

Numéro d'anonymat :

Examen de IPRM

Master Informatique

Partie de Cours de S. Chaumette

Année 2012-2013

Le 16 janvier 2013

Documents autorisés : aucun

Durée : 35 minutes

Ce sujet comporte 3 pages et un article de 2 pages.

Document joint : article « How to share a secret »

Les réponses seront données sur ce document et uniquement dans les zones prévues à cet effet.

Exercice 1. Cet exercice se présente sous la forme d'un QCM. Pour chaque question, on peut cocher plusieurs cases. Une case cochée à tort comptera des points en moins.

a. On appelle migration forte :

- ☐ une migration temporaire
- ☐ une migration avec reprise sur l'instruction suivant la migration
- ☐ un déplacement lié à la charge des machines concernées
- ☐ une migration avec reprise sur l'instruction précédant la migration

b. On appelle migration faible :

- ☐ une migration définitive
- ☐ une migration avec reprise sur l'instruction suivant la migration
- ☐ une migration avec reprise sur un début de fonction/méthode
- ☐ une migration avec reprise sur l'instruction précédant la migration
- ☐ un déplacement lié à l'utilisation de la CPU par l'agent considéré
- ☐ un retour d'une migration forte

c. On ne peut pas réaliser d'agents mobiles sans :

- ☐ une connexion réseau
- ☐ une clef USB
- ☐ des *threads*
- ☐ le format *xdr*
- ☐ un mécanisme de sérialisation
- ☐ un mécanisme de type réflexion

Numéro d'anonymat :

Exercice 2. On imagine qu'une entreprise utilise une application dont elle ne possède plus que le code binaire et qui offre deux fonctions func_1 et func_2. Elle souhaite rendre disponible ces deux fonctions sur le réseau sous la forme de services.

Proposez une solution (explications courtes mais claires), schéma (architecture et fonctionnement) et pseudocode (uniquement si nécessaire).

Exercice 3.

Les questions de cet exercice portent sur l'article joint à ce sujet.

Problème, contexte, utilisation de l'approche (section 1. de l'article).

- a. Quel est le problème posé par Liu et sa solution ?

b. Quelle est la généralisation à laquelle s'intéresse Shamir ?

c. Comment s'appelle ce problème/cette approche ?

d. Donner au moins deux exemples d'utilisations de l'approche proposée

Mise en œuvre (section 2 de l'article)

Quels sont les avantages (ou propriétés intéressantes) de la mise en œuvre proposée en section 2. de l'article ?

Utilisation dans une « infrastructure mobile »

En quoi une telle approche peut-elle aider à la distribution sécurisée de clef dans un réseau de terminaux mobiles ? Comment ?