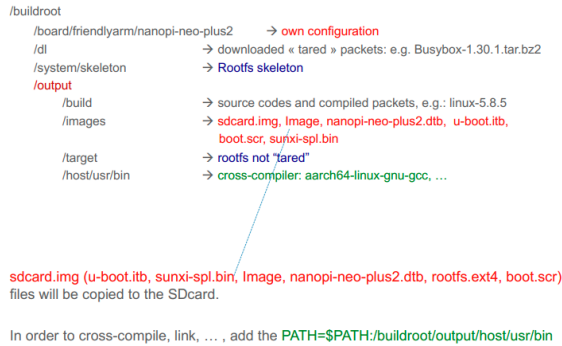


# 1 Buildroot

## 1.1 Principaux répertoires



Ce qui est manquant dans le répertoire dans le dossier output sera recompilé lors de la commande `make` ou en précisant le paquet : `make <package>-rebuild` à refaire.

## 1.2 Principe de fonctionnement

Basé sur des fichiers `make kconfig`, buildroot est un outil qui automatise le processus de construction d'un système Linux embarqué en utilisant la cross-compilation. Lors de la commande `make` il va s'occuper de compiler l'entier du système et préparer une image complète et prête pour l'utilisation.

## 1.3 Configuration pour un hardware donné

Il y a un répertoire situé dans la figure de dessous qui contient plusieurs fichiers intéressants. On y retrouve notamment le fichier `nanopi-neo-plus2/nanopi-neo-plus2.dts` qui contient le FTD ("Flattened Device Tree") qui décrit le hardware. On indique donc à buildroot l'emplacement de ce fichier avec la commande `menuconfig`. Autres fichiers intéressants :

```

● root → /buildroot/board/friendlyarm/nanopi-neo-plus2 (main X) $ ls
boot.cmd          genimage.cfg      nanopi-neo-plus2.dts  rootfs_overlay
busybox-extras.config  linux-extras.config  post-build.sh        ses_linux_defconfig
extlinux.conf      my_patches        readme.txt           uboot-extras.config

```

## 1.4 Patch buildroot

Il faut spécifier le dossier des patches `make menuconfig` nous on a fait dans `/nanopi-neo-plus2/my_patches` et un dossier par package à patcher (il faut aussi éditer `ses_config` pour garder le chemin

des patches). Ensuite la technique consiste à profiter de l'outil `git` et se mettre dans `/buildroot/output/build/uboot-2020.07` et de faire :

```

git init --initial-branch=main
git add .
cd common/
git add .
git commit -m "1st commit"

```

Faire ensuite toutes les modifications à faire, les stager et faire la commande qui crée le patch au format voulu par buildroot :

```

git diff --cached --stat -p > /buildroot/board/friendlyarm/nanopi-neo-plus2/my_patches/uboot/0001_stack_protector.patch

```

On peut ensuite supprimer le paquet en question dans `build` et il se téléchargera et patchera automatiquement au prochain `make`.

## 1.5 Configuration de buildroot, u-boot, kernel

Pour buildroot, on utilise `make menuconfig` ça se sauvegarde dans `.config` ou dans `configs/ses_defconfig` (seulement les changements sont dans ce fichier, qui est à la base une copie de `friendlyarm_nanopi_neo_plus2_defconfig` qui se situe au même endroit).

Pour u-boot, on va dans `make menuconfig` catégorie bootloaders et ça va se sauver dans

```

/buildroot/output/build/uboot-xx/configs/nanopi_neo_plus_defconfig

```

Et dans un fragment files qui ne contient que des petites modifications (save old, make new, use diff, add it to this fragment file):

```

/buildroot/board/friendlyarm/nanopi-neo-plus/uboot-extras.config

```

Pour le kernel, `make linux-menuconfig`, ça se sauve dans `/buildroot/output/build/linux-xx/defconfig` et nous on le copie et le met dans `ses_linux_defconfig`

## 1.6 Génération de la carte SD

Pour créer le fichier `sdcard.img`, on utilise le script `genimage.sh` qui va aller aussi utiliser le fichier `nanopi-neo-plus2/genimage.cfg` qui spécifie les différentes partitions à créer et les images (venant de `output/images`) à mettre dedans.

## 1.7 Génération du rootfs

Il est copié depuis `/buildroot/system/skeleton` pour le mettre dans `/buildroot/output/target`. Il est ensuite possible d'ajouter des fichiers et des répertoires avec le `/nanopi-neo-plus2/rootfs_overlay`. Après la commande `make` le pseudo rootfs est créé et placé dans un des fichiers images de sorties `rootfs.xxx`

## 1.8 rootfs\_overlay

On peut préparer la structure des fichiers de la cible dans ce dossier

## 1.9 Installer un nouveau package dans buildroot

Pour utiliser un package, il faut faire `make menuconfig` et aller choisir le package à aller utiliser. Sinon il faut ajouter le nouveau package "foo" dans le dossier `/buildroot/package`. Il doit contenir au moins :

- `Config.in`: in `kconfig` language : on pourra y accéder à travers `make menuconfig`
- `foo.mk`: fichier qui décrit ou prendre les sources et comment les installer
- `optional foo.hash`: pour vérifier l'intégrité des fichiers à télécharger
- `optional Sxx_foo`: le startup script pour le package foo

# 2 Uboot

## 2.1 Démarrage du NanoPi

1. Lorsque le uP est mis sous tension, le code stocké dans BROM va charger dans ses 32KiB de SRAM interne le firmware "sunxi-spl" stocké dans le secteur n°16 de la carte SD/eMMC et l'exécuter
2. Le firmware "sunxi-spl" (Secondary Program Loader) initialise les couches basses du uP, puis charge l'U-Boot dans la RAM du uP avant de le lancer
3. L'U-Boot va effectuer les initialisations hardware nécessaires (horloges, contrôleurs, ...) avant de charger l'image non compressée du noyau Linux dans la RAM, le fichier Image, ainsi que le fichier de configuration FDT (flattened device tree).
4. L'U-Boot lancera le noyau Linux en lui passant les arguments de boot (bootargs).
5. Le noyau Linux procédera à son initialisation sur la base des bootargs et des éléments de configuration contenus dans le fichier FDT (`sun50i-nanopi-neo-plus2.dtb`).

6. Le noyau Linux attachera les systèmes de fichiers (rootfs, tmpfs, usrfs, ...) et poursuivra son exécution

## 2.2 Principales commandes de Uboot durant le boot

Pour entrer en uboot mode, il faut appuyer sur une touche durant le boot et on arrive dans le prompt u-boot. Ensuite on peut taper help pour avoir une liste des commandes. Les commandes principales sont

- booti - boot Linux kernel 'Image' format from memory
- ext2load - load binary file from a Ext2 filesystem
- ext2ls - list files in a directory (default /)
- ext4load - load binary file from a Ext4 filesystem
- ext4ls - list files in a directory (default /)
- ext4size - determine a file's size
- fatinfo - print information about filesystem
- fatload - load binary file from a dos filesystem
- fatls - list files in a directory (default /)
- fatmkdir - create a directory
- fatrm - delete a file
- fatsize - determine a file's size
- fatwrite - write file into a dos filesystem
- mmcinfo - display MMC info
- printenv - print environment variables
- setenv - set environment variables

Le fichier boot.cmd (transformé en boot.scr par une commande montrée plus bas) contient les commandes que u-boot effectue :

```
setenv bootargs console=ttyS0,115200
earlyprintk root=/dev/mmcblk2p2 rootwait
ext4load mmc 0 $kernel_addr_r Image
ext4load mmc 0 $fdt_addr_r nanopi-neo-plus2.dtb
booti $kernel_addr_r - $fdt_addr_r
```

La commande booti \$kernel\_addr\_r - \$fdt\_addr\_r spécifie l'adresse de l'image, de du fdt et le - précise qu'il n'y a pas de initrd. Voir plus tard avec initramfs où on fera autrement  
Création d'un fichier boot.scr à partir d'un boot.cmd

```
mkimage -C none -A arm64 -T script -d board/
friendlyarm/nanopi-neo-plus2/boot.cmd
output/images/boot.scr
```

## 2.3 Configuration de uboot

make uboot-menuconfig pour configurer (cette config se sauve dans output ubuild uboot-2020.07 .config), make uboot-rebuild ou rm output/build/uboot-xx/.stamp-built et make pour compiler. Après le make 2 fichiers sont créés: u-boot.itb et boot.scr et se trouvent dans output/images/

## 2.4 Sécurisation de uboot

2 choses sont à faire :

- Retirer les informations de debug, c'est à dire l'option -g lors de la compilation
- Ajouter l'option -fstack-protector-strong. Qui permet d'éviter les attack en buffer overflow, un programme va donc s'arrêter en cas de détection de stack smashing.

Pour mettre l'option de protection de stack de base dans uboot, il faut faire un patch en éditant le Makefile de uboot de cette manière:

```
KBUILD_CFLAGS += $(call cc-option,-fstack-
protector-strong)
#KBUILD_CFLAGS += $(call cc-option,-fno-stack-
protector)
```

Et ajouter stackprot.o qui contient une fonction \_\_stack\_chk\_fail dans le /common/ et ajouter la ligne obj-y += stackprot.o dans le Makefile du common.

## 2.5 Etapes pour la création de l'image de u-boot.itb

L'image u-boot.itb contient 3 parties:

- u-boot-nodtb.bin qui est le code de uboot qui a été créé à partir du elf de u-boot avec la commande aarch64-linux-objcopy --gap-fill=0xff qui fait attention à ne garder que le strict nécessaire (sans debug, symbol, relocation)
- b131.bin: trust zone ou ARM Trusted Firmware
- sun50i-h5-nanopi-neo-plus2.dtb : Device Tree blob (voir plus bas)

La commande qui fait ça est :

```
mkimage -f u-boot.its -E u-boot.itb (est c'est dans u-boot.its (fichier texte) qu'est spécifié les différentes parties de l'image u-boot.itb
```

## 2.6 Commande strip sur un elf

La commande aarch64-linux-strip u-boot (la commande aarch64-linux-objcopy le fait automatiquement) supprime les informations de symbole et de debug : voici la différence sur le fichier u-boot.elf

Diassemble with symbols			
arm-linux-gnueabi-hf-objdump -d u-boot			
43e00058 <reset>:			
43e00058:	eb0004f8	bl	43e01440 <save_boot_params_default>
43e0005c:	e10f0000	mrs	r0, CPSR
43e00060:	e3c0001f	bic	r0, r0, #31
43e00064:	e38000d3	orr	r0, r0, #211 ; 0xd3
43e00068:	e129f000	msr	CPSR_fc, r0

Diassemble without symbols			
arm-linux-gnueabi-hf-objdump -d u-boot			
43e00058:	eb0004f8	.word	0xeb0004f8
43e0005c:	e10f0000	.word	0xe10f0000
43e00060:	e3c0001f	.word	0xe3c0001f
43e00064:	e38000d3	.word	0xe38000d3
43e00068:	e129f000	.word	0xe129f000

## 2.7 Création de uImage

uImage est l'image Linux au format uboot elle est créée lors du make. Dans le process du boot.cmd, uboot va spécifier son emplacement dans la variable d'environnement \$kernel\_addr\_r=0x40080000

## 2.8 Flattened Device Tree

Le FTD contient les informations sur le hardware que linux va utiliser pour sa configuration. Le fabricant du uP a sûrement écrit sun50i-h5-nanopi-neo-plus2.dts et on le passe en .dtb avec la commande dtc board.dts -o board.dtb. Lors du boot.cmd on précise l'adresse de ce .dtb dans la variable d'environnement \$fdt\_addr\_r=0x4FA00000

## 2.9 Mapping de la SDCard

La carte SD contient ces éléments

- sunxi-spl.bin: Secondary Program Loader
- u-boot.itb: selon plus haut
- boot: image .ext4 qui contient 3 autres choses: Image, nanopi-neo-plus2.dtb et boot.scr
- rootfs: le filesystem de linux

## 2.10 boot.scr

u-boot au démarrage, sans pression d'une touche, va chercher le fichier boot.scr (format boot script) et l'exécuter. Il contient en fait les instructions du fichier boot.cmd.

## 3 Kernel

### 3.1 Principaux répertoire du noyau linux

Les principaux répertoires du kernel sont listés:

- arch Hardware dependent code
- block Generic functions for the block devices
- crypto Cryptographic algo. used in the kernel
- Documentation Documentation about the kernel
- drivers All drivers known by the kernel
- fs All filesystem know by the kernel
- include kernel include files
- init Init code (function start\_kernel)
- ipc Interprocess communication
- kernel Kernel code, scheduler, mutex, ...
- lib different libraries used by the kernel
- mm Memory management
- net Different protocols, IPv4, IPv6, bluetooth, ...
- samples Different examples, kobject, kfifo, ...
- security Encrypted keys, SELinux, ...
- sound Sound support for Linux kernel
- virt Kernel-based virtual machine

### 3.2 Principales méthodes pour sécuriser le noyau

Pour configurer linux : `make linux-menuconfig` ou `make linux-xconfig`. La commande `sysctl` permet de voir les paramètres du kernel

- ne pas inclure le Linux kernel `.config` dans le kernel : Kernel `.config` support
- protéger la stack en activant la détection de buffer overflow : General architecture-dependant options : `[*] Stack Protector buffer overflow detection`, `[*] Strong Stack Protector`
- `randomize_va_space`: avoir des adresse aléatoire pour la stack si 1 avec 2 ça ajoute le heap random. Pour le faire :  

```
echo 2 >
  ↪ /proc/sys/kernel/randomize_va_space
sysctl -w kernel.randomize_va_space=2
```
- `randomize_slab_allocator` (allocation des kernel objects.o):

```
[*] Allow slab caches to be merged
[*] Randomize slab freelist
[*] Harden slab freelist metadata
[*] Page allocator randomization
```

- `randomize address of kernel image`

```
Kernel feature => [*] Randomize the
  ↪ address of the kernel image
```

- `mettre le kernel code read-only`

```
Kernel Feature => [*] Apply r/o
  permissions of VM areas also to their
  ↪ linear aliases
```

- `optimiser le kernel pour la performance (gcc -O2) plutôt que pour la taille (gcc -Os)`

```
General Setup => Compiler optimization
  ↪ level [*] Optimize for performance
```

- `random number generator: si présent sur le hardware`

```
Device drivers => Character Devices =>
  [*] Hardware Random Number Generator
  ↪ Core support
[*] Timer IOMEM HW Random Number
  ↪ Generator support
[*] Broadcom BCM2835/BM63xx Random
  ↪ Number Generator support
```

sinon utiliser le paquet `haveged` (dans `buildroot menuconfig`, `miscellaneous`). Pour voir l'entropy: `cat /proc/sys/kernel/random/entropy-avail`

- `l'emplacement /dev/mem contient des infos sur kernel memory et process memory. Il faudrait éviter l'accès à d'autres utilisateurs que le root:`

```
Kernel Hacking => [*] Filter access to
  ↪ /dev/mem
=> [*] Filter I/O access to /dev/mem
```

- `strip l'assembleur du kernel durant le link pour rendre le reverse du code encore plus dure`

```
Kernel Hacking => Compile time check and
  ↪ compiler options
=> [ ] Compile the kernel with debug info
=> [*] Strip assembler-generated symbols
  ↪ during link
```

- `diminuer l'accès au kernel syslog`

```
Security options => [*] Restrict
  unprivileged access to the kernel
  ↪ syslog
```

- `initialiser tout le stack et le heap avec des zéros`

```
Security options => Kernel Hardening
  ↪ Options => Memory Initialization
=> Initialize Kernel Stack =>no automatic
  ↪ initialization (weakest) (if possible)
[*] Enable heap memory zeroing on
  ↪ allocation by default
[*] Enable heap memory zeroing on free by
  ↪ default
```

- `empêcher la copie depuis/vers la mémoire du kernel qui est douteuse (taille de mémoire plus grand que l'objet)`

```
Security options
=> [*] Harden memory copies between
  ↪ kernel and userspace
[*] Allow usercopy whitelist violations
  ↪ to fallback to object size
[*] Harden common str/mem functions
  ↪ against buffer overflows
```

- `un soft en python, régulièrement mis à jour peut tester la config du kernel : kconfig-hardened-check.py`

### 3.3 Software attacks

#### 3.3.1 Buffer overflow

L'attaque consiste à utiliser un programme qui va aller écrire dans la stack d'un programme, qui est exécutable. On peut par exemple insérer et exécuter un shell code dans une partie exécutable de la stack. Et ensuite on peut faire ce qu'on veut.

#### 3.3.2 ret2libc

On va aller overflow l'adresse de retour d'une fonction avec l'adresse de `system()` qui est une fonction standard C library (libc). Elle permet d'exécuter une commande en shell. On va donc tenter d'appeler le bash: `/bin/sh`

#### 3.3.3 ROP

Return-oriented programming: on va utiliser plein de petits bouts de codes (gadgets) dans toutes les librairies disponibles et on essaie de faire un programme malicieux. ASLR ou le PIE permettent d'éviter ça.

### 3.4 Protections

#### 3.4.1 ASLR

ASLR (Address Space Layout Randomization) `randomize_va_space` randomizes the stack and heap addresses

### 3.4.2 PIE

Le PIE (Position Independent Executable) fait en sorte que l'adresse des codes change.

### 3.4.3 Canary

C'est une valeur qu'on place à la limite d'un buffer. Si elle est écrasée, on peut savoir qu'il y a eu un buffer overflow.

## 4 Valgrind

Valgrind a 5 outils:

- Memcheck: memory error detector (adresse d'une autre stack, variable non-initialisée)
- Cachegrind: cache and branch-prediction profiler (indexation peu optimisée d'un tableau)
- Callgrind: call-graph generator
- Helgrind: thread error detector
- Massif: Heap and stack profiler (allocation sans free) pour voir: `ms_print massif.out.13866`

## 5 Hardening Linux

### 5.1 Contôler l'intégrité d'un package, d'un programme

En premier télécharger le programme foo et sa signature ensuite il faut vérifier l'intégrité avec

```
gpg --verify foo.tar.gz.asc
```

Il nous répond qu'il peut pas en donnant une RSA key: par ex. 23948UT5. Donc il faut importer cette clé publique:

```
gpg --keyserver keyserver.ubuntu.com --search-keys 23948UT5
```

Et relancer la vérification et c'est bon.

### 5.2 Configurer un nouveau package, programme

Détarer le package et afficher les options de compilationss:

```
tar xvzf foo.tar.gz
cd foo
./configure --help
```

Si il n'existe pas encore dans buildroot (donc une version inférieure n'a jamais été installé) on le place dans /buildroot/packages. Et on va faire les choix de versions dans le foo.mk et ensuite on le configure avec `make menuconfig` le choix de config sont décrits dans `Config.in`

### 5.3 Cross-compiler un programme

Ajout de host et prefix

```
./configure --host=aarch64-none-linux-gnu --
prefix=/root/install
make
make install
```

### 5.4 Contrôler les services, les ports ouverts

Les services sont lancés au démarrage si leur Startup scripts se trouve dans le /etc/init.d Le script rcS commence les autres scripts (S01..., S02..., not rcK) dans l'ordre alphabétique. On essaie d'avoir le moins de services possibles. On est obligé de créer un script pour démarrer automatiquement un nouveau service. Si on supprime un S0.... le service ne sera pas débuté au prochain startup. Pour voir les services en cours: `ps -ale`, le tree: `ps -axjf`, leurs privilèges: `ps aux`, montrer les fichiers ouverts et leurs privilèges: `ls -l | grep sshd`. Pour contrôler les ports ouverts, `netstat -atun` montre les tcp and udp, `lsof | grep IP` montre les fichiers ouverts et `nmap` (scan all tcp ports for the host 192.168.0.11) et (`// scan all udp ports for the host 192.168.0.11`)

```
nmap -Pn -p 1-65535 192.168.0.11
nmap -sU -Pn -p 1-65535 192.168.0.11
```

### 5.5 Contrôler les files systems

Leur structure se trouve dans /etc/stab

### 5.6 Contrôler les permission des fichiers, répertoires

Les users normaux devraient pas avoir accès au syslog files /var/log. Aucun fichier ou repertoires writable devrait exister, à part pour les temporary directories /tmp, /usr/tmp et /var/tmp (`ls /` ou `find /etc -type d -perm -0002 -print`) Les fichiers dans /etc must not have group and other bits writable (`find /etc -type f -perm -0002 -print` ou `find /etc -type f -perm -0020 -print`). SUID ou SGID binaries devraient être désactivés: (`find / -perm -4000 -print` ou `find / -perm -2000 -print`). Faudrait forcer /tmp à être cleaned durant le shutdown et encore mieux si possible: on met /tmp sur un disque en ram

### 5.7 Sécuriser le réseau

De base, trop d'options sont activées et donnent trop d'informations au hacker. Disable IPV6

```
echo 1 > /proc/sys/net/ipv6/conf/all/
disable_ipv6
echo 1 > /proc/sys/net/ipv6/conf/default/
disable_ipv6
Or sysctl -w /net/ipv6/conf/default/
disable_ipv6=1
```

IP source routing must be disabled

```
echo 0 > cat /proc/sys/net/ipv4/conf/all/
accept_source_route
Or sysctl -w net/ipv4/conf/all/
accept_source_route=0
```

Forwarding (Routing) of normal and multicast packets should also be deactivated unless expressively needed

```
echo 0 > /proc/sys/net/ipv4/conf/all/
forwarding
echo 0 > /proc/sys/net/ipv6/conf/all/
forwarding
echo 0 > /proc/sys/net/ipv4/conf/all/
mc_forwarding
echo 0 > /proc/sys/net/ipv6/conf/all/
mc_forwarding
Or sysctl -w net/ipv4/conf/all/forwarding=0
sysctl -w net/ipv6/conf/all/forwarding=0
sysctl -w net/ipv4/conf/all/mc_forwarding=0
sysctl -w net/ipv6/conf/all/mc_forwarding=0
```

Block ICMP redirect messages

```
echo 0 > /proc/sys/net/ipv4/conf/all/
accept_redirects
echo 0 > /proc/sys/net/ipv6/conf/all/
accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/all/
secure_redirects
echo 0 > /proc/sys/net/ipv4/conf/all/
send_redirects
Or sysctl -w net/ipv4/conf/all/
accept_redirects=0
sysctl -w net/ipv6/conf/all/accept_redirects=0
sysctl -w net/ipv4/conf/all/secure_redirects=0
sysctl -w net/ipv4/conf/all/send_redirects=0
```

Enable source route verification in order to prevent spoofing

```
echo 1 > /proc/sys/net/ipv4/conf/default/
rp_filter
Or sysctl -w net/ipv4/conf/default/rp_filter=0
```

Log all malformed packed and ignore icmp bogus ones

```
echo 1 > /proc/sys/net/ipv4/conf/all/
log_martians
echo 1 > /proc/sys/net/ipv4/
icmp_ignore_bogus_error_responses
Or sysctl -w net/ipv4/conf/all/log_martians=1
sysctl -w net/ipv4/
icmp_ignore_bogus_error_responses=1
```

Disable ICMP echo and timestamp responses sent via broadcast or multicast

```
echo 1 > /proc/sys/net/ipv4/
icmp_echo_ignore_broadcasts
Or sysctl -w net/ipv4/
icmp_echo_ignore_broadcasts=1
```

Increase resilience under heavy TCP load by increasing backlog buffer and by enabling syn cookies

```
echo 4096 > /proc/sys/net/ipv4/
tcp_max_syn_backlog
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
Or sysctl -w net/ipv4/tcp_max_syn_backlog=4096
sysctl -w net/ipv4/tcp_syncookies=1
```

la commande `sysctl -p` montre le contenu `/etc/sysctl.conf`

## 5.8 Contrôler-sécuriser les comptes utilisateurs

Ils sont affichés dans `/etc/shadow`. Le `umask`(user file creation right) doit être 0027 dans `cat /etc/profile.d/umask.sh` et ça met 0 dans les others. On peut aussi ajouter un message disant que c'est interdit avant le login dans le fichier `/etc/issue`

## 5.9 Limiter le login root

Le root devrait être uniquement possible par console : `echo "ttyS0" > /etc/securetty`. Seulement le root peut accéder au dir root: `chmod 700/root`. On utilise `sudo` pour prendre les droits de roots. Le PATH du root ne doit pas contenir le current dir ou des writable dir: `PATH not equal ./tmp:/var/tmp: etc`

## 5.10 Sécuriser le noyau

ASLR (comme en dessus) +write protect kernel make linux-config

```
Kernel Feature => [*] Apply r/o permissions of
VM areas also to their linear aliases
General Setup => [*] Set loadable kernel
module data as NX and text as RO
```

Strip-assembler comme plus haut, -fstack-protector, restrict unprivilegiend access to kernel syslog

## 5.11 Sécuriser une application

Ajouter les CFLAGS et LDFLAGS suivant

```
CFLAGS="-fPIE -fstack-protector-all -D\
_FORTIFY_SOURCE=2 -ftrapv"
LDFLAGS="-Wl,-z,now,-z,relro -z,noexecstack, -
pie"
```

- PIE: position independant executable pour avoir ROP
- -fstack-protector-all: ajout de canary random

- `_FORTIFY_SOURCE=2`: overflow check for mem-cpy, ...
- `ftrapv`: integer (only) overflow activate a catchable signal SIGABRT
- `-Wl,-z,now,-z,relro`: tous les symbols dynamiques sont résolut durant le début du porgramme et ça empêche des overwrite attacks

## 5.12 Contrôler le démarrage de Linux

Une solution, dans le but de vérifier qu'on boot sur le bon kernel, consisterait à stocker le hash du kernel sur la partition de boot et avant de booter linux faire le hash de kernel depuis uboot et comparer avec la valeur en partition.

## 5.13 Méthodologie OSSTMM simplifiée

1. Access: compter le nombre d'accès possible, le nombre de port TCP/UDP ouverts (plus haut) + `netsat -atunp`
2. Authentication: compter le nombre d'accès (ssh, console, ...) avec username et password
3. Confidentiality: compter le nombre de connexion où les données sont cryptées (ssh est mieux telnet)
4. Vulnerability, Weekness, Concern: check si un program a des vulnérabilité sur internet, tester les passwords avec les hashcat, .. et tester la robustesse des algorithme de cryptographie
5. Exposure: Ne pas donner la version de openssh sur nmap, c'est débile

# 6 FileSystem

## 6.1 Différents types de systèmes de fichiers et leur applications

Il y a 2 catégories: RAM et Flash. 2 catégories de flash, MTD et MMC/SD-Card. En volatile on a: TMPFS et initRAMFS. En MTD (plus ancien), on a JFFS2, YAFFS2 et (SQUASHFS), UBIFS. En MMC/SD-Card, on a EXT3-4, FAT, BTRFS, NILFS, (SQUASHFS), XFS, ZFS et F2FS. En MMC on a 3 couches: l'interface, le Flash Translation Layer (bad block mgmnt, garbage collection et wear levelling) et la zone de stockage. MMC/SD-Card a le partition alignement qui est critique, les données sont écrites par blocks ou pages. Pour assurer l'alignement, le début de secteur de chaque partition doit être un multiple de  $2^{20}$  (= 1048576) Bytes.

## 6.2 Ext2-3-4

A part le 2, ils sont tous journalisés et ils sont rétrocompatibles (référence pour embedded system). Les différentes commandes pour gérer les .ext4 :

```
# Create a partitions (rootfs), start 64MB,
length 256MB
sudo parted /dev/sdb mkpart primary ext4
131072s 655359s
# Format the partition with the volume label =
rootfs
sudo mkfs.ext4 /dev/sdb1 -L rootfs
# Modify (on the fly) the ext4 configuration
sudo tune2fs <options> /dev/sdb1
# Check the ext4 configuration
mount
sudo tune2fs -l /dev/sdb1
sudo dumpe2fs /dev/sdb1
# mount an ext4 file system
mount -t ext4 /dev/sdb1 /mnt/test // with
default options
```

Pour pouvoir utiliser `mkfs.ext2` et `tune2fs`, il faut configurer `make busybox-menuconfig`, Les principales options sont

- `noatime`, `nodiratime`, `relatime` pour réduire les write non-nécessaires
- `Data=journal` (journal avant écriture) safest
- `Data=ordered` (data d'abord) de base
- `Data=writeback` (pas d'ordre)
- `acl` : support POSIX Access Control Lists
- `default`: options qu'on met dans `/etc/fstab`

## 6.3 Différents FS

### 6.3.1 BTRFS

B-Tree filesystem

### 6.3.2 F2FS

Flash-Friendly File System, log filesystem with many parameter et fonctionne bien sur beaucoup de support

### 6.3.3 NILFS2

New Implementation of a Log-structured File System. Log and B-tree avec un userspace garbage collector

### 6.3.4 XFS

Journaling filesystem, support huge filesystems mais ne supporte pas bien la perte en mode standby

### 6.3.5 ZFS

Zettabyte ( $10^{21}$ ) File System. B-tree with strong data integrity, support huge fs mais pas fait pour de l'embarqué (lot of ram)



## 6.4 Journal, B\_tree/Cow, log filesystem

### 6.4.1 Journal

Garde une trace de toutes les modifications dans un journal. Cela permet de restored corrupted file. Les modifs vont d'abord dans le journal ensuite dans le disk. En cas de corruption: soit le journal est consistant (on replay le journal au mount time), soit il l'est pas et on drop les modifications

### 6.4.2 B-Tree/CoW

Les datas structure génèrent des binary tree. Cow pour copy on write: on ne modifie pas tout de suite l'original et on fait une copie plus loin et on attend le commit. Si il y a une interruption, on garde l'ancien.

### 6.4.3 Log filesystem

Use the storage medium as circular buffer et on écrit toujours à la fin (et on garde compacte). C'est souvent utilisé pour les flash medias. C'est un cow spécifique

## 6.5 SQUASHFS

C'est un compressed, read-only fs use in embedded system

```
#Create the squashed file system dir.sqsh for
the regular directory /data/config/
mksquashfs /data/config/ /data/dir.sqsh
# mount
mount -o loop -t squashfs /data/dir.sqsh /mnt/
dir
#it is possible to copy the dir.sqsh to an
unmount part with dd
umount /dev/sdb2
dd if=dir.sqsh of=/dev/sdb1
# and mount the partition as squashfs
mount /dev/sdb2 /mnt/dir -t squashfs
```

make menuconfig : target pkg, fs and flash : choose squashfs

## 6.6 TMPFS

Dynamic FS qui keep tous les files dans une virtual memory. Il met tout dans le cache interne du kernel et il grow and shrinks selon. On peut ajuster sa taille limite. Par rapport à ramfs on peut resize et swaper. Il doit être mount at /dev/shm (fstab). On mount aussi /tmp et /var comme tmpfs

## 6.7 LUKSFS

Les datas dans la partition luks sont cryptées. Les datas qui sont utilisées dans le userspace sont décryptées par dmccrypt. Linux Unified Key Setup est le standard Linux pour encrypter un hard disk. Toutes les infos de setup sont stockées dans le header pour une

meilleure portabilité. dmccrypt crypts an entire partition. Avantages de luks: comptability via standardization, secure against attacks, support for multiple keys, effective passphrase revocation and free. cryptsetup est un utilitaire pour configurer dmccrypt qui utilise les nodes files /dev/random et /dev/urandom. dmccrypt (device-mapper) crypts target and provides transparent encryption of block en utilisant le kernel crypto api. L'utilisateur peut spécifier une ciphers symmetrical, un mode d'encryption, une clé, ... et surtout un new block device dans le /dev/mapper. Toute données écrites à ce device seront cryptées, et lues seront décryptées. Pour enable dmccrypt, make linux-menuconfig, device driver, multiple devices drivers support, device mapper support crypt target support et mettre <\*>. cryptsetup est un package à ajouter dans menuconfig.

```
# creation d'une passphrase et d'un fichier
dd if=/dev/urandom of=/buildroot/output/images/
/passphrase bs=1 count=64
dd if=/dev/zero of=/buildroot/output/images/
part3.luks bs=1G count=2
#create a LUKS partition
echo YES | sudo cryptsetup --debug --pbkdf
pbkdf2 luksFormat
/buildroot/output/images/part3.luks /buildroot/
/output/images/passphrase
#dump the header information
sudo cryptsetup luksDump /buildroot/output/
images/part3.luks
#create a mapping /dev/mapper/urfs1
cryptsetup open --debug --type luks --key-file
/buildroot/output/images/passphrase /buildroot/
/output/images/part3.luks urfs1
#format the LUKS partition as EXT4
mkfs.ext4 -L luks /dev/mapper/urfs1
#mount the LUKS partition to /mnt/urfs
mkdir /mnt/urfs
mount /dev/mapper/urfs1 /mnt/urfs
#copy rootfs files to LUKS partition
cp /buildroot/output/images/rootfs.ext4 /mnt/
urfs/
#unmount the LUKS partition and remove
existing mapping
umount /mnt/urfs
cryptsetup close urfs1
```

Pour permettre au Nanopi de connaître la passphrase, ajouter ça au post-build.sh avant le umount:

```
cp /buildroot/output/images/passphrase /mnt/
passphrase
```

Cette passphrase doit être ajoutée au fichier de boot.ext4 dans gen-image.cfg et il faut aussi ajouter la partitions luks

```
partition part3 {
partition-type = 0x83
image = "part3.luks"
}
```

Pour faire tout ça au démarrage du Nanopi: /etc/init.d/s40luks

```
# start()
echo -n "Mounting luks rootfs... "
echo "Mounting boot partition"
mount /dev/mmcblk2p1 /mnt
echo -n "Unlocking luks rootfs"
cryptsetup open --type luks --key-file /mnt/
passphrase /dev/mmcblk2p3
urfs1
echo "Unmounting boot partition"
umount /mnt
echo "Mounting part3"
mount /dev/mapper/urfs1 /mnt
mount /mnt/rootfs.ext4 /mnt
echo "LUKS rootfs ready"
# stop()
echo -n "Unmounting luks rootfs"
umount /mnt
umount /mnt
cryptsetup close urfs1
```

## 6.8 LUKS keys

Il y a une master key qui est générée à l'initialisation. La passphrase passe à travers un algo (pbkdf2) et vient se combiner avec la master key dans un "crypt master key cipher" et tout ça donne une encrypted master key qui va être stored. Pour crypt ou decrypt une partition on a de nouveau besoin de la master key et de la passphrase. On peut ajouter plusieurs passphrase.

## 6.9 InitramFS

Permet d'effectuer des tâches le plus vite possible (juste après un boot) à travers un script /init qui peut s'occuper de copier et gérer les partitions luks. Initramfs est un cpio archive file, il peut être généré à la main et il contient at least one file called /init qui va être lancé par le kernel. Il a des commandes très basiques: mount, exec, ...

## 6.10 Création d'un initramFS

On PC, NanoPi rootfs is in this directory: /buildroot/output/target/

**Principle to build an initramfs :**

1. Copy the right files into a directory (\$HOME/ramfs)
2. Copy these files in a cpio archive file
3. Compress this file
4. Add the uboot header

## 7 FileSystemSecurity

### 7.1 Files permissions

Chaque user a un UID et chaque group un GID. Les lists sont `/etc/passwd` et `/etc/group`. Il y a 3 types de permissions: read access (r), write access (w) et execute (access). Et c'est défini pour 3 type de user: owner,group,others (9bits: 3x rwx).

Access type	File	Directory
Read	Read the file content	Allow to read the folder content
Write	Modify (create-delete-rename) the file	Allow to create-delete-rename files in the folder
Execute	Execute the file	Allow to go in the folder

# chmod 744 file // this command changes the file permission  
# chown test:test file // this command changes the file owner

SUID or setuid: change user id on execution to owner (-rws on owner). SGID or setgid: change group ID on execution. Sticky bit: 2 fonctions, 1) process stay in memory after it finished et 2) a directory avec sticky bit permet de supprimer un fichier si on est le file owner (ça sert dans `/tmp` on run). Pour mettre un le sticky bit on fait `chmod 4755`

### 7.2 Contrôler et sécuriser les comptes

Pour créer un user: `adduser mdp` de base c'est du md5 mais on peut configurer pour que ça soit du sha512. Pour changer un mdp: `passwd -a sha512 test1`

### 7.3 Real and effective user id and group id

Le user id réel c'est celui qu'on est `whoami` et le effective c'est celui qu'on prendrait avec le `suid`.

### 7.4 ACL

Access control list qui permet de fine tune les droits dans un directory. Il faut l'ajouter dans `make linux-menuconfig`. Ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs, Tmpfs, JFFS2 et CIFS ont le ACL. On doit ajouter l'option au `fstab` lors du montage. Commande:

```
setfacl -m permissions fileOrDirectory
# example
setfacl -m u::rwx,g::r--,o:--- test // is
↪ equal to: chmod 740 test
# delete acl
setfacl -b test
# voir acl
getfacl TestDirectory/
```

### 7.5 Attributs des fs ext2-4

```
#set
chattr -i file
#get
lsattr file
```

Attributs: -i (peut pas être modifié, supprimé, renommé or lié même pas par le root), -A (date of access is not updated), -S (synchronous), -a (only in append mode), -c (auto compress), -d (not saved by the dump), -j (write to journal before data) et -s (quand le file est destroy, toutes les datas vont à 0)

### 7.6 Rechercher les permissions de fichier faibles

```
#file permissions = 200
find . -perm 200
#rechercher/retraiter le setuid
find / -type f -perm -4000 -ls
chmod u-s /usr/bin/file
chmod -R u-s /var/directory/ // Be careful
```

### 7.7 Sécuriser les répertoires temporaires

`/tmp` ou `/var/tmp` et une install classique linux va mettre le sticky bit (t) à la fin des perm sur tout le `/tmp`. Une solution consiste à mettre ce `/tmp` sur sa propre partition avec les options (nosuid, noexec, nodev (no node file), rw). Ensuite on peut supprimer le `/var/tmp` et faire un lien symbolique qui pointe sur `/tmp`. On peut aussi prendre un fs de type tmpfs pour `/tmp` et tout avoir en ram. Sinon on peut faire du loopback en créant un fichier de 1GB

```
dd if=/dev/zero of=/tmpfs bs=1024
↪ count=1000000
mkfs.ext4 /tmpfs
mkdir /tmp
mount -o loop,nosuid,nosuid,nodev,rw /tmpfs
↪ /tmp
chmod 1777 /tmp
```

et faut ensuite ajouter dans `fstab`

```
/tmpfs /tmp ext4
↪ loop,nosuid,nosuid,nodev,rw 0 0
```

### 7.8 Mémorisation des mots de passe sous Linux

Pour voir les mots de passes: `cat /etc/shadow`

```
username:$6(sha512)ou 1 (md5)$saltvalue$passwd
ordCrypt:lastchanged(days
since01.01.1970):4:5:6(number of days
between password change)
```

### 7.9 Casser un mot de passe

5 types: Dictionary (file with words: a dictionary), Combinator (use 2 dict), Hybrid (dict + some letters), Brute force (try every combination) et Mask (brute force with inputs).

#### 7.10 Hashcat

Rapide (peut être dans GPU)

```
#Summary: -m 0 à MD5
# Nanopi : -m 500 | md5crypt, MD5 (Unix),
↪ Cisco-IOS (MD5) | Operating System
#Straight
hashcat -a 0 -m 0 hashfile dictionaryFile
#Combinator
hashcat -a 1 -m 0 hashfile dictionaryFile1
↪ dictionaryFile2
#Brute force, mask
hashcat -a 3 -m 0 hashfile ?d?d?d
#Hybrid
hashcat -a 6 -m 0 hashfile ?u?u
↪ dictionaryFile ?d?d?d
# nanopi ex dict
hashcat -a 0 -m 500 h_test1.txt rockyou.txt
# nanopi brute force (le hash est dans
↪ h_test2.txt qui est la ligne de shadow)
hashcat -a 3 -m 500 h_test2.txt A?l?s?s3?l6S4
```

## 8 Firewall IPtables

### 8.1 Principes de Netfilter et iptables

il faut configurer le kernel avec `make linux-menuconfig`. Iptables est un programme qui sert à configurer Netfilter qui est dans le noyau linux. La frame qui entre passe à travers la stack du protocol et le netfilter sera appelé. Les principales features de iptables sont stateless et stateful packet filtering, network adress translation, ... On peut créer des parefeu, faire un NAT si on a pas assez d'adresse IP.

### 8.2 Chain-tables

Quand un paquet arrive, il traverse différentes chains qui contiennent des tables. Les chains: INPUT (le paquet vient pour le host local), OUTPUT (le paquet est sent by the local host), FORWARD (vient eth0 et va à eth1), PREROUTING et POSTROUTING (used by NAT). Les tables: Filter table agit sur INPUT, FORWARD et OUTPUT, NAT table (Network Address Translation au moment d'une nouvelle connexion) agit sur PREROUTING, OUTPUT ET POSTROUTING et Mangle table (permet de modifier des paquets) agit sur TOUS les chains.

### 8.3 Différences entre stateless et stateful

Stateless: peut importer l'état (est-ce qu'il a déjà eu une connexion, ...), on refuse ou accepte.

### 8.4 Configuration d'un stateless et d'un stateful

Stateless

```
# list all existing rules in the filter table
iptables -L -n -v -t filter
# flush tables
iptables -F -t filter
# Create new chain
iptables -N dynamic
# This command ignores everything coming from
# 200.200.200.1, -A = append
iptables -A INPUT -s 200.200.200.1 -j DROP
# delete previous rule
iptables -D INPUT -s 200.200.200.1 -j DROP
# log et drop tout le icmp (ping)
iptables -A INPUT -p icmp -j LOG
iptables -A INPUT -p icmp -j DROP
# Accept the ssh service from host 10.0.0.1
iptables -A INPUT -p tcp -s 10.0.0.1 -d 0/0
# --dport 22 -j ACCEPT
# Accept the ssh service from subnet 10.0.0.x
iptables -A INPUT -p tcp -s 10.0.0.0/24 -d
# 0/0 --dport 22 -j ACCEPT
# Reject all incoming TCP traffic destined
# for ports 0 to 1023
iptables -A INPUT -p tcp -s 0/0 -d 0/0
# --dport 0:1023 -j REJECT
# Reject all outgoing TCP traffic except the
# one destined for 10.0.0.1
iptables -A OUTPUT -p tcp -s 0/0 -d !
# 10.0.0.1 -j REJECT
# Drop all SYN packets from 10.0.0.1
iptables -A INPUT -p tcp -s 10.0.0.1 -d 0/0
# --syn -j DROP
# Change the FORWARD chain to an ACCEPT
# policy
iptables -P FORWARD ACCEPT
# Block a incoming telnet only for the port
# ppp0
iptables -A INPUT -p tcp --destination-port
# telnet -i ppp0 -j DROP
```

Statefull, -m connbytes : combien de bytes par paquets en moyenne ont déjà été transférés (pour mettre les download on lower priority).

```
# Local traffic interne ok, from inside to
# outside ok si établi tout le teste non
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -m conntrack --ctstate
# NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -j DROP
```

```
iptables -A INPUT -m conntrack --ctstate
# ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -j DROP
```

Interne permis mais que du ssh depuis l'extérieur

```
iptables -A INPUT -i lo -j ACCEPT // Local
# traffics are allowed between applications
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -i eth0 -p tcp --dport 22
# -m conntrack --ctstate NEW,ESTABLISHED
# -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 22
# -m conntrack --ctstate ESTABLISHED -j
# ACCEPT
```

Seulement SSH connexion, et sort que de connexions établies

```
iptables -A INPUT -i lo -j ACCEPT // Local
# traffics are allowed between applications
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -i eth0 -p tcp --dport 22
# -m conntrack --ctstate NEW,ESTABLISHED
# -j ACCEPT
iptables -A INPUT -i eth0 -m conntrack
# --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 22
# -m conntrack --ctstate ESTABLISHED -j
# ACCEPT
iptables -A OUTPUT -o eth0 -m conntrack
# --ctstate NEW,ESTABLISHED,RELATED -j
# ACCEPT
```

Nanopi permet une connexion ssh, sur le port 62200 après authentification, accepter tous les messages de 192.168.0.4

```
iptables -A INPUT -i lo -j ACCEPT // Local
# traffics are allowed between applications
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
iptables -N dynamic
iptables -N net2fw // New chain: Network to
# Firewall
iptables -A INPUT -i eth0 -j net2fw
iptables -A net2fw -m conntrack --ctstate
# NEW -j dynamic
iptables -A net2fw -m conntrack --ctstate
# RELATED,ESTABLISHED -j ACCEPT
iptables -A net2fw -p tcp -m tcp --dport
# 62200 -j ACCEPT
iptables -A net2fw -j LOG --log-prefix
# "net2fw:DROP:" --log-level 6
```

```
iptables -A net2fw -j DROP
# After ssh authentication, insert a new rule
# in the dynamic chain
iptables -A dynamic -s 192.168.0.4 -j ACCEPT
```

### 8.5 NFQUEUE

Les cibles NFQUEUE doivent faire en sorte que le paquet aille à l'userspace. Typiquement l'icmp:

```
iptables -A INPUT -t filter -p icmp -j
# NFQUEUE --queue-num=0
```

## 9 TPM

### 9.1 Principe de chiffrement symétrique, asymétrique, fonction de hachage et signature digitale

#### 9.1.1 Chiffrement symétrique

Cipher=chiffrement, connu de tout le monde (AES, CHACHA20, ...) La même clé est utilisée pour l'encryption que la decryption. Le cleartext est découpé en block, chaque block a la même longueur (64, 128bits) et chaque block est encrypté avec un algo (AES, IDEA, ...) et une clé. CBC: chaque block est encodé avec le résultat du précédent c'est un XOR bit par bit entre IV (connu pour le premier) et le bit à encoder.

```
# encrypt a file
openssl enc -aes-256-cbc -e -in t.txt -out
# t.enc
# decrypt a file
openssl enc -aes-256-cbc -d -in t.enc -out
# t.txt
```

#### 9.1.2 Chiffrement asymétrique

La clé d'encryption (publique ou privée) n'est pas la même que celle de decryption (publique ou privée). Algo: Elliptical Curves, RSA, DSA, ... et c'est très lent. Alice et Bob doivent échanger la clé publique. Sans digital signature: Bob doit encrypter avec la public key de Alice et elle va la decrypter avec sa clé privée. Avec digital signature: Bob encrypte avec sa clé privée et Alice décode avec sa clé publique.

```
# compute private-public keys
openssl genrsa -out rsa_key.pem 2048
# get public key
openssl rsa -in rsa_key.pem -pubout -out
# rsa_key_pub.pem
# show private-public keys
openssl rsa -in rsa_key.pem {text
# show public key
openssl rsa -in rsa_key_pub.pem {pubin {text
# encrypt t.txt with public key
```



```
openssl rsautl -encrypt -pubin -inkey
  ↳ rsa_key_pub.pem -in t.txt -out t.rsa
# decrypt t.rsa with private key
openssl rsautl -decrypt -inkey rsa_key.pem
  ↳ -in t.rsa -out t1.txt
```

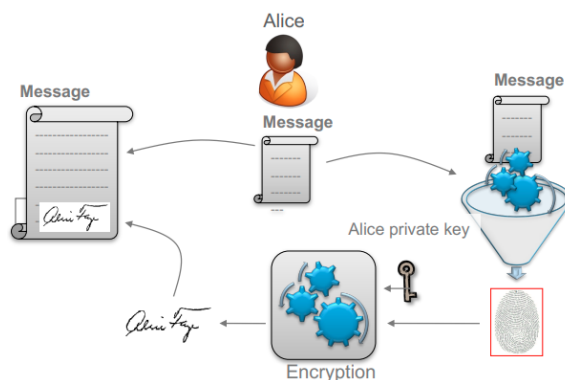
### 9.1.3 Fonction de hachage

Une fonction  $H$  qui prend une entrée  $m$  de n'importe quelle taille et qui génère  $h$  qui est une fixed-size string (according to md5, sha512). 2  $m$  différentes ne devraient jamais donner la même sortie  $h$  sinon c'est une collision (catastrophique).

```
md5sum file
a6a0e8d0522e2c5de921b1c455506320
```

### 9.1.4 Signature digitale

Objectif : intégrité du message et authentification de l'origine du message.



```
# 3 même ligne que Asym cipher
# sign t.txt with public key
openssl dgst -sha256 -sign rsa_key.pem -out
  ↳ t.sign t.txt
# decrypt t.rsa with private key
openssl dgst -verify -sha256 rsa_key_pub.pem
  ↳ -signature t.sign t.txt
```

## 9.2 Différentes implémentations des TPM

Discrete: Implémentation dans le semiconducteur d'un chip dédié. Integrated: Partie d'un chip, ex ARM: TrustZone. Hypervisor: Virtual TPMs provided by and rely on hypervisors. Software: Emulator software avec pas plus de protection qu'un os.

## 9.3 Architecture interne d'un TPM

Il contient des algo asym et sym, des fonctions de hash, des random generator, des key generator, de la NV Ram (persistente), des PCR (platform configuration register) et de la RAM classique.

## 9.4 Hiérarchies des TPM

Endorsement: réservé pour des objets créés et certifiés par le fabricant (la eseed est gen randomly at manufacture time et ne bougera jamais (peut servir d'ID)). Platform: réservé pour des objets créés par le OEM qui construit la plateforme (la pseed est gen randomly at manufacture time mais peut être changée : tmp2\_changepps). Owner hierarchy: reserved for us, on peut regen la oseed avec tmp2\_clear. Null hierarchy: réservé pour des clés éphémères qui sont régénérées at reboots. Toutes les clés (peut importe la hiérarchie) sont générées avec des Key Derivation Function). Les TPMS génère des clés qui sont à base de true random source et ces clés ne quittent que le TPM de manière cryptée par sa clé parent.

## 9.5 Créer et utiliser des TPM

```
tmp2_createprimary -C <A> -G rsa2048 -c <B>.ctx
```

<A>	<B>
e	e_primary
p	p_primary
o	o_primary
n	n_primary

## 9.6 Commandes principales

```
tmp2_getcap handles-transient #voir clé dans la RAM
tmp2_getcap handles-persistent #voir clé dans la NV-RAM
tmp2_evictcontrol -c o_primary.ctx # sauve une clé en NV-RAM
tmp2_readpublic ... # pour lire la clé publique et ensuite utiliser openssl pour la voir
tmp2_flushcontext! -t ##effacer toute la RAM
tmp2_create -C o_prim -G rsa2048 -u child_pub -r child_priv #créer clé enfant
tmp2_load -C o_prim -u child_pub -r child_priv -c child #charger clé enfant
shred passwd, rm -f passwd #supprimer de l'hôte
```

## 9.7 encrypter-décrypter, signer-vérifier

```
tmp2_rsaencrypt -c child -s rsaes clearfile -o encryptedfile
tmp2_rsadecrypt -c child -s rsaes encryptedfile -o clearfile
tmp2_sign -c child -g sha256 -o file.sign file
tmp2_verifysignature -c child -g sha256 -s file.sign -m file
```

## 9.8 PCR

Tout registrer est chaque fois hash pour chaque modification. Un update est appelé extend. La spécification de la plateforme TPM spécifie les PCR attributes et ou va quoi est standardisé.

```
tmp2_pcrreset 0
tmp2_pcrextend 0:sha1=8c83...(hash)
```

## 9.9 Sauver des données sur le TPM

On va par exemple créer un mot de passe, le sauver sur le TPM, le supprimer sur le host et le récupérer quand il y a besoin.

```
tmp2_evictcontrol -c passwd.ctx 0x81010000 -C
  ↳ #sauver
tmp2_unseal -c 0x81010000 > passwd #récupérer
```

## 9.10 Sauver des données sur le TPM et les protéger avec une PCR policy

Par exemple unseal data seulement si les valeurs des registres PCV n'ont pas changé (pas eu de tentative de hacking).

```
sha1sum passwd #calcul hash
tmp2_pcrreset 0 #flush PCR0
tmp2_pcrextend 0:sha1=8c839... #sauve hash
tmp2_createprimary -C o -G rsa2048 -c primary
tmp2_startauthsession -S session
tmp2_policypcr -S session -l sha1:0 -L pcr0_policy #créer politique
tmp2_flushcontext session
tmp2_create -C primary -g sha256 \
-u passwd_pcr0.pub -r passwd_pcr0.priv \
-i passwd -L pcr0_policy
tmp2_evictcontrol -c passwd_pcr0 0x81010000 -C
  ↳
tmp2_flushcontext session
shred passwd
rm -f passwd
tmp2_startauthsession --policy-session -S session
tmp2_policypcr -S session -l sha1:0
tmp2_unseal -p session:session -c 0x81010000 > passwd
```