TADJER Badr | TRAN Leo | ARRADI Naoufal

M1-APP-LS1

TP3

|  |
| --- |
|  |

**CHIFFREMENT ASYMÉTRIQUE**

1. **Quelle est la version du paquet OpenSSL de votre système ? Où se trouvent les certificats des différents CA (Certification Authority) sur votre environnement ?**

|  |
| --- |
| Sur MacOS, OpenSSL se nomme LibreSSL |
|  |
| Les certificats se situent dans le répertoire /etc/ssl/certs |

1. **Chiffrement asymétrique avec RSA :**
   1. **Générer un couple de clés (publique, privée) pour Alice et sauvegardez-le dans un fichier cle.pem. Quel est le codage utilisé dans ce fichier ?**

openssl genrsa -out cle.pem 2048

Le fichier est codé en base64

* 1. **Comment extraire la clé publique sauvegardée dans cle.pem afin de la stocker dans pub.pem ?**

openssl rsa -pubout -in cle.pem -out pub.pem

* 1. **Bob, qui est en possession du fichier pub.pem, veut chiffrer un message secret et l’envoyer à Alice en utilisant la clé publique d’Alice. Il envoie à Alice le message chiffré. Quelle est la commande à utiliser ?**

openssl rsautl -encrypt -in message.txt -out encrypted\_message.txt -inkey pub.pem -pubin

* 1. **Quelle est la commande qui permet à Alice de déchiffrer le secret en utilisant sa clé privée ?**

openssl rsautl -decrypt -in encrypted\_message.txt -inkey cle.pem

**LES CERTIFICATS ÉLECTRONIQUES**

1. **C’est quoi un certificat électronique et c’est quoi son utilité ?**

Un certificat électronique est un certificat qui certifie qu’une clé publique appartient bien à la personne qui prétend être le propriétaire légitime de cette clé. L’utilité d’un certificat électronique, est d’authentifier une personne et peut également servir pour chiffrer les échanges.

1. **Récupération, visualisation et transcodage de certificats**
   1. **Saisir le script get-cert.sh suivant :**

|  |
| --- |
|  |

* 1. **Expliquer le rôle de la commande s\_client, de la commande openssl et de la commande sed.**

|  |
| --- |
| **s\_client** : connexion à distance vers un hôte en utilisant SSL/TLS. |
| **openssl** : boîte à outils pour la cryptographie et les communications sécurisée. |
| **sed** : la commande sed permet le traitement de fichier,  Ex : supprimer des lignes, afficher le contenu, afficher un certain contenu du fichier, etc… |

* 1. **Exécuter ce script afin de récupérer le certificat d’un site Internet de votre choix, puis visualiser ce certificat (qui est au format PEM).**

|  |
| --- |
|  |

* 1. **Convertir ce certificat du format PEM au format DER. C’est quoi la différence entre ces deux formats ? quels sont les autres formats possibles ?**

openssl x509 -in efrei.pem -out efrei.der -outform DER

Les fichiers au format PEM comportent un entête et un pied de page, les données entres sont en base 64.

Les fichiers au format DER, contiennent des certificats codés en binaire.

Les autres formats sont PEM, DER, P7B, PFX.

1. **Création d’un certificat x509 auto-signé : créer un couple de clés publique/privée, puis créer une requête de certificat. Utiliser ensuite ces deux informations pour générer un certificat auto signé.**

Créer un couple de clés publique/privée : (cle.pem)

openssl genrsa -out cle.pem 2048

Requête de certificat et certificat auto-signé : (ca.crt)

openssl req -new -x509 -key cle.pem -out ca.crt -days 1095

**TESTER LES LIAISONS TLS/SSL**

Le paquet OpenSSL embarque avec lui un serveur SSL. Nous allons l’utiliser pour comprendre le fonctionnement du protocole SSL.

1. Commencer par lancer le serveur SSL d’OpenSSL (commande s\_server) sur le port 10000 en utilisant le certificat autosignée que vous avez généré dans l’étape précédente ainsi que la clé
2. Lancer Wireshark pour capturer le trafic, puis tester l’accès à ce serveur à partir d’un navigateur web graphique ou bien textuel (lynx). Analyser tout l’échange SSL et expliquer toutes les étapes opérationnelles du protocole SSL.
3. C’est quoi la notion de suite de chiffrement présente dans le message Client Hello ? Est-ce que l’ordre des propositions de ces suites de chiffrement est important ? Afficher la liste des suites de chiffrement d’OpenSSL.
4. Afficher la trace d’une session SSL avec le client de test incorporé dans openssl.  
   C’est quoi le premier message chiffré ? à quoi sert-il ? (Faire une petite recherche pour répondre à cette question).
5. En utilisant OpenSSL, accéder à un site SSL sur Internet. Quelle est la suite de chiffrement choisie ?
6. Audit d’un site SSL :
   1. Télécharger le script testssl.sh. De préférence, faites-le en le clonant à partir de github comme c’est indiqué sur le site de téléchargement.
   2. Tester la robustesse d’un serveur web en utilisant ce script
7. Installer un serveur Apache, Activer le module ssl ainsi que le site virtuel ssl par défaut. Ensuite tester sa robustesse avec le script testssl.sh. Faites les changements nécessaires pour durcir la configuration de votre site.