INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

4A STI

Réseaux non filaires

Examen mars 2015

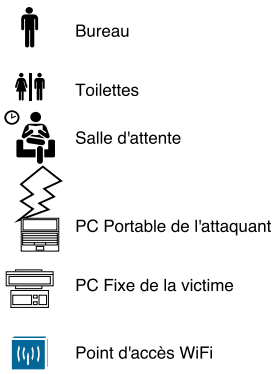
Durée: 1h — Documents autorisés & Calculatrice avec logarithme

Communication sans fil — (6 points)

1 – 6pts Un attaquant essaye d'**injecter** des paquets WiFi malveillants sur l'ordinateur de la victime.

Il n'a pas accès directement au bureau de la victime, mais il peut accèder librement avec son PC portable, à une autre partie du bâtiment composée de :

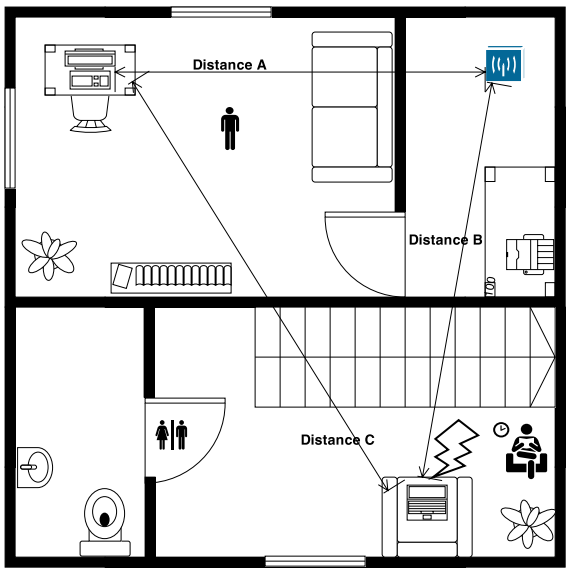
- une salle d'attente avec un fauteuil dans lequel il peut s'installer sans éveiller les soupçons ;
- des toilettes où il peut également séjourner, mais moins longtemps ;



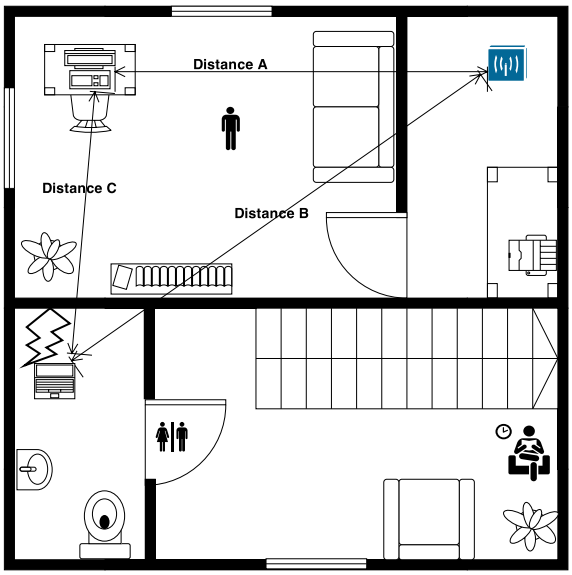
Suivant le placement de l'attaquant, on détermine trois distances :

- distance «A» : du PC de la victime installé sur un bureau au point d'accès WiFi situé dans l'annexe du bureau ;
- distance «B» : du PC portable de l'attaquant au point d'accès WiFi ;
- distance «C» : du PC de la victime au PC portable de l'attaquant ;

Voici les deux placements de l'attaquant :



Version «SA»



Version «WC»

Les murs ont les caractèristiques suivantes :

- celui séparant le PC de la victime du point d'accès induit une atténuation de -12dB ;
- celui separant les WC du bureau de la victime induit une atténuation de 20dB à cause du revêtement en carrelage et de la présence de tuyaux en cuivre pour l'alimentation en eau ;
- celui séparant la salle d'attente du bureau : -12dB.

Les caractéristiques des composants WiFi du PC de la victime et du point d'accès sont les suivantes :

- la puissance de transmission, «*TX Power*», est de 20dBm pour les deux ;
- le gain de l'antenne du PC et du point d'accès est de 2dBi ;
- la perte due à la connexion de l'antenne est de -0,5dB pour le PC de la victime, et de -1dB pour le point d'accès (son antenne est connectée par un câble) ;

Pour la carte WiFi de l'attaquant :

- la puissance de transmission est de 20dBm ou 30dBm, son antenne est de 2dBi et son «cable loss» est de -0.5dB.

Enfin, les contraintes pour le WiFi sont les suivantes :

- on considère qu'une valeur de «*link margin*» supérieure à 20dB est nécessaire pour assurer un échange correct de paquet ;
- suivant le débit que l'on veut obtenir, et la modulation nécessaire pour l'atteindre, la sensibilité du récepteur varie suivant le tableau suivant :

Mbps	Type	PER	dBm
54	OFDM	10%	-68
48	OFDM	10%	-68
36	OFDM	10%	-75
24	OFDM	10%	-79
18	OFDM	10%	-82
12	OFDM	10%	-84

*La modulation OFDM, «Orthogonal frequency-division multiplexing», combine différents «*sous-canaux*» qui corresponde chacun à une faction de la bande passante du canal WiFi utilisé (sur chacun de ses sous-canaux une modulation différente peut être utilisée afin d'optimiser les performances).*

Ici, nous ne considérerons que les différentes valeurs de débit associées aux différentes valeurs de sensibilité du récepteur.

Questions :

a. Sachant que la distance «A» est de 8m, quel débit maximum peut être atteint entre le PC de la victime et le point d'accès ? *(1pt)*

b. Si l'attaquant essaye d'injecter des paquets vers le PC de la victime **avec le même débit que la victime partage avec le point d'accès**, est-ce qu'il peut le faire : *(2pts)*
   - ◇ en version WC, avec une distance «C» de 6m, pour une puissance TX de 20dBm ? de 30dBm ?
   - ◇ en version SA, «salle d'attente», avec une distance «C» de 15m, pour une puissance TX de 20dBm ? de 30dBm ?

c. Un **outil de détection des injections** a été installé sur le point d'accès. *(2pts)*
   Est-ce qu'il pourra détecter une attaque :
   - ◇ en version WC et avec une distance «B» de 13m ?
   - ◇ en version SA et avec une distance «B» de 14m ?

   Si oui, est-ce que l'on pourra aussi savoir où se trouve l'attaquant ?

d. Est-ce que l'emploi d'une **antenne directionnelle** «yagi» d'un gain de 14dBi permettrait de découvrir toutes les attaques ainsi que l'emplacement des attaquants ? *(1pt)*

Composant radio embarqué nRF24L01 — (2 points)

2 – 2pts

a. Comment peut-on faire du «multiplexage spatial» avec le composant nRF24L01 ?
Est-ce que le choix du débit influence ce «multiplexage» ?

b. Comparez le MAC, «*Medium Access Control*», du composant nRF24L01 à celui du WiFi pour la gestion des erreurs : quel est le plus performant ?

MANet — (2 points)

3 – 2pts

a. Est-ce que l'utilisation d'**antenne directionnelle** affecte le fonctionnement des algorithmes de routage proactifs et/ou réactifs ?
Quels en sont les effets ?

b. L'utilisation d'un algorithme de **routage réactif** est-elle possible dans le cadre de l'utilisation du composant nRF24L01 ?
Expliquez comment vous feriez cette adaptation ?
Pourrait-elle offrir la sécurité des échanges par chiffrement ?

Rappel

$$log_{10}(x) = \frac{ln(x)}{ln(10)}$$