SeS (Secure Embedded System)

Objectifs de l'examen oral du lundi 31 janvier 2022

Rappel :
L'examen oral aura lieu :
1) A Lausanne si on peut le faire en présentiel à Lausanne
2) A distance, si on ne peut pas faire d'examen en présentiel

Je vous informerai dès que j'aurai des informations.

Conditions d'examen :

a. Après le tirage au sort d'une enveloppe contenant deux questions traitant de sujets différents, l'examen oral se déroulera en deux phases :
   - une phase de préparation de 20 minutes et
   - une phase de présentation de 20 minutes.

b. Durant la phase de préparation, l'étudiant-e préparera les réponses aux questions sur transparents. Pour sa préparation, l'étudiant-e aura le droit à un résumé de **5 pages imprimées recto-verso sous forme papier**. Les portables, tablettes ou smartphones ne sont pas autorisés.

c. Durant la phase présentation, l'étudiant-e exposera ses solutions au collège de professeurs au rétroprojecteur et répondra aux questions subsidiaires. Ces questions permettront au collège de professeurs d'établir le niveau de connaissance et de compétences de l'étudiant-e. Durant la présentation, l'étudiant ne pourra utiliser que les transparents rédigés précédemment dans la phase de préparation (ne pourra pas utiliser le résumé).

d. A la fin de l'examen, les questions et les transparents seront récupérés et conservés par le collège de professeurs.

SeS (Secure Embedded System)

Objectifs de l'examen oral du lundi 31 janvier 2022

Les étudiant-e-s devront être capable :

Buildroot

1. D'expliquer les principaux répertoires de buildroot
2. D'expliquer comment configurer, compiler buildroot, u-boot, kernel
3. D'expliquer comment le rootfs est généré
4. D'expliquer le rootfs_overlay

u-boot

5. D'expliquer le démarrage du NanoPi
6. De connaître, expliquer les principales commandes de u-boot utilisées durant le démarrage
7. De savoir comment configurer u-boot
8. D'expliquer comment améliorer la sécurité de u-boot
9. De connaître les différentes étapes pour la création de l'image de u-boot.itb
10. Savoir ce que fait la commande strip sur un fichier elf
11. De connaître les différentes étapes pour la création de uImage
12. Se connaître les différents formats du kernel
13. De connaître l'utilité du Flattened Device Tree
14. De connaître de manière générale le mapping de la SDCard
15. D'expliquer le fichier boot.scr

Compilation du noyau

16. De connaître les principaux répertoires du noyau Linux
17. De connaître les principales méthodes pour sécuriser le noyau Linux
18. D'expliquer le principe des software attacks : buffer overflow, ret2libc, ROP
19. D'expliquer le principe des protections contre les softwares attack : ASLR, PIE, canary

Valgrind

20. De connaître les différents outils de Valgrind et leur utilisation
21. Pour un code donné avec des erreurs, savoir quel-s outil-s de Valgrind utiliser

SeS (Secure Embedded System)

Objectifs de l'examen oral du lundi 31 janvier 2022

Hardening Linux

22. De contrôler l'intégrité d'un package, d'un programme
23. De configurer un nouveau package, programme
24. De cross-compiler un programme
25. De contrôler les services, les ports ouverts
26. De contrôler les « file systems »
27. De contrôler les permissions des fichiers, répertoires
28. De sécuriser le réseau
29. De contrôler-sécuriser les comptes utilisateurs
30. De limiter le login root
31. De sécuriser le noyau
32. De sécuriser une application
33. De contrôler le démarrage de Linux

Filesystem

34. De connaître les différents types de systèmes de fichiers ainsi que leurs applications
35. De connaître les caractéristiques des filesystems ext2-3-4, ainsi que les commandes associées
36. D'expliquer les différents « files systems » utilisés dans les systèmes embarqués (ext2-3-4, BTRFS, F2FS, NILFS2, XFS, ZFS, …)
37. Expliquer les « files system » de type Journal, B_Tree/CoW, log filesystem
38. De connaître les caractéristiques du filesystem Squashfs, ainsi que les commandes associées
39. De connaître les caractéristiques du filesystem tmpfs, ainsi que les commandes associées
40. De connaître les caractéristiques du filesystem LUKS, ainsi que les commandes associées
41. Savoir expliquer la gestion des clés de LUKS
42. De connaître les caractéristiques du filesystem InitramFS, ainsi que les commandes associées
43. De savoir créer un initramFS

SeS (Secure Embedded System)

Objectifs de l'examen oral du lundi 31 janvier 2022

Filesystems security

44. De connaître les « files permissions » sous Linux
45. De contrôler et sécuriser les comptes utilisateurs sous Linux
46. De connaître les real-effective userID and groupID
47. De connaître les ACL
48. De connaître les attributs particuliers des filesystems ext2-3-4
49. De rechercher des permissions de fichier faibles
50. Comment sécuriser les répertoires temporaires
51. De savoir comment les mots de passe sont mémorisés sous Linux

Firewall Iptables

52. De connaître les principes de Netfilter, iptables
53. Savoir expliquer les notions de chain-tables
54. Savoir expliquer les différences entre les firewall Stateless et Stateful
55. Savoir configurer avec iptables un firewall simple de types Stateless (pages 17-19) et Stateful (pages 27,28 et 30)
56. Savoir expliquer le principe de fonctionnement de knockd et les liens avec iptables
57. Savoir expliquer le principe de fonctionnement de fwknop et les liens avec iptables

TPM

58. Savoir expliquer le principe des chiffrements symétrique, asymétrique, fonctions de hachage, la signature digitale
59. Connaitre les différentes implémentations des TPM (discrete, integrated, Hypervisor, Software)
60. Connaitre l'architecture interne d'un TPM
61. Connaitre les différentes hiérarchies des TPM (endorsement, platform, owner, null)
62. Savoir créer, utiliser des clés avec un TPM
63. Connaitre les commandes principales d'un TPM (pas tous les paramètres, mais savoir expliquer ce que font ces commandes, être capable de dessiner ce que font les commandes)
64. Savoir encrypter-décrypter, signer-vérifier avec un TPM
65. Savoir utiliser les registres PCR
66. Savoir sauver des données sur le TPM
67. Savoir sauver des données et les protéger avec une PCR policy