

Annexe A

Travaux Pratiques 1

Dans ce premier TP nous vous proposons un code minimaliste du premier noyau pour le système d'exploitation Sextant. L'objectif de ce TP est de comprendre les mécanismes permettant de charger en mémoire puis d'exécuter un système d'exploitation mais aussi de se familiariser avec l'environnement logiciel qui vous accompagnera pour les prochains TP.

Question 1 - Durée estimée : 30 minutes

Modifier le fichier de bootloader pour changer le menu de démarrage en vue de remplacer SOLUTION par CORRECTION. Pour cela vous devez modifier le fichier de configuration du menu de boot et générer l'image grâce à l'utilitaire mkisofs.

Quelle signification donnez vous à l'option -tftp ./ de qemu ?

Le programme s'exécutant dans Qemu boucle indéfiniment : donner les 3 lignes correspondantes.

Quelle est la valeur retournée par notre premier noyau ?

Question 2 - Durée estimée : 60 minutes

Sous Qemu il est possible de récupérer beaucoup d'information sur l'état de la machine grâce à l'option monitor.

Faites une copie d'écran de qemu.

Trouvez la commande permettant d'afficher la valeur retournée par main. Commencer par déterminer comment afficher les registres processeurs puis où est sauvegardé le retour d'une fonction system.

De là, déterminer la valeur retournée par notre noyau. Est-ce la bonne ? Pourquoi ?

Décompilez le code de notre noyau via l'utilitaire Objdump. Faites la même opération via Qemu grâce à la commande xp. Pour rappel le code est dans la section .text

Suivant l'adresse de début pour le désassemblage le code assembleur affiché n'est pas exactement le même. Pourquoi ? Vous pouvez vous aider de la section 3.1 de cet article de recherche :

<http://www2.cs.arizona.edu/solar/papers/CCS2003.pdf>

Our des slides (à partir de 15)

<http://security.di.unimi.it/sicurezza1112/slides/Lezione4.pdf>