Nom : Rebini
Prénom : fatma

21605369

mars 2018

UVSQ – M2 SeCReTs 2018
Contrôle de connaissances
Cours sur la sécurité des réseaux Wi-Fi

NB : les feuilles d'énoncé seront utilisées pour inscrire la totalité des réponses. Pour certaines des questions de cette partie, il convient de cocher non pas une, mais plusieurs réponses exactes. Vous pouvez ajouter une courte justification écrite sous votre réponse, si cela vous semble nécessaire. La consultation du cours est autorisée.

1. Combien de canaux fréquentiels Wi-Fi distincts de 20 MHz sont définis dans la bande ISM à 2,4 GHz ?

- ☐ Un seul
- ☐ 8
- ☑ 14
- ☐ 26

2. Sur quelle(s) autre(s) bande(s) de fréquences peut (ou peuvent) fonctionner certaines versions de la norme Wi-Fi (par exemple 802.11a, 802.11ac, 802.11ad alias *WiGig*, …) ?

- ☐ 433 MHz
- ☐ 900 MHz
- ☑ 5 GHz
- ☑ 60 GHz

3. Quelle est la portée d'un signal radio Wi-Fi (sur la bande ISM à 2,4 GHz), en ligne directe et sans obstacle,

avec des équipements standards et telle qu'évoquée dans la norme 802.11 ?

- ☐ Moins de 10 mètres
- ☑ Une centaine de mètres
- ☐ Plusieurs kilomètres
- ☐ Plusieurs milliers de kilomètres

lorsque l'on dispose d'émetteurs, récepteurs et d'antennes de très bonne qualité ?

- ☐ Moins de 10 mètres
- ☐ Une centaine de mètres
- ☑ Plusieurs kilomètres
- ☑ Plusieurs milliers de kilomètres

4. A propos du mode moniteur (ou *monitor*) des modems Wi-Fi et de leur pilote (*driver*) :

Quelle est la particularité du mode moniteur ?

- ☐ Il permet de recevoir les trames radio 802.11 de toutes les bandes de fréquences en même temps
- ☐ Il permet de recevoir toutes les trames radio 802.11 d'un canal fréquentiel donné
- ☐ Il permet de faire fonctionner son terminal en mode point d'accès
- ☐ Il permet d'accéder à plusieurs points d'accès Wi-Fi simultanément

Quel(s) système(s) d'exploitation supporte(nt) nativement le mode moniteur de très nombreux modems Wi-Fi ?

- ☐ MacOS X
- ☐ OpenSolaris
- ☐ Windows 10
- ☐ Linux
- ☐ Android

5. Quelle entité produit et maintient les spécifications techniques des réseaux Wi-Fi ?

- ☐ La Wi-Fi Alliance
- ☐ L'ITU-T (International Telecommunications Institute)
- ☐ L'IEEE (Institute of Electrical and Electronics Engineers)
- ☐ Le 3GPP (3rd Generation Partnership Project)

6. Le protocole WEP (*Wired Equivalent Privacy*) a pour rôle d'assurer la confidentialité et l'intégrité des communications des utilisateurs. De nombreuses faiblesses ont cependant été révélées à son sujet, dès 2001.

Quel algorithme de chiffrement à flot est utilisé pour produire des masques (ou *keystream*, suites chiffrantes) qui permettent d'assurer la confidentialité des données transmises ?

- ☐ AES en mode CCMP
- ☐ RC4
- ☐ A5/1

Quel algorithme est utilisé pour produire des sommes de contrôle (*checksum*) qui permettent au récepteur de vérifier l'intégrité des trames de données démodulées?

- ☐ SHA-1
- ☐ MD5
- ☑ CRC-32

Quelles sont les conditions favorables pour espérer casser une clé WEP rapidement ?

- ☑ Lorsqu'un utilisateur légitime du réseau Wi-Fi y est connecté et échange des trames de données que l'attaquant peut acquérir
- ☐ Lorsque l'attaquant dispose de tables précalculées (*rainbow tables*) à partir de très nombreuses clés WEP possibles
- ☐ Lorsque l'attaquant est à proximité du point d'accès, facilitant l'injection de trames Wi-Fi spécifiquement forgées

7. Quels est l'algorithme de chiffrement défini dans la norme 802.11i dès 2003, correspondant au profil de sécurité WPA, et facilitant la transition avec WEP ?

- ☑ AES en mode CTR (ou mode compteur)
- ☐ TKIP
- ☐ 3DES en mode CBC-MAC
- ☐ Michael

Quel est l'algorithme de chiffrement et de contrôle d'intégrité défini dans la norme 802.11i dès 2003, correspondant au profil de sécurité WPA2 ?

- ☐ SHA-1
- ☐ TKIP
- ☑ AES en mode CCMP
- ☐ 3DES en mode CCMP

8. Pour pouvoir déchiffrer les trames Wi-Fi échangées entre un terminal légitime et un point d'accès configuré en WPA2 avec une authentification WPA-PSK (utilisant une *passphrase*), de quoi l'attaquant a-t-il besoin ? Pourquoi ?

- ☐ Du SSID diffusé par le point d'accès
- ☐ De la capture des échanges d'authentification WPA-PSK préliminaires (utilisant le protocole EAP) entre le terminal et le point d'accès
- ☐ De la *passphrase* WPA-PSK configuré sur le point d'accès
- ☐ Il n'est pas possible de déchiffrer les trames Wi-Fi protégées par WPA2

9. Parmi les protocoles de sécurité suivants, quel est celui ou quels sont ceux qui protègent l'intégrité de l'adresse MAC de l'émetteur d'une trame de données ?

- ☐ WEP
- ☐ TKIP
- ☑ AES-CCMP

10. Depuis plusieurs années, le protocole WPS (*Wi-Fi Protected Setup*) est très largement déployé sur les points d'accès Wi-Fi.

A quoi sert-il ?

- ☐ Remplacer l'authentification WPA-PSK qui est trop complexe
- ☑ Permettre la configuration d'une configuration WPA-PSK sur un terminal sans nécessiter de clavier et / ou d'écran (le terminal peut être un objet connecté, par exemple une montre)
- ☐ Chiffrer la connexion Wi-Fi sans passer par une étape préalable d'authentification mutuelle entre terminal et point d'accès

Le mode par défaut consiste à saisir sur le terminal un code PIN de 8 digits inscrits au dos du point d'accès Wi-Fi. Est-ce suffisamment sécurisé, et pourquoi ? Combien un attaquant doit-il tester de combinaisons avant de trouver le code PIN WPS du point d'accès ? Expliquer.