

# DEA Informatique - Rennes 1 - 2003-2004

## SFRC

### Sécurité des systèmes informatiques

(Durée : 1h30)

Ludovic Mé

janvier 2004

## 1 Exercice 1 : authentification cryptographique

Un mécanisme d'authentification avancé est mis en place dans une organisation qui ne se satisfait pas du passage en clair de mots de passe sur le réseau. Le protocole d'authentification cryptographique de Needham-Schroeder est retenu. Il s'exprime de la manière suivante :

1.  $A \rightarrow S : A, B, N_A$
2.  $S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$
3.  $A \rightarrow B : \{K_{AB}, A\}_{K_{BS}}$
4.  $B \rightarrow A : \{N_B\}_{K_{AB}}$
5.  $A \rightarrow B : \{N_B - 1\}_{K_{AB}}$

Précisez ce que sont les entités communicantes A, B et S ? Quelles sont les clés impliquées et entre qui sont-elles partagées ? Faire un schéma. Les utilisateurs peuvent-ils avoir confiance dans ce protocole ? Donnez votre réponse de manière informelle ou de manière formelle.

## 2 Exercice 2 : étude de cas

### Description de l'environnement

Un organisme d'enseignement supérieur (OES) regroupe des étudiants répartis en trois années d'étude. Lors de la troisième année, les étudiants se spécialisent en informatique (INF) en automatique (AUT) ou en électronique (EON).

Les enseignants sont répartis en trois départements (DINF, DAUT et DEON). Ils interviennent devant les étudiants des deux premières années et devant les étudiants de troisième année de leur spécialité. Les enseignants manipulent des informations «sensibles» : corrigé de TP, textes d'examens, ...

Il existe un service administratif qui manipule des données sensibles : notes des élèves, salaires des enseignants, ... Les enseignants n'ont pas accès à ces données.

Le système informatique est constitué par un réseau de machines hétérogènes (UNIX et Windows). Il existe cinq serveurs : un serveur de fichiers, un serveur de messagerie et trois serveurs d'exécution. Il existe un administrateur unique pour tout l'organisme.

Les utilisateurs sont identifiés et authentifiés par l'intermédiaire d'un annuaire unique. On supposera ce mécanisme d'authentification sans faille.

### **Travail à faire**

1. Proposez une politique de sécurité interdisant les accès illicites aux informations sensibles décrites ci-dessus et permettant à chacun(e) :
  - de protéger des informations que lui/elle estime sensibles,
  - de partager des informations avec qui il/elle veut.Si besoin est, vous rajouterez des exigences qui vous semblent importantes. En cas d'exigences contradictoires, vous en éliminerez certaines et justifierez vos choix.
2. Expliquez comment votre politique peut être mise en œuvre (architecture réseau, configuration des systèmes, services et mécanismes de sécurité à mettre en place).