



# Présentation synthétique

## La sécurité des réseaux sans fil

Les réseaux sans fil sont aujourd'hui en pleine expansion et le nombre de projets de déploiement révèle l'avenir prometteur de cette technologie. Mais l'ombre de l'insécurité plane sur ce dessein et l'utilisation de ce type d'infrastructure ne doit se faire que dans le cadre d'une politique de sécurité précise et adaptée.

Une référence actuelle pour la mise en place de tels réseaux est la norme IEEE 802.11b dite Wi-Fi. En France, l'Autorité de Régulation des Télécommunications (ART) a indiqué les restrictions réglementaires d'utilisation de ces réseaux<sup>1</sup>. La grande particularité du Wi-Fi est d'être un système rapide à déployer, pour un coût apparemment raisonnable. En effet, il suffit pour constituer un réseau local sans fil (WLAN) d'équiper les postes informatiques d'un adaptateur 802.11b et si nécessaire, d'installer dans les locaux des points d'accès. Ce type de réseau, aussi appelé Réseau Local Radioélectrique (RLR), utilise donc des ondes radio pour véhiculer des données entre les postes.

**Les applications sont multiples puisqu'elles permettent aussi bien la constitution de réseaux privés et fermés que la mise en place de réseaux publics et ouverts. Sur ce second point, les choses sont actuellement en pleine évolution. L'ART vient en effet d'autoriser l'utilisation de bornes de réseaux radio-électriques pour la fourniture au public de services Internet haut débit, en particulier dans les lieux de passage ("hotspot").**

### 1- Risques

Les avantages annoncés du Wi-Fi restent à relativiser au regard de ses nombreuses faiblesses et vulnérabilités<sup>2</sup> en matière de disponibilité des liaisons, d'intégrité des messages et de confidentialité des échanges.

Le Wi-Fi est très sensible au brouillage. Cette vulnérabilité est intrinsèque à toutes les techniques de réseaux sans fil, techniques qui se prêtent aux attaques en déni de service sur les équipements du réseau, voire à la destruction physique de ces équipements dans le cas de bruits créés artificiellement dont la puissance dépasserait les tolérances admises.

S'y ajoutent des problèmes de saturation de fréquence ou de bande passante lorsque de trop nombreux terminaux sont connectés. Dans certaines conditions, le débit peut chuter considérablement, même sur des courtes distances dépourvues d'obstacles.

Par ailleurs, il est actuellement possible d'écouter et/ou de s'introduire dans un réseau radio d'établissement depuis la rue, à l'aide d'un simple ordinateur portable équipé d'une carte 802.11b et d'un logiciel spécialisé disponible sur Internet. Ceci permet d'écouter des transmissions de données, voire de les falsifier, portant ainsi atteinte à la confidentialité et à l'intégrité des échanges. Il est également important de préciser que l'option de chiffrement proposée, le WEP (Wired Equivalent Privacy), ne remplit pas les garanties de sécurité attendus ; des outils libres ou gratuits sont à disposition sur Internet pour passer outre cette protection peu efficace.

<sup>1</sup> <http://www.art-telecom.fr/communiqués/communiqués/2002/07-11-2002.htm>

<sup>2</sup> <http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002.pdf>



Malgré tous les avantages que représente l'installation d'un réseau sans fil, il est important de prendre conscience des dangers qu'il engendre, car la responsabilité juridique de l'exploitant peut être rapidement engagée. Dès lors, il devient nécessaire de prendre des mesures aptes à protéger l'installation, ses contenus et de prendre en compte le coût induit par cette sécurisation.

## 2- Planification et organisation

La mise en place d'un réseau sans fil doit être réalisée par un spécialiste. C'est un projet à part entière qu'il convient de bien étudier; pour cela un planning doit être clairement défini et un chef de projet nommé. Ce dernier devra, en particulier, analyser les risques sur le plan de la sécurité et prévoir la formation des techniciens et administrateurs de son équipe.

Cette planification doit passer par l'étude des divers aspects relatifs à la mise en place d'un réseau sans fil ainsi que par l'organisation de la gestion, voire de la surveillance de l'exploitation.

## 3- Protection physique des matériels et des sites

Il est nécessaire de prendre en compte, lors du déploiement d'un réseau, la sécurité physique des équipements et des sites. Le choix du périmètre d'implantation, le nombre et la nature des installations dépendront notamment de l'analyse des paramètres suivants :

- étude environnementale (risque d'inondation, foudre...);
- accessibilité du site d'implantation (en particulier protection des bornes);
- caractérisation et contrôle de la propagation du signal sur le site;
- étude des moyens de secours à mettre en œuvre;
- ...

La protection physique nécessite un contrôle anti-intrusion des accès aux locaux où les matériels de connexion seront installés.

## 4- Chiffrement, authentification

Que la protection physique des données au regard de la confidentialité soit recherchée ou non, le recours à une authentification forte et un chiffrement efficace pour la liaison comme pour le réseau est nécessaire. Ceci exclut donc de tout faire reposer sur la seule utilisation du WEP, (un préalable) et demande de recourir à des solutions complémentaires (dont IPSEC –Internet Protocol Security).

Par ailleurs, l'authentification forte (sans mots de passe réutilisables) des usagers autorisés à se connecter permet de limiter les accès frauduleux.

La plupart des réseaux filaires utilisent très peu de moyens techniques sûrs pour réaliser l'authentification des utilisateurs et assurer la confidentialité des données. Cette non mise en œuvre de moyens cryptographiques, pourtant existants, fait courir un risque qui peut rester maîtrisé dans le cas de réseaux filaires, mais le passage à une technologie sans fil augmente ce risque de façon très conséquente.

Pour en savoir plus, vous pouvez vous référer au document intitulé « Recommandations sur la sécurisation des réseaux sans fil ».