Une (très) bref introduction à GNU/Linux

Ayitic
Port-au-Prince, Haïti.
11 - 16 Août 2014

Lucien Loiseau

Les composantes d'un OS

Composante d'un système

- Matériel : Les composants électronique (CPU, mémoire, carte vidéo, carte Ethernet, etc.)
- Noyau : Il contrôle le fonctionnement du matériel et en fournit une abstraction au logiciel
- Logiciel : fournit à l'utilisateur une interface et des services

Le système GNU/Linux

GNU et Le noyau Linux

- GNU est un projet et un système d'exploitation complet, initié par Richard Stallman, et devait être à la base équipé du noyau Hurd (le noyau Hurd n'a jamais été réellement terminé)
- Linux est un noyau développé par Linus Torvald en 1991 qui est dépuis utilisé avec GNU pour former GNU/Linux

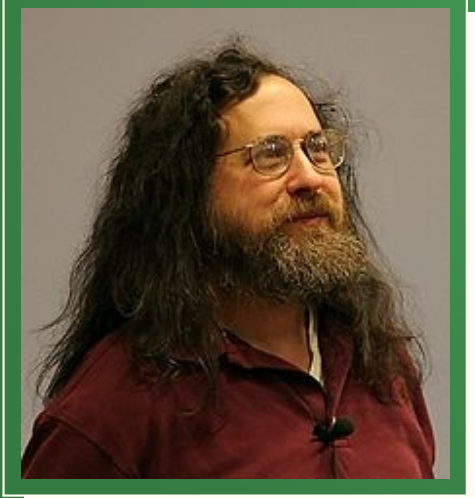


FIGURE: Richard Stallman

FIGURE: GNU/Linux

FIGURE: Richard Stallman

Qu'est ce que le logiciel libre ?

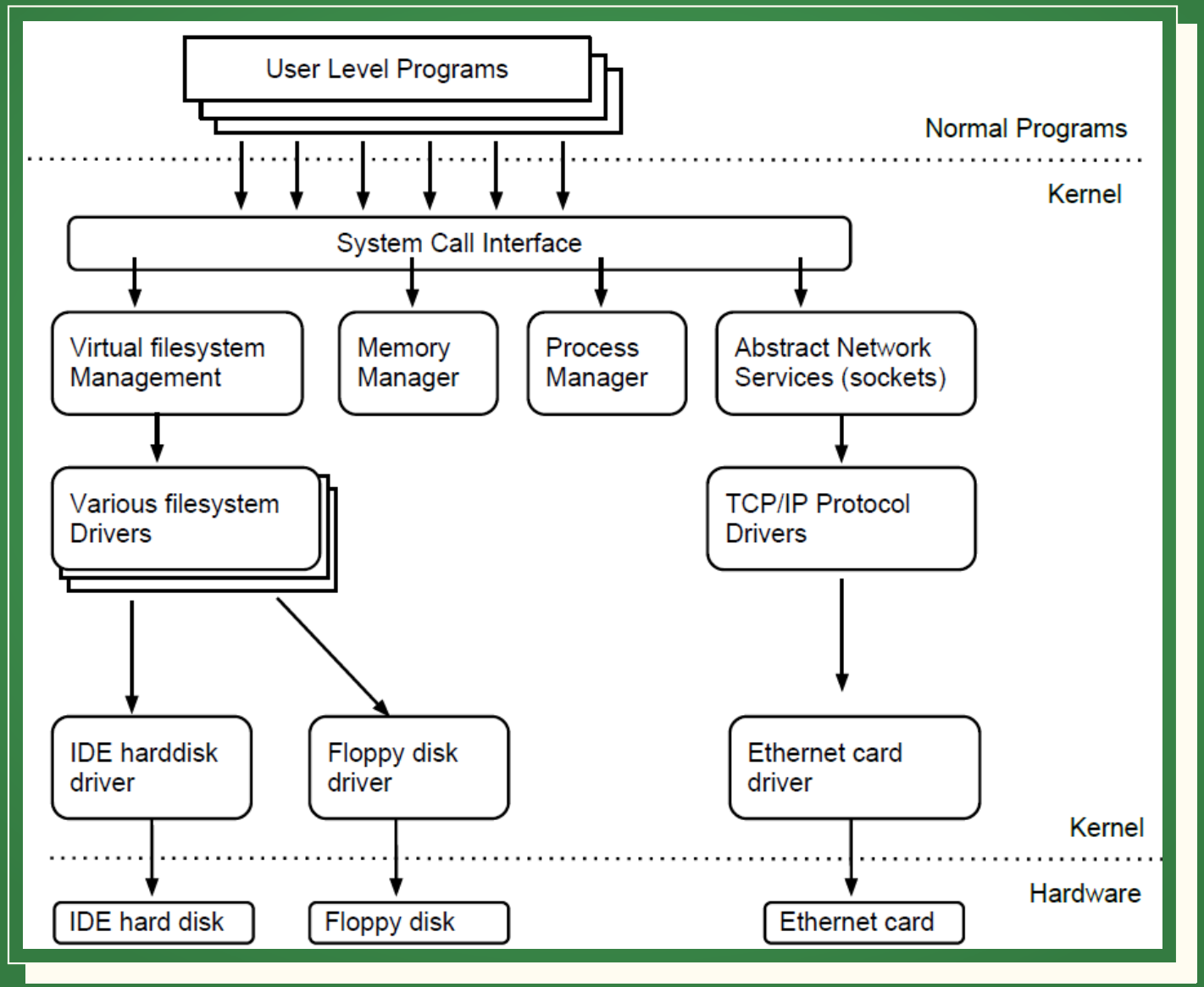
Les 4 libertés d'un logiciel libre

- Liberté d'**exécuter** le programme
- Liberté d'**étudier** le fonctionnement du programme (à travers le code source)
- Liberté de **redistribuer** des copies
- Liberté d'**améliorer** le programme et de distribuer ces amélioration

Considération en terme de sécurité

- le libre accès au code source permet l'examen du logiciel par des experts indépendants
- le libre accès au code source rend impossible le recours à la sécurité par l'obscurité
- la découverte de failles de sécurité est facilitée par la publication du code source
- la liberté d'améliorer le code source (et de les partager) facilite la correction des vulnérabilités

Le Noyau Linux



Sous Linux, tout est fichier

4 types de fichiers

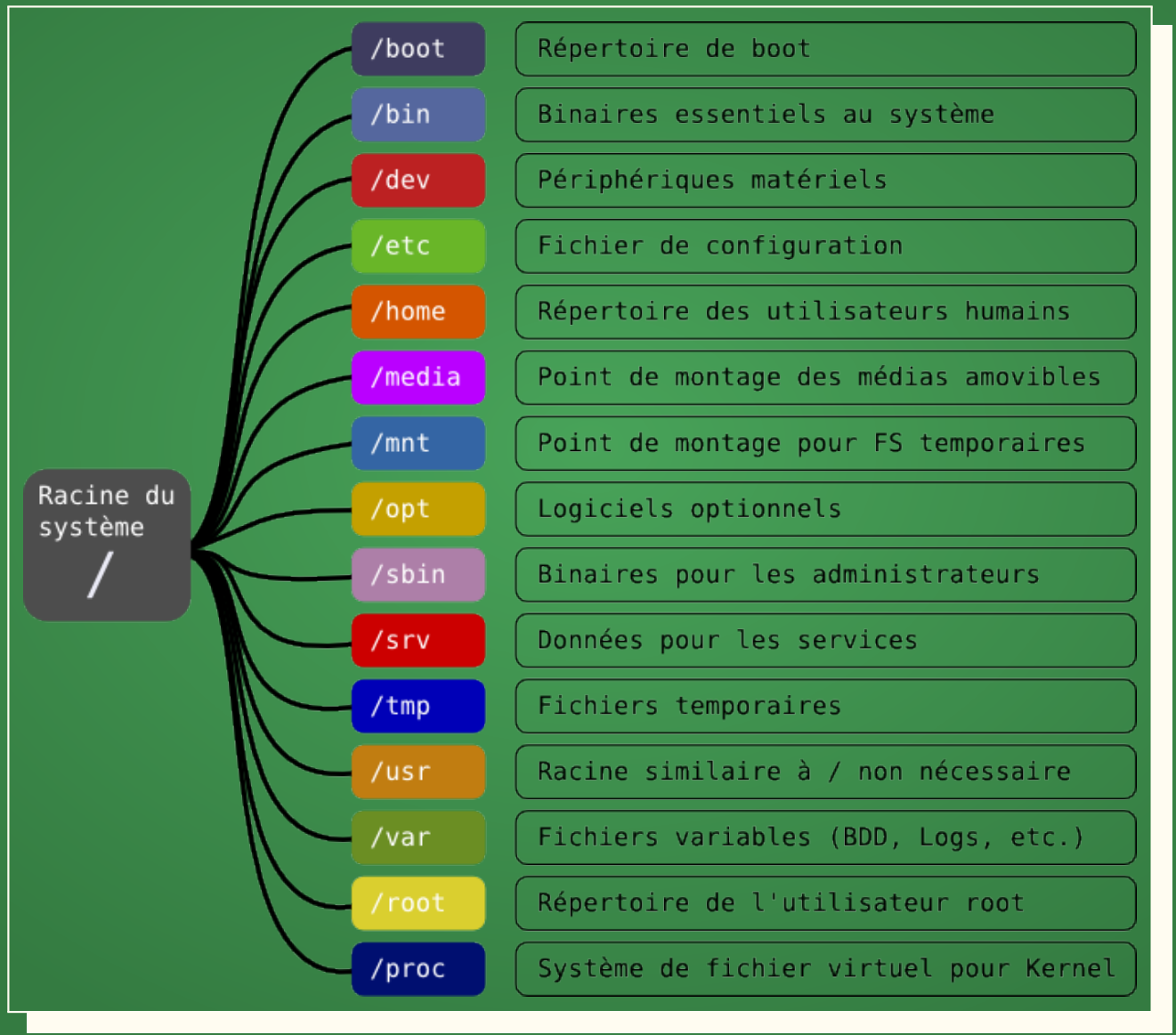
- Les fichiers normaux
- Les liens symboliques
- Les répertoires
- Les fichiers spéciaux (virtuels, sockets, etc.)

vraiment tout est fichier ?

Un fichier signifie qu'on peut "lire" et "écrire" dedans.

- ce qui sort de la carte son ? /dev/dsp
- input/output du disque dur ? /dev/hda
- /dev/null ? supprime tout ce qui y est écrit (trou noir)

L'arborescence Filesystem Hierarchy Standard (FHS)



Utilisateurs : Exercice

Exécuter la commande `pwd`

- dans quel répertoire vous trouvez vous ?
- déplacez vous à la racine avec `cd /` et tapez `ls`

Utilisateurs : Exercice

Exécuter la commande `pwd`

- dans quel répertoire vous trouvez vous ?
- déplacez vous à la racine avec `cd /` et tapez `ls`

```
[lucien@archlinux:~] [ven. juil. 18 01:13:39]
% pwd
/home/lucien
[lucien@archlinux:~] [ven. juil. 18 01:13:40]
% cd /
[lucien@archlinux:/] [ven. juil. 18 01:13:42]
% ls
bin  boot  dev  etc  home  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
```

FIGURE: Je me trouve dans mon répertoire utilisateur

Utilisateurs et Administrateurs

Les utilisateurs

- GNU/Linux est un système multi-utilisateur, ceux ci sont listés dans le fichier **/etc/passwd**
- Chaque ligne contient les informations suivantes :

user	passwd	UID	GID	nom complet	home	shell

- il n'y a pas de différence entre un utilisateur humain et un utilisateur système

```
[lucien@archlinux:~] [mer. juil. 16 19:14:49]
% cat /etc/passwd
root:x:0:0:root:/root:/bin/zsh
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
mail:x:8:12:mail:/var/spool/mail:/bin/false
ftp:x:14:11:ftp:/srv/ftp:/bin/false
http:x:33:33:http:/srv/http:/bin/false
uuidd:x:68:68:uuidd:/:/sbin/nologin
dbus:x:81:81:dbus:/:/sbin/nologin
nobody:x:99:99:nobody:/:/bin/false
polkitd:x:102:102:Policy Kit Daemon:/:/bin/false
usbmux:x:140:140:usbmux user:/:/sbin/nologin
avahi:x:84:84:avahi:/:/bin/false
lucien:x:1000:1000::/home/lucien:/bin/zsh
```

Utilisateurs : Exercice

Exécuter `whoami` dans un terminal

- qui est l'utilisateur courant ?
- quel est son User ID, Group ID et son répertoire home ?

Utilisateurs : Exercice

Exécuter `whoami` dans un terminal

- qui est l'utilisateur courant ?
- quel est son User ID, Group ID et son répertoire home ?

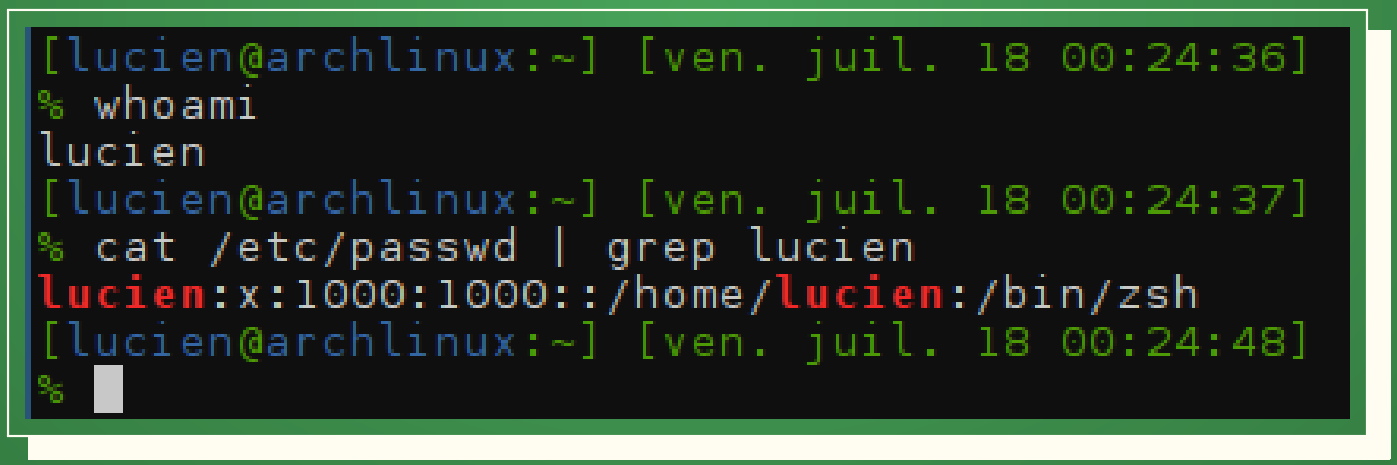


FIGURE: mon utilisateur courant est `lucien`, mon UID et GID est 1000

Permissions : Exercice Introductif

Essayez maintenant `cat /etc/shadow` dans un terminal

- Pouvez vous l'ouvrir ?
- Qui est le propriétaire de ce fichier ?

Permissions : Exercice Introductif

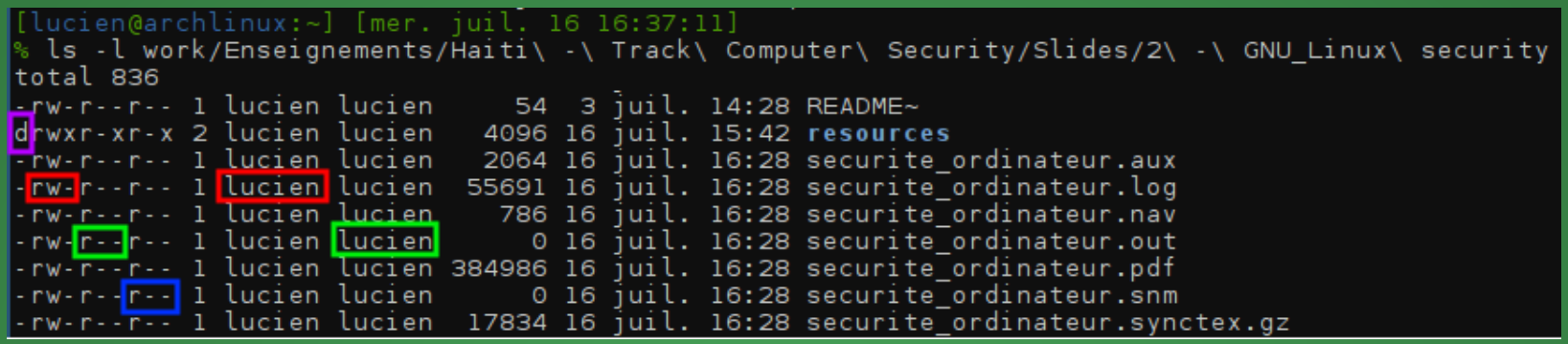
Essayez maintenant `cat /etc/shadow` dans un terminal

- Pouvez vous l'ouvrir ?
- Qui est le propriétaire de ce fichier ?

```
[lucien@archlinux:~] [mer. juil. 16 16:37:32]
% ls -l /etc/shadow
-rw------- 1 root root 950  8 juil. 15:24 /etc/shadow
```

FIGURE: Le fichier shadow appartient à **root** et n'est pas accessible en lecture par les autres utilisateurs

Permissions des fichiers : Read, Write, Execute



User, Group, Other

- User : permissions du propriétaire sur ce fichier
- Group : permissions du groupe sur ce fichier
- Other : permissions des autres utilisateurs sur ce fichier

	Fichiers	Répertoire
Read :	Lire	Lister les fichiers
Write :	Modifier/Supprimer	Ajouter/Enlever
eXecute :	Exécuter	Entrer dedans

Permissions des fichiers : SUID, SGID, Sticky

SetUID ? ! SetGID ? ! StickyBit ? !

- SetUID : un fichier executé avec set UID aura les privilèges du propriétaires !

```
[lucien@archlinux:~] [ven. juil. 18 00:07:40]
% ls -l $(which passwd)
-rwsr-xr-x 1 root root 47200 10 mai   15:23 /usr/bin/passwd
```

- Sticky Bit : interdit de supprimer un fichier d'un autre utilisateur

```
[lucien@archlinux:~] [ven. juil. 18 00:05:43]
% ls -l / | grep tmp
drwxrwxrwt  15 root root   440 17 juil. 21:30 tmp
```

Gare au bit SetUID !

Les programmes avec le bit SetUID sont une surface d'attaque très fréquente pour l'élévation de privilèges !

Permissions des fichiers

Les commandes

- `chown`: permet de changer le propriétaire et/ou le groupe d'un fichier
  - `chown lucien:lucien slides.pdf`
- `chmod`: permet de changer les permissions d'un fichier

– `chmod o-rw slides.pdf`	{user, group, other}	{-, +}	{read, write, xecute}
– `chmod 750 slides.pdf`	read (4)	write (2)	execute (1)
– `chmod 4750 slides.pdf`	SetUID (4)	SetGID (2)	sticky bit (1)

Permissions des fichiers

Les commandes

- `chown`: permet de changer le propriétaire et/ou le groupe d'un fichier
  - `chown lucien:lucien slides.pdf`
- `chmod`: permet de changer les permissions d'un fichier

– `chmod o-rw slides.pdf`	{user, group, other}	{-, +}	{read, write, xecute}
– `chmod 750 slides.pdf`	read (4)	write (2)	execute (1)
– `chmod 4750 slides.pdf`	SetUID (4)	SetGID (2)	sticky bit (1)

Essayez de changer les permissions de `/etc/shadow`

- Est-ce que cela a fonctionné ?

Processus

Les processus

- À chaque processus est associé un Processus ID (PID) et deux paires de (User ID (UID) , Group ID (GID))
- Pourquoi deux paires ?
  - Real (UID,GID) : Les IDs de l'utilisateur réel (celui qui a appelé le processus)
  - Effective (UID,GID) : Les IDs effectifs (détermine ce que le processus peut faire)

Processus

Exemple avec le programme passwd

- pour pouvoir modifier le fichier /etc/passwd, son effective UID est root
- mais comment le programme passwd sait que c'est lucien qui veut changer son mot de passe ?

Processus

Exemple avec le programme passwd

- pour pouvoir modifier le fichier /etc/passwd, son effective UID est root
- mais comment le programme passwd sait que c'est lucien qui veut changer son mot de passe ?

```
[lucien@archlinux:~] [ven. juil. 18 17:25:56]
% ltrace passwd 2>&1 | grep uid
getuid()                                                = 1000
getuid()                                                = 1000
getpwuid_r(1000, 0xe26030, 0xe26070, 256)               = 0
getuid()                                                = 1000
```

  - `getuid` : permet de récupérer le Real UID (ici 1000 c'est à dire lucien)
  - `getpwuid_r` : permet de lire une entrée du fichier `/etc/passwd`

WARGAME