République Tunisienne

Ministère des Technologies de la Communication

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Les réseaux sans fil (WiFi)

Public Cible	Date de Publication	Date de Révision	Version
Simple Utilisateur	Mai 2008	Mai 2009	02

Introduction

Un réseau sans fil est un réseau dans lequel au moins deux terminaux sont capables de communiquer entre eux grâce à des signaux radioélectriques. Les réseaux sans fil ne sont pas tous récents, mais avec le développement de l'informatique et des systèmes d'information, la technologie est venue au besoin primaire de l'homme : la mobilité et la facilité. Ces réseaux dits aussi wireless sont de plusieurs sortes : WiFi (Wireless Fidelity), BlueTooth, BLR (Boucle Locale Radio), UMTS (Universal Mobile Telecommunications System).

Un réseau sans fil est un réseau dans lequel au moins deux terminaux sont capables de communiquer entre eux grâce à des signaux radioélectriques.

L'avantage des réseaux à technologie sans fil d'un point de vue esthétique réside dans le fait que l'on n'a plus besoin de relier physiquement les équipements par câble, ce qui permet aux nombreux utilisateurs de s'affranchir des longs câbles encombrants, favorisant ainsi, de bénéficier des avantages de la mobilité et de la facilité. Cet atout induit des vulnérabilités de sécurité majeures. Ainsi, et avant de se lancer dans la mise en place d'un réseau à technologie sans fil (WiFi, Bluetooth, ..), il faut être conscient des risques inhérents à cette technologie.

Ces réseaux sont de plusieurs sortes dont on cite par exemple: WiFi (Wireless Fidelity), BlueTooth, BLR (Boucle Locale Radio), UMTS (Universal Mobile Telecommunications System).

Les différentes normes du réseau sans fil :

La norme IEEE 802.11 est la norme initiale qui est un standard international du réseau local sans fil. Cette norme a permis de répondre aux besoins d'un marché de masse, grand public et professionnel, avec des coûts abordables, en décroissance continue, et des matériels à la fiabilité éprouvée.

Elle est subdivisée en plusieurs révisions caractérisées par leur débit, dont on cite principalement les deux versions majeures:

- ☑ 802.11 b à 11 Mbit/s.
- ☑ 802.11 g à 54 Mbit/s.

Présentation du WiFi (802.11) :

La norme 802.11 utilise deux types de couches basses du modèle OSI qui sont :

- ☑ La couche physique qui est la première couche de ce modèle (elle permet la conversion entre bits et signaux électriques ou optiques à travers trois types de codage différents).
- ☑ La couche liaison de données qui gère les communications afin d'assurer une liaison sans fil utilisant des ondes radioélectriques.

Cette dernière est composée de deux sous-couches à savoir : la couche de contrôle de la liaison logique appelée aussi Logical Link Control (LLC) et la couche de contrôle d'accès au support dite Media Access Control (MAC).

Les différents types de technologies sans fil :

On peut classer les réseaux sans fil dont la norme 802.11 en particulier, en quatre volets possibles :

- Les réseaux personnels sans fil : Wireless Personal Area Network (WPAN)
- Les réseaux locaux sans fil : Wireless Local Area Network (WLAN)
- Les réseaux métropolitains sans fil : Wireless Metropolitan Area Network (WMAN)
- Les larges réseaux sans fil : Wireless Wide Area Network (WWAN)

Les différents modes de fonctionnement du WiFi :

Afin de connecter deux ou plusieurs ordinateurs via la technologie du sans fil, deux modèles de déploiement se présentent :

- Le mode infrastructure : c'est le résultat de la réalisation d'une connexion directe (sans un élément tiers) entre les ordinateurs équipés d'une carte réseau WiFi.
- Le mode Ad-Hoc : il consiste à implanter, dans la zone qui doit être couverte par le réseau, un ou plusieurs points d'accès à intervalle régulier qui agissent comme des concentrateurs.

Les principaux risques qui touchent la sécurité du WiFi :

L'interception de données que peut effectuer toute personne se trouvant dans le rayon de portée d'un point d'accès en écoutant toutes les communications circulant sur le réseau, le détournement de connexion afin d'obtenir l'accès à un réseau local ou à Internet, le brouillage des transmissions en produisant des interférences au moyen des signaux radio émis et les dénis de service (envoi d'informations afin de perturber volontairement le fonctionnement du réseau) constituent les principaux risques que peut subir un réseau sans fil faute à sa mauvaise protection.

Comment sécuriser son réseau WiFi ?

Dans le but de sécuriser votre WiFi, il suffit d'appliquer quelques mesures de sécurité dont on cite principalement :

1/ Changer le mot de passe utilisateur de votre routeur WiFi :

Puisque l'utilitaire de configuration du routeur est sécurisé par un nom d'utilisateur et un mot de passe, il faut donc commencer par changer ce dernier. Pour y accéder, il suffit de taper l'adresse IP de votre routeur dans le navigateur Internet (par exemple : 192.168.1.1) et de sélectionner l'option adéquate.

2/ Définir le nom de votre réseau (SSID) :

Tout réseau WiFi a un nom. D'où, il serait impératif de changer ce nom en évitant qu'il soit trop simple, de le cacher à la vue des utilisateurs malintentionnés et de cocher la case correspondante à la désactivation de la diffusion du nom SSID pour qu'il n'apparaisse pas dans la liste des connexions possibles de vos voisins.

3/ Activer le cryptage de votre réseau (clef de sécurité) :

Deux types de cryptage de donnée existent actuellement : WEP (Wired Equivalent Privacy) et WPA (Wi-Fi Protected Access), et le choix de la technique à adopter dépend du matériel disponible. Il sera donc utile de crypter votre réseau sans-fil pour restreindre l'accès qu'aux utilisateurs disposant de votre clef numérique.

4/ Filtrer les adresses MAC :

Les appareils (PC ou PDA) connectés à un réseau WiFi disposent d'une carte réseau équipée d'une adresse spécifique appelée l'adresse. Dans l'utilitaire de configuration de votre routeur, il faut activer l'option de filtrage puis saisir les adresses

MAC de chacun de vos appareils afin que seuls ces appareils puissent accéder au réseau.

5/ Configurer les machines WiFi :

Afin que tout puisse bien fonctionner, il faut faire correspondre les données rectifiées tels que le nom SSID et la clef numérique de cryptage pour que les appareils puissent se connecter au routeur et à l'Internet.

6/ Activer le partage de fichiers :

Pour pouvoir accéder aux fichiers des différents ordinateurs connectés en WiFi, il est primordial d’avoir l’option partage de fichiers activé.