Examen module Sécurité des Systèmes d'Exploitation

Les documents (notes, slides) sont admis, pas internet !

Questions de cours (0xc points): *Les questions portent spécifiquement sur l'architecture Intel x86 32 bits (IA-32). Justifiez vos réponses (… brièvement).*

- Q1 - En mode protégé, pourquoi le registre EIP n'est pas suffisant pour calculer correctement l'adresse de l'instruction courante ?
- Q2 - Quel est le niveau de privilèges le plus élevé, autorisé par la segmentation ?
- Q3 - Par quel procédé peut-on augmenter son niveau de privilèges en mode protégé ?
- Q4 - Par quel procédé peut-on abaisser son niveau de privilèges en mode protégé ?
- Q5 - A quoi sert le TSS dans les OS modernes (Windows/Linux) ?
- Q6 - A quelle(s) faille(s) de sécurité élémentaire l'implémentation des appels systèmes peut-elle être exposée ?
- Q7 - Citez un intérêt, du point de vue de la sécurité, offert par la pagination.
- Q8 - Quel problème de sécurité majeur pose le bit R/W des entrées de tables de pages ?
- Q9 - Combien de niveaux de privilèges existe-t-il lorsque l'on utilise la pagination ?
- QA - Que se passe-t-il lorsqu'on accède au registre CR0 en ring 3 ?
- QB - Expliquez pourquoi il est dangereux, pour un noyau, de sauver le contexte d'une tâche dans la mémoire utilisateur de cette tâche. Dans quelle zone de mémoire un noyau devrait-t-il le sauvegarder ?
- QC - Quels sont les avantages, toujours du point de vue de la sécurité, des micro-noyaux par rapport aux noyaux monolithiques ?

Problème 1 (0x4 points): *Pagination*

Dans la suite de l'énoncé, PPN signifie Physical Page Number (numéro de page physique). Considérons la configuration suivante de tables de pages pour un processeur Intel x86 32 bits.

Le Page Directory à l'adresse physique 0x00001000 contient:

PDE 0: PPN=0x00002, PTE_P, PTE_U, PTE_W
PDE 1: PPN=0x00003, PTE_P, PTE_U, PTE_W
PDE 2: PPN=0x00002, PTE_P, PTE_U, PTE_W
... les autres PDEs sont à zéro

La Page Table 1 à l'adresse physique 0x00002000 (PPN 0x00002) contient:

PTE 0: PPN=0x00005, PTE_P, PTE_U, PTE_W
PTE 1: PPN=0x00006, PTE_P, PTE_U, PTE_W
... les autres PTEs sont à zéro

La Page Table 2 à l'adresse physique 0x00003000 contient:

PTE 0: PPN=0x00005, PTE_P, PTE_U, PTE_W
PTE 1: PPN=0x00005, PTE_P, PTE_U, PTE_W
... les autres PTEs sont à zéro

Questions: *justifiez vos résultats*

- P1Q1 - Listez toutes les adresses virtuelles qui *mappent* l'adresse physique 0x00005555.
- P1Q2 - L'adresse virtuelle 0x402000 (4*1024*1024 + 8192) est-elle *mappée* ?
- P1Q3 - A quelle adresse virtuelle (s'il en est) le noyau doit-il écrire pour modifier le *mapping* de l'adresse virtuelle 0x402000 ?
- P1Q4 - Expliquez précisément ce que la Page Table 2 devrait contenir afin de permettre au noyau d'écrire dans le Page Directory. Plusieurs réponses sont possibles. Expliquez-en une.

Problème 2 (0x4 points):

Imaginez un noyau de système d'exploitation offrant de la sécurité (isolation des tâches et du noyau) sans le mécanisme matériel des appels systèmes (`int XX`, `sysenter/sysexit`).

Questions: *Pensez à justifier systématiquement mais brièvement vos réponses*

- P2Q1 - Citez les éléments du processeur que le noyau doit configurer pour mettre en place une isolation ring 3 / ring 0.
- P2Q2 - Proposez une solution permettant au ring 3 de communiquer avec le ring 0 sans compromettre la sécurité du système.
- P2Q3 - Quelles sont les vulnérabilités potentielles de votre solution ? Comment les éviter ?
- P2Q4 - Décrivez brièvement, l'exécution d'un appel système hypothétique fondé sur votre concept.