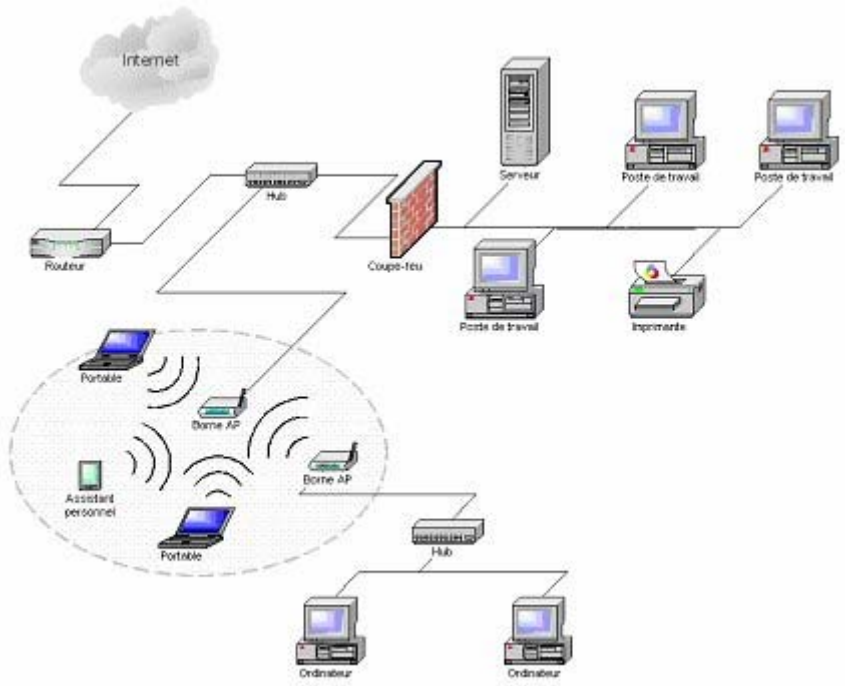
Réseaux sans fil : menaces, enjeux et parades

1. Introduction

Le présent document a un double objectif : d'une part sensibiliser les entreprises et les administrations aux risques inhérents au déploiement d'un réseau sans fil (RSF) de type 802.11b et d'autre part, présenter les solutions qui permettent d'augmenter la sécurité pour ce mode de connexion. Ce document ne traite pas des autres normes, telles que : 802.11a, 802.11i, 802.1x, Hiperlan, etc. ni des infrastructures personnelles ou des *hot spots*.

2. Infrastructure

Le RSF de type 802.11b repose sur une norme (cf. annexes). Il s'agit d'un protocole de transmission radio de proximité sur des canaux préétablis.



Une infrastructure typique qui combine ad hoc et connexion Internet

Le RSF présente des intérêts immédiats : simplicité de déploiement, mobilité des employés, interopérabilité des équipements, faible coût en comparaison de l'installation et de la maintenance d'un réseau câblé. Il faut le considérer *a priori* comme un réseau ouvert au public mais également **comme une « bulle de risque » en 3D** : en effet, la connexion peut se faire de la rue, d'un autre étage, voire d'un avion (*warflying*, cf. références). En conséquence, toute connexion non maîtrisée peut remettre en cause la sécurité de l'ensemble du système d'information.

La facilité et le faible coût de mise en œuvre sont à mettre en perspective avec l'indispensable renforcement de la configuration préexistante de sécurité. Cette démarche sera identique pour tout équipement portable récent qui possède, par défaut, la possibilité de connexion à un réseau environnant ou à d'autres équipements ayant la même ressource (connexion *ad hoc*).

3. Menaces et impacts

Menaces	Vecteurs	Moyens	Finalités	Exemples
Interception	Flux de connexion et de contrôle	- Crypto-analyse (*crack*, *brute force*) - *Man in the Middle* (MiM) - Mascarade / Rejeu - Altération de message	- Atteinte DIC[1] contre les données du S.I. - Atteinte aux ressources internes du S.I. - Atteinte aux ressources de connexion du S.I.	- Consultation des serveurs de données - Internet gratuit
	Flux de données	- Captation - Fausse borne AP (MiM) - Altération de message	- Divulgation - Exploitation frauduleuse	- Données financières de caisses enregistreuses
Disponibilité	Equipements	- Déni de service (logique) - Brouillage par susceptibilité électromagnétique	- Indisponibilité du RSF - Indisponibilité de ressources véhiculées *via* le RSF	- Caméra de vidéo-surveillance - Sondes de détection
War-Xing	- *War driving* - *War driving* et géolocalisation (GPS) - *War chalking*[2]	- Localisation de proximité	- Opportunité ultérieure d'interception ou d'indisponibilité	- Cartes sur Internet - Marquage au sol
Attaques *ad hoc*	- Flux de connexions - Flux de données	- *ARP cache poisoning* - *Man in the Middle*	- Génération de pertes de paquets réseau - Dysfonctionnement de la machine	- Accès au réseau filaire - Attaques DoS classiques

[1] Disponibilité, Intégralité, Confidentialité
[2] Marquage (au sol ou sur les murs) à proximité

Commentaires

Le war-Xing ne constitue une menace qu'à partir du moment où le RSF est mal sécurisé.
Les technologies de détection de proximité ou d'interception s'appuient sur des logiciels de scanning. Les scanners actifs engagent un dialogue avec le réseau : requêtes d'identification ou de connexion. Les scanners passifs se contentent d'écouter les différents canaux. Ces équipements sont extrêmement portables, il peut s'agir d'un PDA et d'une antenne bricolée d'apparence anodine.
Tous les secteurs d'activité sont concernés par cette exposition aux risques. A titre d'exemple, les PME de par leurs faibles engagements en moyens de sécurité ; les institutions financières, le monde médical et celui de la recherche-développement en raison du caractère confidentiel et stratégique des données traitées.

4. Contre-mesures

Ces contre-mesures sont nécessaires en raison de la faiblesse de l'implémentation du protocole. Aujourd'hui, un système de firewall (DMZ) doit s'intercaler entre le RSF et le réseau local préexistant.
Il serait vain de refuser systématiquement cette technologie. S'il y a pression des utilisateurs ou de la direction, il est préférable d'en contrôler le déploiement pour éviter le constat ultérieur d'installations « sauvages » (comme ce fut le cas pour les modems au début de l'Internet grand public).
Soulignons que certains environnements industriels et médicaux ne se prêtent pas à l'utilisation des cartes et bornes AP en raison de susceptibilité électromagnétique ou d'environnement trop contraignant (chaleur, poussière, etc.). Les équipements grand public ne sont pas suffisamment « durcis » et il serait extrêmement risqué de déployer de telles ressources sur des systèmes temps réel ou pour des systèmes de détection (sécurité incendie). Partout ailleurs, des problèmes de couverture géographique et/ou de brouillage peuvent survenir en présence de matériaux entravant la propagation (béton, treillis métallique) ou d'équipements rayonnants (machines outils, fours à micro-onde).
Si une architecture RADIUS ou VPN est déjà en place, le déploiement d'un réseau sans fil peut être envisagé sans un surcoût important tout en maintenant la protection du réseau local. Dans les autres cas, et notamment pour les PME, les compétences sécurité et les investissements complémentaires doivent être pris en considération en début de projet. Une solution intermédiaire consisterait à seulement commencer le déploiement du RSF à partir de normes plus récentes, par exemple 802.11i.

A) Reconfiguration des équipements

Les mesures de reconfiguration sont généralement peu coûteuses. Elles concernent essentiellement un re-paramétrage des équipements.

Architecture et topologie

- Deux architectures s'opposent. Soit chaque borne AP est reliée au réseau filaire : les contraintes sont identiques à celles d'un réseau câblé. Soit toutes les bornes AP sont reliées entre elles et une seule est reliée au réseau. Dans ce cas, le trafic d'authentification va dégrader le débit. Quelle que soit la solution choisie, la liaison avec le réseau filaire doit se faire *via* une architecture firewall.
- La disposition physique des bornes AP a des conséquences. Lorsque c'est possible, choisir des antennes au lobe de rayonnement directif et placer les AP en des lieux qui réduisent les propagations en dehors du volume souhaité, par exemple en hauteur ou dans le coin d'une pièce. C'est ainsi

qu'il faudra être vigilant quant aux infrastructures métalliques ou gaines de ventilation qui agissent comme des guides d'onde et propagent le signal au-delà du périmètre souhaité.

- Attention aux interférences entre réseaux dans un même espace. Il est possible de répartir l'attribution des bandes de fréquence entre les différentes infrastructures. Le RSF est aussi susceptible de brouillage par d'autres équipements (par ex. Bluetooth, fours à micro-onde, répartiteurs TV… toute transmission sur la bande 2,4 GHz).

Points d'accès (bornes AP)

- Réduire la puissance d'émission par une commande logicielle.
- Privilégier le paramétrage en mode local (ex. par le port série) et donc, éviter les commandes à distance. Ce choix doit être fait au moment de l'achat ; le surcoût est d'environ 5 %. Ce mode d'administration reste très contraignant si on opte pour des authentifications *via* l'adresse MAC ou un système RADIUS en raison des mises à jour de listes (ACL). Des problèmes d'interopérabilité peuvent se poser pour des matériels de technologies différentes.
- Activer le WEP dans sa version 104 bits ou même dans sa version 40 bits. Ce dernier constitue déjà un durcissement de la sécurité même s'il existe quelques logiciels permettant la crypto-analyse des clefs, y compris sur WEP2.
- Choisir un SSID : éviter la diffusion publique qui implique un *broadcast* plus lointain. Choisir un nom de réseau qui ne rappelle pas celui de l'entreprise ou de l'activité pour ne pas susciter la tentative d'intrusion. Ne pas laisser le SSID par défaut de l'AP qui renseigne alors sur la marque de fabrique (et ses éventuelles vulnérabilités). Attention également à l'emploi d'un serveur DHCP qui invite à la connexion toute station appartenant au groupe SSID.
- Filtrer par l'adresse MAC : solution seulement envisageable pour un parc réduit de stations connectées car sinon, la mise à jour des tables d'adresses devient rapidement ardue.

Equipements portables

- Activer par une commande logique les modes BSS et ESS pour prévenir la connexion sur une fausse borne AP (scénario *man in the middle*).
- Si un portable n'est pas censé se connecter à un réseau sans fil, il est préférable de désactiver la ressource pour prévenir une connexion accidentelle ou sur une fausse borne AP qui se situerait à proximité de l'entreprise ou dans un lieu public. En fonction des équipements, déplacer un cavalier sur la carte mère, désactiver la ressource au niveau du BIOS ou désactiver le pilote de périphérique au sein du système d'exploitation (par exemple, Windows XP intègre par défaut la gestion des cartes sans fil).

B) Renforcement des ressources de sécurité

Les actions à mener sont des domaines humain, organisationnel et technique.

Sensibilisation de tous les utilisateurs quant aux enjeux

- Les plus concernés sont souvent les informaticiens, les commerciaux, les consultants, la Direction susceptibles d'être attirés par une technologie très conviviale. Il est recommandé de formaliser la politique de déploiement.
- Le déploiement d'un RSF domestique est un autre point de compromission pour des équipements à usage professionnel qui s'y connecteraient. En l'absence d'un périmètre de sécurité, les répertoires

en mode partagé sont, par exemple, un moyen pour accéder à des informations confidentielles de l'entreprise ou de l'administration.

Changement dynamique des clefs WEP

Il est possible de provoquer le changement périodique de la clef WEP pour prévenir ou réduire les possibilités d'interception. Si le poste portable se prête souvent à une telle modification, d'autres équipements, comme les tablettes, risquent de poser des problèmes. L'interopérabilité de tous les équipements peut être dégradée.

Authentification durcie

- Mise en place d'un système RADIUS, d'une architecture VPN, d'IPSEC, etc.
- Emploi du protocole 802.1x (LEAP, PEAP) qui nécessite une expertise plus forte.

Le RFC (*Request for Comments*) 2284 pour EAP (*Extensible Authentication Protocol*) explique ce standard pour l'authentification, le contrôle de l'utilisateur et le changement à la volée des clés d'encryptage.

PEAP et TTLS sont 2 standards concurrents poussés par différents acteurs pour améliorer EAP.

Géolocalisation des bornes

Cette cartographie peut être envisagée périodiquement. Elle nécessite l'installation d'un équipement GPS pour réaliser le positionnement des bornes.

Enregistrement des journaux de connexion

Certaines bornes permettent la transmission de *logs* pour un traitement centralisé. Ils seront ainsi sauvegardés pour analyser des situations atypiques.

Correction des bogues logiciels

Des dysfonctionnements logiciels, voire des faiblesses de sécurité, peuvent être corrigés par la mise à jour des programmes des bornes AP.

5. Cadre réglementaire

Il est nécessaire de consulter périodiquement l'ART car le cadre légal évolue.

Attention aux actions d'audit : le risque d'intrusion sur un autre RSF à proximité existe. Il est donc impératif d'identifier le réseau à auditer et de manipuler avec circonspection des scanners actifs qui, par définition, vont s'introduire sur tous les réseaux accessibles dans l'espace environnant.

Rappelons également que l'attaque « par rebond » reste une opportunité : le RSF va servir de premier point de connexion pour une attaque sur Internet. L'entreprise ou l'administration se trouve donc à l'origine de l'acte de malveillance.

A ce jour, il n'existe pas encore de jurisprudences concernant l'application des règles de déploiement ou les actions malveillantes réalisées.

6. Références

A) Réglementation et conseils de sécurité

http://www.etsi.org
http://www.art-telecom.fr/
http://standards.ieee.org/wireless
http://www.wi-fi.com/
http://www.hsc.fr/ressources/presentations/
http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/
http://www.weca.net

B) Logiciels et procédures d'attaque

http://www.netstumbler.com/
http://www.bretmounet.com/ApSniff/
http://wepcrack.sourceforge.net/
http://www.warchalking.org