MSE | MASTER OF SCIENCE IN ENGINEERING

Secure Embedded Systems

Laboratoire I

U-Boot & Linux Kernel

Savy Cyrille - Mueller Michael

2015

HES-SO//Master
Orientation TIC

Professeur	: Schuler Jean-Roland
Branche	: SES
Salle de laboratoire	: 5
Dernière mise à jour	: 23 avril 2015

Table des matières

Chapitre 1

Introduction

La sécurité dans les systèmes embarqués, qui sont présents de plus en plus souvent dans un nombre de domaine grandissant, est primordiale pour éviter les abus de personnes malintentionnées (voir éviter les erreurs humaines possibles...).

Le but de ce laboratoire était de découvrir l'environnement U-Boot sur la plateforme "Odroid" basée sur un processeur "Samsung", l'Exynos5422 ! C'est une plateforme beaucoup plus performante que celles utilisée précédement au cours de CSEL, qui elle est basée sur un processeur Freescale AFP27.

Dans ce laboratoire, nous avons pu appliquer certaines méthodes de software hardening en changeant quelques commandes de compilation, notamment pour ôter les symboles de "debug".

Chapitre 2

Question 1

2.1 What is the real name for the node file "/dev/root"

Si on lance la commande suivante :

```
# ls -al /dev/root
lrwxrwxrwx    1 root     root             9 Jan  1 00:00 /dev/root -> mmcblk0p2
```

On remarque que "root" est un lien symbolique sur /dev/mmcblk0p2.

2.2 What are the major and minor number for the "/dev/root" node file

Par analogie, on regarde les informations sur le fichier pointé :

```
ls -al /dev/mmcblk0p2
brw-rw----    1 root     root      179,   2 Jan  1 00:00 /dev/mmcblk0p2
```

On voit le numéro majeur est 179 et le numéro mineur 2.

2.3 How the kernel knows that the rootfs in in the second partition

Le noyau sait que notre "rootfs" est sur "mmcblk0**p2**", car c'est un paramètre de boot que nous avons configuré dans "u-boot".

Chapitre 3

Question 2

3.1 Mount manually the usrfs partition

Voilà la commande de montage avec les paramètres par défauts :

```
# mkdir /mnt/usr
# mount -o rw,suid,dev,exec,async /dev/mmcblk0p3 /mnt/usr/
# mount
        ...
        /dev/mmcblk0p3 on /mnt/usr type ext4 (rw,relatime,data=ordered)
```

On voit que notre système à bien monté la partition au bon endroit.

3.2 Modify /etc/fstab

Voilà la version avec le montage automatique du "usrfs" :

```
# cat /etc/fstab
# /etc/fstab: static file system information.
#
# <file system> <mount pt>     <type>   <options>          <dump> <pass>
/dev/root       /              ext2     rw,noauto          0      1
/dev/mmcblk0p3  /mnt/usr       ext4     defaults           0      1
proc            /proc          proc     defaults           0      0
devpts          /dev/pts       devpts   defaults,gid=5,mode=620   0      0
tmpfs           /dev/shm       tmpfs    mode=0777          0      0
tmpfs           /tmp           tmpfs    mode=1777          0      0
sysfs           /sys           sysfs    defaults           0      0
```

Chapitre 4

Question 3

4.1 EXT4 Performances

Chapitre 5

Conclusion

Ce laboratoire nous a permis de mettre en pratique la théorie vue en cours ainsi que de rafraîchir nos connaissances précédentes sur Linux embarqué. Les systèmes embarqué étant "limités" (cette affirmation est aujourd'hui à moitié vraie... Notre plate-forme est tout de même dotée d'un octo-coeur ARM et de beaucoup de mémoire vive. Mais ce n'est pas forcément le cas de tous les systèmes sur le marché) en performances nécessitent un traitement particulier quand à leur sécurité.

On peut facilement prendre ces systèmes et en extraire les données. Une partie de la sécurité peut être crée à la conception hardware du système (protection des ports JTAG, etc...), mais le reste doit être géré au niveau du software.

Nous avons vu quelques techniques de protections en modifiant les variables de compilation. L'utilisation de la cryptographie devrait être mieux appliquée au niveau du bootloader (notre version ne la support pas, mais elle existe dans les versions supérieure). Contrôler le noyau chargé en mémoire par un hash et/ou une signature (avec ou sans certificats) serait adéquat.
La protection du système de fichiers fait partie de la seconde partie du laboratoire.