Module TR-c8

TD N° 3 – SST/TLS & Certificats

Exercice 1 – Certificats

1. Un responsable a obtenu un certificat X.509 pour un site web auprès d'une autorité de certification. Quel est le but de ce certificat ?
2. Outre la signature de l'autorité de certification, quelles sont les deux informations essentielles que l'on trouve de manière générale dans un certificat ?
3. Lorsque Alice se connecte sur le site web, son navigateur vérifie la validité du certificat fourni. Quelle clef sera utilisée par son navigateur ? comment est-elle obtenue ?

Exercice 2 – Scénarios de sécurité

1. Discuter les scénarios suivants en terme de sécurité :
    - Deux certificats différents sont signés par la même clef privée.
    - Deux certificats différents contiennent la même clef publique.
    - Deux certificats différents qui ont la même signature.

Exercice 3 – SSL/TLS

Le protocole HTTPS est une version du protocole HTTP qui utilise SSL/TLS pour sécuriser les échanges de données. Il est utilisé dans de nombreuses applications web, par exemple les applications bancaires, de commerce électronique ou encore de messagerie sur le Web. HTTPS permet de chiffrer les communications entre le serveur et la machine du client, mais aussi d'authentifier le serveur, voire le client, à l'aide de certificats X.509.

On s'intéresse dans cet exercice à l'interprétation des messages d'erreur pouvant survenir lors d'une connexion à un site web en utilisant le protocole HTTPS. Donner une explication détaillée aux messages d'erreurs affichés par le navigateur dans les deux cas suivants :

1. Figure 1 : connexion au site web **https://gaspar.eplf.ch**
2. Figure 2 : connexion au site web **https://www.airable.com**

Exercice 4 – Chaînes de certification

Alice reçoit le certificat de Bob signé par l'autorité de certification Trent. Malheureusement Alice ne connaît pas la clef publique de Trent. Il se trouve que cette clef (i.e., clef publique de Trent) est certifiée par l'autorité de certification VeriSign (dite racine) dont Alice a entièrement confiance.

1. Dessinez le graphe hiérarchique des différents certificats, en indiquant à chaque fois les clés authentifiées.
2. Dessinez le graphe de la chaîne de confiance qui en résulte. Comment Alice pourra-elle vérifier le certificat de Bob ?
3. Que pouvez-vous dire de la validité de la clef contenu dans le certificat de Bob ?

Exercice 5 – sécurité avec SSH

Alice tente de se connecter à **`machine2`** grâce à SSH. Elle obtient le message suivant :

```
login@machine1 :~> ssh –l Alice machine2
```

The authenticity of host 'machine2 (192.168.3623)' can't be established.

RSA key fingerprint is 3a:1f:23:5e:9c:d4:86:22:33:0d:39:01:28:0b:ea:c5

Are you sure you want to continue connecting (Yes/No)?

1. Expliquer le message et décrire précisément la procédure qu'Alice devra suivre avant de poursuivre la connexion.