ENSEIRB MATMECA BORDEAUX

Année 2009-2010 — 1ère session

Sécurité des Systèmes d'Information
IT 218
Paul Dorbec

Filière : Informatique — Année : 2009-2010 — Semestre : S4

Date de l'examen : 10 mai 2010 — Durée de l'examen : 2h

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

Autre : .....

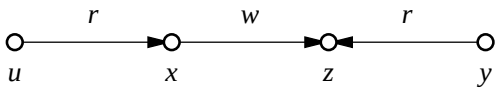
**SUJET**

Le sujet comporte 3 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 Modèle Take-Grant

Voici une situation dans le cadre du modèle "Take-Grant":

- l'utilisateur $u$ détient un droit *read/take* sur un élément $x$.
- l'élément $x$ détient un droit *write/grant* sur la ressource $z$.
- un autre élément $y$ détient un droit *read/take* sur la ressource $z$.




**Question 1.1 (2pts)**
*Expliquez comment l'utilisateur u peut obtenir le droit d'accès* (read/take) *à la ressource z dans cette situation.*

**Question 1.2 (3pts)**
*Même question quand u ne détient pas le droit* read *sur x mais un droit* call.

# 2 Analyse de protocole

Voici la description d'un protocole permettant d'établir une clé de session $K_{A,B}$ entre Alice et Bob, utilisant un arbitre Trent.
Les interlocuteurs (et identifiants) sont $A$, $B$ et $T$. Alice et Bob tirent des nombres aléatoires $N_A$ et $N_B$ "frais". Alice et Trent partagent une clé secrète $K_{A,T}$, Bob et Trent une clé secrète $K_{B,T}$, et on suppose que Trent a la compétence pour établir une clé de session sûre $K_{A,B}$.
Initialement :

- Alice connait : $A, B, T, K_{A,T}$
- Bob connait : $B, T, K_{B,T}$
- Trent connait : $T, A, B, K_{A,T}, K_{B,T}$

Le protocole se déroule ainsi:

1. $A \longrightarrow B$ : $\Big(A, N_A\Big)$
2. $B \longrightarrow T$ : $\Big(B, \big\{A, N_A, N_B\big\}_{K_{B,T}}\Big)$
3. $T \longrightarrow A$ : $\Big(\big\{B, K_{A,B}, N_A, N_B\big\}_{K_{A,T}}, \big\{A, K_{A,B}\big\}_{K_{B,T}}\Big)$
4. $A \longrightarrow B$ : $\Big(\big\{A, K_{A,B}\big\}_{K_{B,T}}, \big\{N_B\big\}_{K_{A,B}}\Big)$

**Question 2.1 (2pts)**
*Décrivez brièvement ce que sont censés connaître les acteurs à chaque étape du protocole, et justifiez.*

**Question 2.2 (1pt)**
*L'un des intérêts de ce protocole est de ne faire que deux communications avec Trent. Expliquez en quoi cette restriction est pertinente.*

**Question 2.3 (1pt)**
*Expliquez le rôle des nombres $N_A$ et $N_B$.*

**Question 2.4 (2pts)**
*À l'étape 4, Bob connait le nombre $N_A$. Que pensez-vous de l'idée consistant à retirer $N_B$ du protocole et à remplacer $\{N_B\}_{K_{A,B}}$ par $\{N_A\}_{K_{A,B}}$ ?*

**Question 2.5 (2pts)**
*Un an après la parution de ce protocole, Needham a découvert à l'aide de la logique* BAN *que le protocole permettait à Alice de réutiliser une vieille clé $K_{A,B}$. Décrivez comment cela est possible.*

Pour corriger ce problème, Needham a proposé la variante suivante:

1. $A \longrightarrow B$ : $\Big(A, N_A\Big)$
2. $B \longrightarrow T$ : $\Big(B, N_B\big\{A, N_A\big\}_{K_{B,T}}\Big)$
3. $T \longrightarrow A$ : $\Big(N_B, \big\{B, K_{A,B}, N_A\big\}_{K_{A,T}}, \big\{A, K_{A,B}, N_B\big\}_{K_{B,T}}\Big)$
4. $A \longrightarrow B$ : $\Big(\big\{A, K_{A,B}, N_B\big\}_{K_{B,T}}, \big\{N_B\big\}_{K_{A,B}}\Big)$

Cependant, avec cette nouvelle version, Mallory peut procéder à une nouvelle attaque en lançant deux fois le protocole simultanément. Voici une description de l'attaque, où $M(X)$ désigne Mallory se faisant passer pour $X$ :

i.1. $A \longrightarrow M(B)$ : $\Big(A, N_A\Big)$

i.2. $B \longrightarrow M(T)$ : $\Big(B, N_B\big\{A, N_A\big\}_{K_{B,T}}\Big)$

ii.1. $M(A) \longrightarrow B$ : $\Big(A, N_A, N_B\Big)$

ii.2. $B \longrightarrow M(T)$ : $\Big(B, N'_B\big\{A, N_A, N_B)\big\}_{K_{B,T}}\Big)$

i.3. *Omise*

i.4. $M(A) \longrightarrow B$ : $\Big(\big\{A, N_A, N_B\big\}_{K_{B,T}}, \big\{N_B\big\}_{N_A}\Big)$

**Question 2.6 (2pts)**
*Expliquez sur quoi cette attaque repose et en quoi elle fonctionne.*

**Question 2.7 (2pts)**
*Proposez un moyen de corriger le protocole de Needham pour prévenir cette attaque*

# 3 Détection d'intrusion

Les systèmes de détection d'intrusion (IDS) ont pour fonction principale de détecter et d'analyser toute tentative d'effraction dans un système. Pour ce faire, ils analysent à l'aide de composants logiciels ou matériels les flux en transit sur un réseau (IDS réseau ou NIDS) ou l'activité sur un système hôte (IDS hôte ou HIDS). Dans le cas de la détection d'une activité anormale, la plupart des IDS alerte l'administrateur du système (pour ne pas entraver une utilisation normale du système) et quelques uns tentent de contrer l'attaque d'eux-même.

Pour reconnaitre une attaque, deux stratégies existent. La première stratégie est dite *par scénario* : l'IDS compare les activités avec des scénarios connus, et soulève une alerte s'il reconnait un scénario d'attaque de sa base. La deuxième stratégie est dite *comportementale* : le système analyse le comportement de l'utilisateur, définit un profil de comportement habituel de l'utilisateur, et signale une intrusion lorsqu'il détecte un comportement ne correspondant pas à ce profil.

**Question 3.1 (3pts)**
*Discutez des avantages et des inconvénients de chacune de ces stratégies*

Un IDS peut commettre des erreurs dans deux sens. Le système peut ne pas détecter une attaque en cours; on parle alors de *faux négatif*. Par opposition, on parle de *faux positif* lorsque le système soulève une alerte sans qu'aucun comportement anormal n'ait eu lieu.

**Question 3.2 (3pts)**
*Les conséquences d'un faux négatif sont évidentes. Expliquez en quoi les faux positifs peuvent être vraiment gênants voir conduire à des problèmes de sécurité.*

**Question 3.3 (3pts)**
*Les IDS sont sensibles aux attaques par Déni de Service (DoS). Expliquez.*