Composition de Sécurité logique - 2005

La composition est décomposée en trois parties :
- Une partie d'étude de cas
- L'utilisation d'une API de sécurité
- Une partie d'analyse des risques

Il est recommandé aux élèves de bien choisir l'ordre des parties selon leurs compétences et rapidités.

Le support de cours est permis. La majeure partie des questions font appel au sens pratique d'ingénieur et le suivi du cours en classe, il est recommandé à l'élève de ne pas perdre son temps pour rechercher les solutions dans le support de cours.

1. Etude de Cas Réel. Transfert d'Argent (12 points)

La société EFT-SA offre la possibilité à des clients à des destinataires de l'argent de la façon suivante :
- Le client se présente à un guichet de EFT-SA, remplit un bordereau papier indiquant :
  - le nom et l'adresse du destinataire bénéficiaire du transfert du fond,
  - optionnellement le numéro du passeport du destinataire,
  - optionnellement une question secrète à laquelle le destinataire doit répondre, la réponse attendue
  - le montant des fonds transmis.
- Selon le montant du transfert, EFT-SA ajoute des commissions de l'ordre de 3%.
- Le client paie le total en liquide au guichetier.
- Le guichetier introduit les diverses informations au niveau d'une application qui génère un numéro unique de transaction.
- Le numéro est donné au client qui doit le transmettre au bénéficiaire.
- Le bénéficiaire peut se présenter à n'importe quel guichet de EFT-SA. Après :
  - Avoir présenté son nom, le numéro de transaction, et son montant,
  - avoir présenté s'il est exigé son passeport,
  - avoir répondu à la question secrète optionnelle,

  le guichetier peut lui payer.

a) Quelle forme proposez vous au numéro de transaction et pourquoi (3 lignes).

EFT-SA veut offrir le même service à des clients occasionnels par le Web. Le paiement se fait en utilisant des cartes de crédit en saisissant le numéro à chaque transaction.

b) Quels sont les risques logiques dans le cas de ce service (nommez trois)? (6 lignes)
c) Quelle est la précaution minimale pour accéder au site du service d'EFT-SA par le Web et pourquoi ? (1 ligne)
d) Comment EFT-SA peut vérifier le numéro de carte de crédit ? (1 ligne)
e) Que doit ajouter EFT-SA au montant à faire payer au client ? (1 ligne)
f) EFT-SA veut limiter les transactions pour les clients occasionnels à 200 USD. Commenter (3 lignes).
g) Définir les règles de filtrage du firewall au niveau du serveur pour les clients se connectant à ce service.

EFT-SA veut offrir le même service à des clients fidèles par le Web. Le paiement se fait en utilisant des cartes de crédit dont le numéro est saisi une fois dans la gestion des cartes du client. Une authentification forte par carte à puce est exigée. Pour séparer les deux types de clients (occasionnels et fidèles) le port 8443 est utilisé pour les clients fidèles.

h) Quelles sont les nouvelles règles de filtrage du firewall ?
i) Quelle est la version de SSL utilisée ?
j) Pour des montant supérieurs à 500 USD une signature supplémentaire est exigée. Pour quelle raison ?
k) Que proposez vous pour que le client sache si le destinataire a bien reçu son argent ?

Les clés RSA utilisées sur les cartes à puce sont de 1024 bits. Elles sont inscrites sous la forme des composantes du théorème des restes chinois (Sp, Sq, p, q, u , v et N).

Rappel :

N = p *q , S : exposant privé, v exposant publique.
Sp = S mod (p-1)
Sq = S mod (q-1)

p2 = (M mod p) exp Sp mod p
q2 = (M mod q) exp Sq mod q

u = (p exp -1 mod q)
alors Signature = p2 + (u * (q2-p2)) mod q * p

l) Définir le mapping de la carte puce .

2. API de sécurité (5 points)

Utiliser les requêtes PKCS11 pour implémenter le chiffrement et signature d'un fichier. Les algorithmes utilisés sont le AES, SHA1 et RSA. N'oubliez pas de mettre les commentaires.

3. Analyse de Risques

Traîter au choix 2 questions sur 4. Toutes les questions n'ont pas la même note compte tenu de la difficulté variable.

a) Est il vrai que la machine la plus sécurisée est la machine qui ne présente aucune connexion et pourquoi ? (Deux Points)
b) Un canular (in english a hoax) est une fausse information transmise à des destinataires leur indiquant par exemple que leur machine est infectée par un virus caractérisé par la présence de certains fichiers. Est-ce que les canulars sont dangereux ou pas et pourquoi ? (Trois Points)
c) Décrypter un message est-il toujours dangereux (pour son destinataire ou propriétaire) et pourquoi? (Trois Points)
d) Les différents organismes postaux offrent des vignettes qui remplacent les timbres. Le prix de l'envoi est imprimé sur chaque vignette en fonction de l'envoi ; la vignette peut être ensuite collée sur l'enveloppe ou le colis. Pour assurer la sécurité de la vignette plusieurs techniques sont utilisées selon les organismes postaux. Analyser et/ou commenter la vignette utilisée par la Poste Allemande. (Cinq Points)