Département d'informatique
Faculté des sciences exactes et des sciences de la nature et de la vie
Université Mohamed Khider, Biskra

Année universitaire 2019/2020.

Sécurité Informatique — Série d'exercices N 2 (L3) (Solutions)

Exercice 1

[Challal 2016]

1. Soit le protocole cryptographique suivant :
   `M1 : B ==> A : B.PKb`
   `M2 : A ==> B : {m}PKb`
   Ce protocole est vulnérable à une attaque de type « man in the middle ». Un intrus "I" peut attaquer ce protocole comme suit :
   ◯ I intercepte `M1`
   I bloque `M1`
   I remplace `M1` par : `M1 : I ==> B : A.PKi`
   I intercepte `M2`
   I bloque `M2`
   I remplace `M2` par : `M2 : I ==> A : {m}PKa`
   √ **I intercepte** `M1`
   I bloque `M1`
   I remplace `M1` **par :** `M1 : I ==> A : B.PKi`
   I intercepte `M2`
   I bloque `M2`
   I remplace `M2` **par :** `M2 : I ==> B : {m}PKb`
   ◯ I intercepte `M1`
   I bloque `M1`
   I remplace `M1` par : `M1 : I ==> A : B.SKb`
   I intercepte `M2`
   I bloque `M2`
   I remplace `M2` par : `M2 : I ==> B : {m}PKb`

2. L'objectif d'un certificat numérique est d'assurer
   ◯ La confidentialité de la signature numérique du porteur du certificat
   √ **L'authenticité de la clé publique correspondante à la clé privée du porteur du certificat**
   √ **La correspondance entre l'identité et la clé publique correspondante à la clé privée du porteur du certificat**
   ◯ L'authenticité de la signature numérique de l'autorité de certification

3. Le protocole SSL/TLS permet d'assurer
   √ **Le contrôle d'intégrité.....(car le protocole utilise le MAC)**
   √ **La confidentialité des échanges entre le client et le serveur.....(le protocole utilise un chiffrement symétrique pour les données éhangées entre le client et le serveur)**
   √ **L'authentification de l'origine de données .....(assurée par le code MAC)**
   ◯ L'authentification du serveur optionnellement....(l'authentification du serveur est plutot obligatoire)
   √ **L'authentification du client optionnellement.....(le client envoie optionnellement son certificat au serveur)**

Exercice 2 (Devoir)

[Challal 2016] Le ministère des finances décide d'automatiser la déclaration des revenus annuels imposables. Il existe une recette des impôts au niveau de chaque mairie, mais vu l'absence d'un réseau privé reliant ces structures administratives, le ministère décide de réaliser l'opération à travers le web. Ainsi, chaque personne physique ou morale concernée (commerçant, agriculteur, entreprise, ...) devrait pouvoir faire sa déclaration de revenus en utilisant un navigateur web. Le ministère met à disposition des citoyens un site web qui collectera les revenus déclarés en vu de les stocker dans une base de données. Le ministère fait appel à votre expertise et vous remet un cahier de charge, dans lequel on peut souligner les points suivants :

(a) Le système de télé-déclaration fiscale doit être conforme à la loi 15-04 sur la certification électronique. Le texte de loi est joint à ce cahier de charge (*cf.* loi 15-04 certification électronique) ;

(b) Les déclarations doivent rester confidentielles ;

(c) Chaque déclarant doit être authentifié avant de procéder à la déclaration ;

(d) Afin de donner une valeur légale aux déclarations, les déclarants doivent signer numériquement leur déclaration ;

(e) Les structures du ministère ne seront pas disposées à recevoir les déclarants. Tout rapprochement nécessaire de l'administration fiscale devrait se faire au niveau des recettes des impôts des mairies.

Questions :

1. Proposez une architecture, à base d'une PKI, pour sécuriser le système de télé-déclaration tout en répondant au cahier de charge du ministère des finances.
2. Citez puis expliquez succinctement comment les protocoles et mécanismes cryptographiques, que vous introduisez, réalisent les impératifs du cahier de charge.
3. Expliquez comment déployer votre système à l'échelle nationale.