Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Master 2ème année

TMC

Examen février 2015

Durée : 1h30 – Documents autorisés

Technologies NFC et RFID — 5 points

1 – 5pts

a. L'un des usages classiques de la technologie NFC est le contrôle d'accès. Après avoir rappelé pourquoi un contrôle reposant uniquement sur l'identifiant d'un badge n'est pas suffisant pour assurer un bon niveau de sécurité, proposez une solution pour l'améliorer *(2pts)*

b. Un des modes de fonctionnement d'un terminal NFC est le mode HCE. Pour améliorer la sécurité de cette émulation, une solution consiste à utiliser un Secure Element pour stocker les cartes à émuler. Actuellement des propositions sont faites pour fournir des SE dans le cloud.
Expliquez l'intérêt, mais aussi l'impact, que pourrait avoir l'utilisation d'un SE dans le cloud sur un système d'authentification utilisant un protocole de bornage de distance (Distance Bounding Protocol). *(2pts)*

c. Comment peut-on procéder pour effectuer un déni de service sur un Distance Bounding Protocol? *(1pt)*

IBE — 10 points

2 – 4pts

a. Serait-il intéressant de combiner la technique du SUCV et celle de l'IBE tel qu'il est proposé par Jon Callas ?

b. Expliquez comment en utilisant cette combinaison un nœud :
- ◇ obtient ou génère son identité ;
- ◇ peut être joint par un autre au travers du réseau ;
- ◇ est authentifié ;

c. Est-ce que cette combinaison protégerait contre les «*sybil attacks*» ?

d. Quelles propriétés de sécurités offriraient ou non ces identités ?

3 – 6pts

On voudrait pouvoir définir un type de réseau ad hoc utilisant des identités sécurisées et dont l'existence pourrait être limité dans le temps.
Une application serait d'utiliser ce genre de réseau pour les session de travail d'une organisation de normalisation (par exemple dans le domaine des télécommunications) :
- ☐ chaque jour les représentants de chaque entreprise concurrente se réunissent pour échanger et voter pour différentes normes ;
- ☐ il crée/accède au réseau ad hoc permettant des identités sécurisées le matin ;
- ☐ chaque soir le réseau est «détruit» : les identités ne sont plus réutilisables le lendemain.

Questions :

a. Comment peut être mis en œuvre un tel réseau à l'aide d'une PKI ? *(2pts)*

b. Comment peut être mis en œuvre un tel réseau à l'aide d'un IBE ? «off-line» ou «on-line» ? *(2pts)*
*Vous décrirez comment avec chaque proposition une identité est définie le matin et comment elle est «*détruite*» le soir.*

c. Enfin, quelle proposition, du point de vue de l'utilisteur, semble la meilleure en terme de confiance ? *(2pts)*

MANETs — 5 points

4 – 3pts

Protocoles de routage réactif :

a. Pourquoi le chemin de routage n'est-il appris que lors du «RREP» et non du «RREQ» dans le protocole AODV ? *(1pt)*

b. Est-ce que l'utilisation d'un mécanisme de «cache» dans un protocole **réactif** revient à en faire un protocole de routage **proactif** ? Pourquoi ? *Vous justifierez votre réponse*. *(2pts)*

5 – 2pts

Décrivez comment une «*sybil attack*», c-à-d créer des faux nœuds, peut impacter un algorithme de routage comme OLSR et comment un attaquant peut en tirer parti ?