TD 5 Protocole TLS

Documentation

> TLS v1.1 : http://tools.ietf.org/html/rfc4346

> TLS v1.2 : http://tools.ietf.org/html/rfc5246

> TLS v1.3 : https://tools.ietf.org/html/rfc8446

Question 1

Dans quel contexte utilise-t-on le protocole TLS ?

Suites d'algorithmes

Question 2

Décrivez sommairement les grandes étapes du protocole TLS, depuis la tentative de connexion du client jusqu'à l'échange de messages chiffrés.

Question 3

A partir de la documentation de TLSv1.3, donnez la définition d'un "cipher suite" et précisez ceux qui doivent OBLIGATOIREMENT être implémentés et ceux qui sont RECOMMANDÉS. Dans chaque cas, vous préciserez le rôle de chaque algorithme (chiffrement, fonction de hachage, $\cdots$) et les propriétés de sécurité de l'algorithme responsable du chiffrement (i.e. confidentialité, intégrité, authentification, non-répudiation, $\cdots$).

Question 4

Même question pour TLSv1.2 (vous vous restreindrez aux cipher suites obligatoires). Attention, la définition d'un "cipher suites" est légèrement différente.

Échange de clés

Question 5

Précisez les extensions obligatoires dans TLSv1.3 et précisez le rôle des extensions 2, 3, 5 et 6. Concluez sur l'algorithme d'échange de clé utilisé dans TLSv1.3.

Question 6

Comparez l'algorithme d'échange de clé choisi pour TLSv1.3 à ceux autorisés pour TLSv1.2. A votre avis, pourquoi ce choix ?

Question 7

Dans TLSv1.2, dans le cas de l'utilisation de l'échange de clé basé sur RSA, quel schéma de remplissage (padding) est utilisé dans le standard ? Discutez sa sécurité vis-à-vis d'un jeu d'indistinguabilité IND-CPA et IND-CCA2. Quelle évolution pourriez-vous apporter à cette construction pour renforcer sa sécurité ?

Question 8

Dans TLS v1.2, comparez les cipher suites RSA, DHE_RSA et DH_RSA, notamment l'algorithme responsable de l'échange de clé et l'algorithme utilisé pour la vérification des certificats. Quelles suites permettent la confidentialité persistante ?

Dérivation de clés

Question 9

Donnez la définition du PRF de TLSv1.2 et son rôle.

Question 10

A votre avis, pourquoi avoir préféré HKDF au PRF de TLSv1.2 pour TLSv1.3 ? Vous pouvez comparer la structure interne des deux algorithmes.

Question 11

Donnez la différence entre pre-master secret et master secret dans TLSv1.2, et donnez l'algorithme qui permet de passer du premier au deuxième.

Question 12

Donnez la méthode qui permet de générer les paramètres suivants dans TLSv1.2 :

> client write MAC key

> server write MAC key

> client write encryption key

> server write encryption key

> client write IV

> server write IV

A quoi servent-ils ?

Contrôle d'intégrité

Question 13

Donnez la méthode utilisée dans TLSv1.2 pour garantir l'intégrité des messages. Comparez à TLSv1.3.

Question 14

Dans TLS v1.2, étudiez la composition d'un chiffré dans le cadre d'un chiffrement symétrique en mode CBC. Est-ce une construction Encrypt-and-MAC, MAC-then-Encrypt ou Encrypt-Then-MAC ? Listez les avantages et inconvénients d'une telle construction. Comparez à TLSv1.3.

Gestion du vecteur d'initialisation

Question 15

Après génération, est-il autorisé de garder le même IV (ou Nonce) tout le long de la communication dans TLSv1.2 ? Est-ce un choix judicieux ?

Question 16

Comparez la gestion de l'IV dans les trois dernières versions de TLS (i.e. 1.1, 1.2, 1.3) et remplissez un tableau récapitulatif précisant s'il est secret, aléatoire et/ou personnalisable. Concluez sur l'évolution de la gestion de l'IV dans le standard.

Conclusion

Question 17

A partir des questions précédentes, faites le bilan des évolutions en terme de cryptographie entre TLSv1.2 et TLSv1.3.