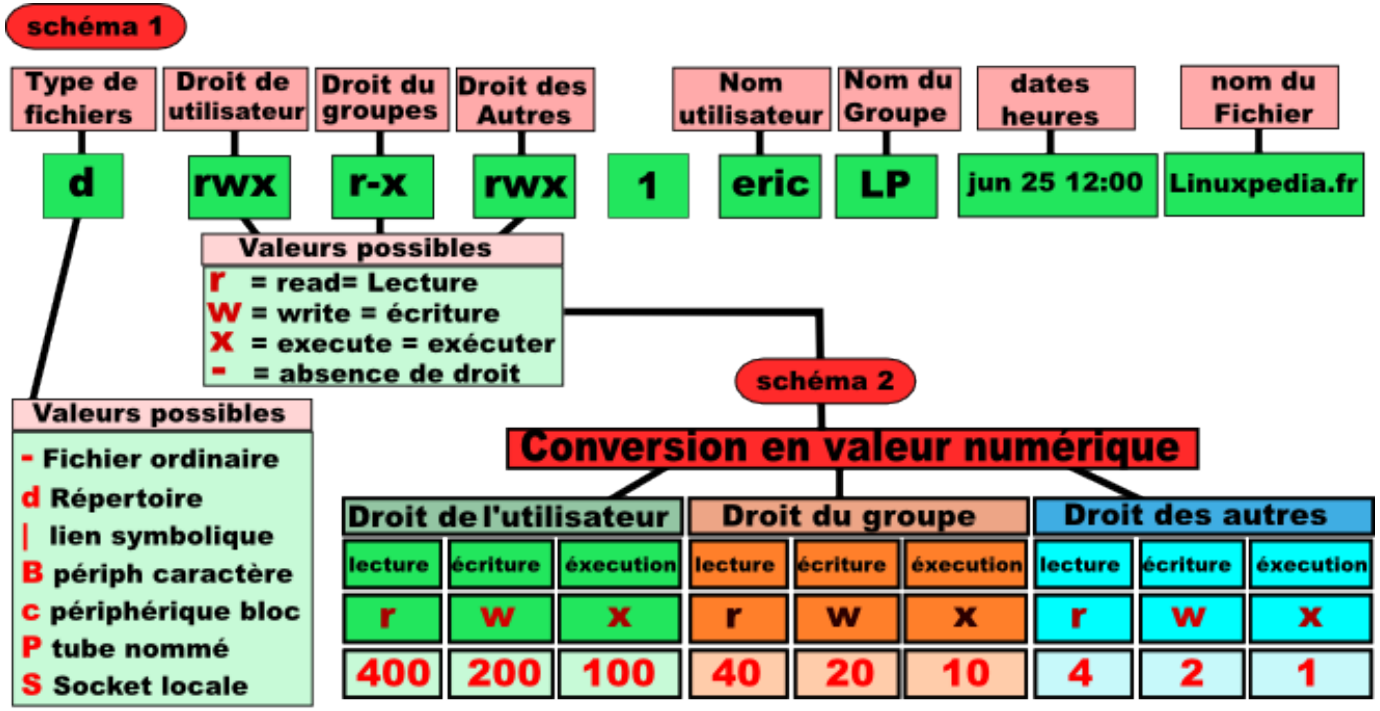
Tester la présence du fichier

```
$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

Le mettre en place en installant le paquet

Les droits et permissions de base

```
$ ls -l
```



www.linuxpedia.fr/doku.php/droits_et_permissions_sous_linux

Droits d'endossement (SetUID et SetGID) et Sticky bit

suid programme exécuté avec droits du propriétaire et non les droits de l'utilisateur

```
-rwsr-xr-x 1 root root 54256 mai   17  2017 /usr/bin/passwd
```

sgid programme exécuté avec droits du groupe et non les droits du groupe de l'utilisateur
ou bien si fichier dans un répertoire avec sgid alors droit du groupe et non du créateur

```
-rwxr-sr-x 1 root tty 27368 juin  14  2017 /usr/bin/wall
-rwxr-sr-x 1 root crontab 36080 avril  5  2016 /usr/bin/crontab
```

stiky bit dans répertoire avec ce droit, seuls les propriétaires des fichiers pourront les effacer

```
drwxrwxrwt  13 root root    20480 févr. 11 22:13 /tmp
```

- Représentés par *s* et *t* si les droits sont positionnés
- Configurables avec 4e octal à gauche : suid=4, sgid=2 et stiky bit=1 e.g. "6755" pour "rwsr-sr-x" avec un suid + un guid

Droits d'endossement (SetUID et SetGID) et Sticky bit

Faille

Attention aux effets de bord ! Par exemple : éditeur avec droits SUID/GUID peut permettre de modifier fichiers de configuration non autorisés pour simple utilisateur
Editeur Emacs permet aussi l'exécution de commandes shell via sa console interne...

Protection

Pour trouver les fichiers possédant les droits d'endossement

```
$ find / -perm -2000 -o -perm -4000 -exec ls -l {} \; 2>/dev/null
-rwsr-xr-x 1 root root 26456 2010-03-12 00:12 /bin/ping6
-rwsr-xr-x 1 root root 31100 2010-01-26 18:09 /bin/su
-rwsr-xr-x 1 root root 72188 2010-03-22 18:51 /bin/mount ...
```

Restreindre leur accès

- Dans `/dev` `chmod 660 /dev/lp`,
- Dans `/bin` `chmod 750 /bin/mount`, `chmod 4750 /bin/su`, ...
- Dans `/sbin` `chmod 750 /sbin/dhcpd`, `chmod 750 /sbin/fdisk`, ...

Suppression des compilateurs

Faille

Un compilateur offre la possibilité à un pirate d'exécuter des scripts potentiellement nuisible

Protection

Désinstaller les compilateurs après installation du système

- pour savoir ce qui est installé

```
dpkg -l | grep  gcc
```

- pour les désinstaller (très radical)

```
dpkg -l | grep -i gcc | xargs dpkg -r
```

- pour limiter les utilisateurs

```
chmod 700 gcc
```