IUT DE COLMAR

R401 – Infrastructure de sécurité

Année 2022-23

TP1/2 - Chiffrement et TLS

MARTIN BAUMGAERTNER

10 juin 2023

Table des matières

1 TP1 - Chiffrement et PKI

1.1 Chiffrement

1.1.1 Permutation

Question 1

Le message déchiffré que j'obtiens est `MAITRE CORBEAU SUR UN ARBRE PERCHEX`
Voici ce que j'ai fait pour obtenir ce message :

1. J'ai créé une liste des lettres de l'alphabet, dans l'ordre.
2. J'ai créé une deuxième liste, contenant les nombres 1 à 6.
3. J'ai apparié les lettres et les chiffres des deux listes, dans l'ordre spécifié dans la clé.
4. J'ai utilisé les chiffres pour créer une nouvelle séquence de lettres, en remplaçant chaque lettre du message d'origine par la lettre qui lui correspond dans la nouvelle séquence.
5. J'ai supprimé tous les espaces de la chaîne obtenue.

1.1.2 Substitution

Question 2

Voici le message que j'ai trouvé `UN SECRET`

1.1.3 Diffie-Hellman

Question 3

J'ai obtenu `K = 117`

1.1.4 Chiffrement symétrique AES

Question 5

Voici le résultat que l'on obtient en base64 :

```
U2FsdGVkX1+QhnAugHjdc6bhMEMibXxWGQSE6ZKN56o=,
```

L'option "-nosalt" lors d'une commande openssl permet de ne pas rajouter de valeur aléatoire au code avant son hachage. En effet "salt" rajoute une valeur aléatoire pour renforcer le code/mot de passe.

1.2 PKI

1.2.1 Création du Certificat Racine (ou CA) et de sa clé privée.

CA signigie **C**ertificate **A**uthority. C'est une entité qui émet des certificats numériques.

1.2.2 Lecture du certificat

Ci-dessous, un tableau avec les différents **champs** et **fonctions** du certificat.

Champ	**Fonction**
Version	Version du certificat
Serial Number	Numéro de série du certificat
Signature Algorithm	Algorithme de signature
Issuer	Entité qui a signé le certificat
Validity	Période de validité du certificat
Subject	Entité à qui le certificat est destiné
Subject Public Key Info	Informations sur la clé publique
X509v3 extensions	Extensions du certificat

1.2.3 Contenu du CSR

CSR signifie **C**ertificate **S**igning **R**equest. C'est une requête de signature de certificat.
Voici ci-dessous un tableau listant les **champs** et **fonctions** du CSR.

Champ	**Fonction**
Version	Version du CSR
Subject	Entité à qui le certificat est destiné
Subject Public Key Info	Informations sur la clé publique
X509v3 extensions	Extensions du certificat

1.2.4 Création de la liste de révocation

CRL signifie **C**ertificate **R**evocation **L**ist. C'est une liste de révocation de certificats.

2 TP2 - TLS Authentification

2.1 Openssl

2.1.1 Openssl et firefox

Question 1

Pour eviter d'avoir des messages d'erreurs et pour que firefox accepte de se connecter au serveur sans rajouter des exception de sécurité, il faut :

— que le certificat du serveur soit signé par une autorité de certification reconnue par firefox.
— correctement configurer le serveur web en utilisant le port HTTPS (443)

Question 2

L'interface sur laquelle est faite la capture dépend de notre machine sur la mienne il s'agit de l'interface nommée `eth0`.
Le filtre utilisé afficher les paquets propre à **TLS** est tout simplement le filtre `tls`.

Question 4

Ci après le schéma du handshake du protocole TLS1.2 entre le client et le serveur :

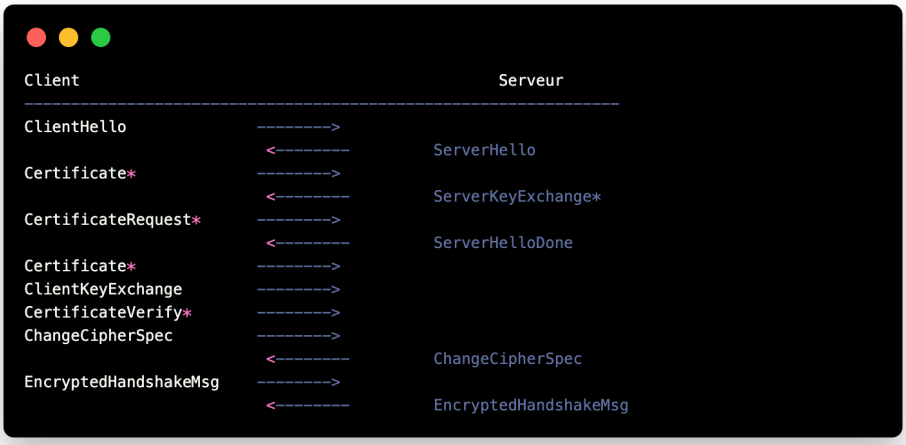

FIGURE 1 – Handshake TLS1.2

2.2 Vérification OCSP

Question 5

L'erreur remontée par le navigateur indique que le certificat est révoqué.

Question 6

Une fois avoir exporté l'index des certificats et en relançant le responder OCSP nous avons bien la page internet qui s'affiche.

2.3 Vérification OCSP stapling

Question 7

Non, cela ne règle pas les problèmes de latence et de confidentialité. Cette variante d'OCSP permet au serveur web de fournir la réponse de vérification dans un nouveau message du Handshake, elle ne règle pas les problèmes inhérents à OCSP. Ces limitations ont conduit les navigateurs modernes à désactiver la vérification OCSP par défaut pour améliorer l'expérience utilisateur.

2.4 Apache

Question 9

Pour utiliser mes certificats j'ai du indiqué l'emplacement de mon certificat finissant par l'extension **.crt** dans le fichier **default-ssl.conf**, à la ligne **SSLCertificateFile**. Et, à la ligne **SSLCertificateKeyFile** j'ai dû indiquer l'emplacement de ma clé privé.

Voici donc les lignes :
— `SSLCertificateFile /etc/ssl/mondomaine/mondomaine.crt`
— `SSLCertificateKeyFile /etc/ssl/mondomaine/mondomaine.key`

Il ne faut pas oublier de rédemarrer Apache pour les modifications soient prises en compte avec la commande `sudo service apache2 restart`