ENSEIRB MATMECA BORDEAUX

Année 2010-2011 — 1ère session

Sécurité des Systèmes d'Information
IT 218
Paul Dorbec

Filière : Informatique — Année : 2ième — Semestre : S4

Date de l'examen : 25 mai 2011 — Durée de l'examen : 2h

Documents autorisés ☒ sans document ☐
Calculatrice autorisée ☐ non autorisée ☒

Autre : .....

SUJET

Le sujet comporte 2 pages. Il est composé de 3 exercices indépendants, qui peuvent être traités dans un ordre quelconque. Le barème est donné à titre indicatif.
Un certain nombre de questions sont "ouvertes". Il est alors demandé de ne pas ce contenter de donner une solution évidente, mais de discuter un peu plus en profondeur des aspects non triviaux de la question.

1 Quelques questions simples

Question 1.1 (1pt)
Qu'est-ce qu'une attaque par dictionnaire?

Question 1.2 (1pt)
Décrivez brièvement le principe d'une zone démilitarisée (DMZ).

Question 1.3 (1pt)
Qu'est ce qu'un code correcteur d'erreur?

Question 1.4 (1pt)
Pourquoi le client ssh *râle-t-il si je donne à mon fichier* ∼/.ssh/id_rsa *les droits* rwxrwxrwx*, alors que ce n'est pas un problème pour* ∼/.ssh/id_rsa.pub*?*

Question 1.5 (1pt)
Pourquoi faut-il faire particulièrement attention lorsque l'on développe un programme destiné à avoir le bit SETUID *activé ?*

Question 1.6 (1pt)
Sur une même machine, Alice regarde un film sur son écran, tandis que Bob, à distance, compile des programmes via ssh*. Quel problème peut se poser ? Comment le résoudre ?*

2 Logique de Burrows-Abadi-Needham

Le système dit de *logique BAN* est un système formel permettant de vérifier la sécurité d'un protocole. À partir d'hypothèses de départ et de la description des différentes étapes d'un protocole, l'utilisation de règles de réécriture permet d'analyser la sécurité du protocole.
Je vous rappelle les notations, qui sont les suivantes :

- $P \models X$: P croit X
- $P \triangleleft X$: P voit X
- $P \succ X$: P a dit X
- $P \overset{K}{\longleftrightarrow} Q$: K est une bonne clé partagée par P et Q
- $\#(X)$: X est frais.

Question 2.1 (2pts)
Expliquez la règle d'inférence suivante :

$$\frac{P \models P \overset{K}{\longleftrightarrow} Q, P \triangleleft \{X\}_K}{P \models Q \succ X}$$

Question 2.2 (2pts)
Expliquez la règle d'inférence suivante :

$$\frac{P \models Q \succ X, P \models \#(X)}{P \models Q \models X}$$

Question 2.3 (3pts)
Une critique de la méthode de la logique BAN est qu'elle ne tient pas compte des relations arithmétiques entre les messages. Expliquez.

3 Virus, biodiversité et économie de mécanismes

Question 3.1 (2pt)
Rappelez le principe de l'économie de mécanismes. Illustrez le avec un exemple.

Question 3.2 (2pts)
Il est fréquemment dit que les systèmes d'exploitation de types Unix/Linux sont plus ou moins protégés des virus du fait de leur diversité. Expliquez.

Question 3.3 (3pts)
Ces deux dernières affirmations portent-elles une contradiction? Etayez.