Sécurité informatique :La sécurisation des liaisons sans fil

Vincent Lecrubier

Table des matières

Les réseaux sans fil et leurs caractéristiques

Caractéristiques importantes

Il existe de nos jours de nombreuses normes de réseaux sans fil. Les réseaux sans fil utilisent toujours les ondes électromagnétiques comme support de transmission. Les caractéristiques de ces réseaux sont dictées par l'utilisation qui leur est destinée.

Nous nous intéresserons dans cet exposé seulement aux liaisons numériques. Les liaisons analogiques tendent d'ailleurs à disparaître aujourd'hui en raison de leur besoin en bande passante plus important et de leur fiabilité moins élevée. Les principales caractéristiques différenciant les réseaux sans fil numériques sont :

- Débit maximal, variant de quelques kilobits par seconde à plusieurs centaines de mégabits par seconde..
- Nombre maximal d'utilisateurs connectés, allant de 2 à plusieurs centaines.
- Portée, de quelques mètres à plusieurs centaine de kilomètres.
- Sécurisation des échanges, allant de systèmes non sécurisés, à des systèmes alliant sauts de fréquences et techniques de cryptographie avancées.
- Fréquence utilisée, inversement proportionnelle à la longueur d'onde, qui varie selon les liaisons de quelques micromètres (infrarouges) à quelques milliers de kilomètres (communication en ELF avec les sous marins)

Nous ne ferons pas de différence dans cet exposé entre les liaisons concernant deux terminaux, et les réseaux concernant un nombre indéterminé de terminaux. En effet, dans la quasi totalité des cas, la mise en réseau de terminaux est équivalente à l'établissement de plusieurs liaisons bidirectionnelles. En particulier, les problèmes de sécurité des réseaux sans fils sont identiques entre des réseaux complexes et des liaisons entre deux terminaux.

Différents types de réseaux sans fils

Les différents types de liaisons sans fils civils peuvent être regroupés en plusieurs catégories représentant leur porté maximale. Aujourd'hui, les réseaux civils grand public suivants sont opérationnels :

- WPAN (Wireless Personnal Area Network)
    - Bluetooth (IEEE 802.15.1 puis IEEE 802.15.3) : Existant depuis 1996, il est utilisé pour remplacer les câbles entre les appareils et périphériques. La portée est de quelques mètres avec un débit de quelques Mbit/s, la sécurisation était assez faible, mais a été améliorée depuis l'arrivée de Bluetooth 2.
    - Zigbee (IEEE 802.15.4) : Émergeant depuis 2003, cette norme est destinée à permettre la communication à faible débit entre des objets, comme par exemple en domotique. Optimisée pour réduire la consommation électrique et disposant d'une portée de quelques mètres avec un débit de 20 à 250 Kbit/s.
    - Liaisons infrarouges : Utilisées par exemple pour diverses télécommandes. La portée optique peut aller jusqu'à plusieurs dizaine de mètres avec un débit variant selon les implémentations de quelques Kbit/s à quelques Mbit/s.
- WLAN (Wireless Local Area Network)
    - Wifi b (IEEE 802.11 b) : Première norme Wifi ratifiée en 1999. Visant à mettre en place des réseaux locaux sans fil. Cette première norme spécifie un débit de 11Mbit/s sur une portée de quelques centaines de mètres au maximum.
    - Wifi g (IEEE 802.11 g) : Datant de 2003, cette modification du Wifi b étend le débit jusqu'à 54Mbit/s.
    - Wifi n (IEEE 802.11 n) : La dernière évolution majeure de la norme Wifi, permet des débits jusqu'à 300Mbit/s. Certaines antennes Wifi permettent d'atteindre des portées de plusieurs dizaines de kilomètres.
- WMAN (Wireless Metropolitan Area Network)
    - WiMax (IEEE 802.16) : Avec une portée de 50km et un débit de 70 Mbit/s, cette norme récente est actuellement utilisée pour fournir une connexion internet à des foyers dont le câblage serait trop couteux.
- WWAN (Wireless Wide Area Network)
    - GSM : Appelée aussi « 2G », avec un débit maximal de 24 Kbit/s et une portée de plusieurs kilomètres, cette norme a été le premier standard en matière de transmissions numériques pour la téléphonie mobile, et est encore utilisée de nos jours.
    - GPRS : Appelée « 2,5G », cette norme est une amélioration du GSM, ajoutant la transmission par paquets. Son débit maximal de 50 Kbit/s en pratique.
    - UMTS : C'est la principale norme de type « 3G » en Europe. Son débit atteint jusqu'à 1 Mbit/s à l'arrêt.
    - HSDPA : Appelée « 3G+ », cette norme augmente encore le débit jusqu'à 7,8Mbit/s.

Il existe de plus de nombreux réseaux sans fil civils spécialisés, par exemple dans l'aviation civile, dans le domaine ferroviaire, de l'énergie...

Au niveau militaire, de nombreux type de liaisons sans fil existent, cependant pour l'OTAN, il existe deux standards principaux.

- Liaison 16 : Actuellement la plus utilisée pour les communications de données tactiques, cette liaison permet de transmettre des données telles que la position des différentes unités du théâtre d'opérations, des plans de vol, comptes rendus de missions, etc... La configuration des réseaux en liaison 16 n'est pas dynamiques, la topologie du réseau reste la même tout au long d'une mission. La portée de chaque émetteur est de l'ordre de 600km, mais le réseau peut s'étendre sur de plus grandes distances.
- Liaison 22 : Compatible avec le liaison 16, cette norme permet plus de souplesse dans la configuration du réseau. Les intervalles de temps ne sont pas affectés à une seule unité mais peuvent être affectés en fonction des besoins temporels d'émission, et plusieurs réseaux peuvent être interconnectés.
- On peut aussi parler d'un exemple de liaison militaire atypique : la communications avec les sous marins en ELF. Les fréquences extrêmement basses (ELF), de l'ordre de 70Hz, sont les seules fréquences non atténuées par l'eau de mer. Elles sont utilisées pour émettre des messages stratégiques en direction des sous marins en patrouille autour du globe, qu'ils soient en plongée ou pas. La longueur de l'antenne d'émission étant proportionnelle à la longueur d'onde, il faut une antenne de plusieurs milliers de kilomètres. C'est pourquoi les émetteurs consistent en deux stations séparées de plusieurs milliers de kilomètres, utilisant la croute terrestre qui les sépare comme antenne. Le besoin de dispositifs de sécurisation de la transmission est ici évident.

Enjeux de la sécurisation des réseaux sans fil

Besoin

On entend par « sécurisation des réseaux sans fils » plusieurs notions, plus ou moins importantes et plus ou moins implémentées sur chaque type de réseau.

- Authentification : garantie de l'identification des membres du réseau. L'identité des membres du réseau doit être certifiée et connue avec certitude. Exemples : Liaisons militaires, connexion Wifi pour lesquelles la Loi Hadopi demande aujourd'hui que l'identité des téléchargeurs soit connue avec précision.
- Confidentialité : impossibilité pour un tiers non accrédité d'accéder aux informations privées transmises. Exemples : Paiement en ligne, conversations téléphoniques...
- Validité des informations transmises : un tiers ne doit pas être capable de modifier les informations transmises sur le réseau ou d'émettre des informations falsifiées. Exemples : Télévision numérique terrestre, liaisons militaires...
- Intégrité des informations transmises. Un tiers malveillant ne doit pas être en mesure d'empêcher la transmission d'informations sur le réseau. Exemples : liaisons militaires, applications domotique pour lesquelles le brouillage peut être problématique (portes automatiques ou télécommandées...)
- Globalement, les deux derniers points font partie d'une notion plus générale : la qualité de service du réseau doit être résistante aux attaques.

Risques

Tous les risques menaçant les réseaux filaires existent aussi pour les liaisons sans fil. Cependant, le mode des transmission des réseaux sans fil en aggrave certains, et génère des menaces supplémentaires, spécifiques à ce type de réseau. Les risques les plus importants pour les liaisons sans fils sont :

- Brouillage des communications, empêchant toute communication sur le réseau. Exemple : brouillage des communications stratégiques militaires par une puissance adverse, guerre électronique.
- Interception par un intrus des données transmises. Exemple : interception d'informations de login transmises sur le réseau UMTS.
- Injection par un intrus des données falsifiées. Exemple : Piratage d'un réseau domotique afin d'ouvrir les portes pendant l'absence du propriétaire.
- Utilisation des ressources du réseau par un intrus. Exemple : squat d'une connexion Wifi par un voisin.

Les stratégies de sécurisation

Cryptographie

Une solution implémentée sur tout les réseaux sans fils non publics de nos jours est évidemment la cryptographie, qui consiste à chiffrer le message transmis sur les ondes.

Les algorithmes de chiffrement sont tous des algorithmes à clé privée. Dans la majorité des cas, il doit donc y avoir un échange « physique » des clés avant de démarrer toute communication. La clé échangée physiquement n'est que rarement utilisée directement en tant que clé cryptographique, mais elle sert surtout de souche permettant d'initialiser des clés plus complexes, ou déterminer la série de changements de clés ou de fréquences..

Voici quelques exemples de connexions cryptées et du moyen d'échange des clés :

- ZigBee et Bluetooth : Algorithme AES 128 dont la clé est prédéfinie dans l'appareil, ou entrée par l'utilisateur. L'échange de clé se fait donc par voie orale entre les utilisateurs, ou par mémorisation dans le cas d'un même utilisateur sur les deux appareil.
- Wifi : Algorithme WEP, puis WPA et WPA2, dont la clé est définie par l'appareil hôte. Dans le cas des passerelles Wifi, la clé est stockée dans le routeur Wifi, et imprimée sur celui ci ou sur des étiquettes fournies. L'utilisateur entre cette clé au clavier sur l'appareil client. L'échange de clé se fait donc par mémorisation ou lecture par l'utilisateur.
- Wimax, GSM et 3G : Différents algorithmes dont la clé est stockée dans la carte SIM et dans un centre d'authentification de l'opérateur (cf page 8). L'échange physique de clé se fait donc lors de la mise en service de la carte SIM, lorsque le vendeur entre à la main le numéro de carte SIM et l'associe avec un compte client auprès de la base de donnée de l'opérateur.
- Liaison 16 et Liaison 22 : La clé est enregistrée avant le début des opérations sur une bande de papier perforée, qui est lue par le terminal radio équipant l'unité à relier au réseau. L'échange de clé se fait donc par l'échange en main propre de la bande perforée contenant la clé cryptographique.

Nous voyons donc que dans tous les cas de réseaux sans fils, aux vulnérabilités habituelles des méthodes cryptographiques (Attaques par injection de paquets, par rejeu...), il faut ajouter un risque très important : celui dû à l'opérateur humain.

En effet, dans tous les cas présentés à l'exception du Wifi en WEP, il semble bien que le moyen le plus simple de pirater la connexion soit tout simplement de s'emparer de la clé au moment de son échange physique entre les deux stations à connecter. Et cet échange physique fait tout le temps appel à un opérateur humain. Si l'on reprend les exemple cités plus haut, on peut trouver les vulnérabilités suivantes liées à l'opérateur.

- ZigBee et Bluetooth : La clé par défaut est souvent conservée (cf page 8), ou bien les clés choisie par l'opérateur ne sont pas aléatoires mais se retrouvent facilement par des méthodes de « social engineering » qui font de plus en plus parler d'elles.
- Wifi : L'utilisateur mal informé laisse souvent un mode de cryptage trop faible (clé WEP ou WPA1). Si l'utilisateur spécifie lui même la clé, elle est souvent retrouvable facilement à l'aide d'attaques par dictionnaires.
- Wimax, GSM et 3G : Il est possible d'extraire des informations de la carte SIM d'un téléphone oublié par inadvertance, prêté, etc...

- Liaison 16 et Liaison 22 : Un manque de vigilance de l'opérateur détenant la clé sous forme de bande perforée peut très bien permettre à un espion de s'emparer du code à moindre frais, lui facilitant ensuite la tâche pour pirater ou écouter les communications cryptées, bien qu'il existe d'autres niveaux de sécurités.

Évasion et sauts de fréquence

Cette technique, spécifique aux réseaux radio, permet de faire face au risque de brouillage et de piratage. La fréquence sur laquelle sont transmises les informations n'est pas fixe, mais change régulièrement, afin d'éviter qu'un intrus puisse rester connecté pendant longtemps. La suite de fréquences utilisées est pseudo aléatoire, et seuls les appareils authentifiés ont accès à la clés permettant de connaître l'enchainement des fréquences. Un appareil non authentifié pourra agir sur une fréquence donnée, mais sa connexion sera perdue au changement de fréquence suivant.

Afin de pirater le réseau, en plus des obstacles cryptographiques habituels, l'intrus doit faire face au problème du saut de fréquences, et doit trouver un moyen de connaître les fréquences qui seront utilisées à chaque instant afin de pouvoir avoir un accès continu au réseau. De plus, un brouillage est plus difficile à réaliser car le brouillage d'une seule fréquence n'est pas suffisant pour détruire la connexion.

Par exemple, le Bluetooth effectue 1600 changements de fréquence par seconde. La liaison 16 en effectue 77000.

Cas d'utilisation

Connexion Bluetooth

Pour lancer une connexion entre deux appareils, il faut passer par une phase d'appairage, limitée dans le temps. D'abord l'appareil receveur doit être en mode de « découverte », ce qui permet aux autres terminaux de le détecter et de lancer la connexion. Ensuite, l'appareil qui reçoit la connexion fixe un code. Ce code peut soit être donné par l'utilisateur à l'aide d'un clavier, soit être prédéfini dans la mémoire de l'appareil si celui ci ne dispose pas de clavier. L'appareil se connectant doit disposer du même code. Typiquement, l'utilisateur de terminal récepteur entre le code dans le terminal émetteur à l'aide du clavier.

Lorsque la phase d'appairage est terminée, les deux appareils stockent le code en vue d'une utilisation ultérieure, afin d'éviter de répéter la phase d'appairage à chaque connexion. A partir ce code, ils génèrent une clé cryptographique qu'ils utiliseront lors de leurs communications.

Nous voyons donc que l'utilisateur définit un mot de passe permettant de générer la clé cryptographique lors de l'appariement avec un autre appareil. La fragilité de cette méthode est celle inhérente aux mots de passe. Une attaque par dictionnaire est très facile. Une proportion importante de liaisons Bluetooth utilise des mots de passe tels que « 0000 », « 1234 ». Cependant, le mode « découverte » étant généralement limité dans le temps, la vulnérabilité du système est assez courte, mais largement suffisante pour un pirate motivé.

Connexion GSM

La première phase est l'authentification, qui se fait à l'aide du centre d'authentification de l'opérateur. Le centre d’authentification et la carte SIM partagent une clé sécrète Ki qui n’est jamais transmise sur le réseau. Pour authentifier l’utilisateur, le réseau génère un nombre aléatoire qu’il transmet au mobile et attend une réponse. Le mobile utilise alors une fonction à sens unique qui lui permet de calculer une réponse en utilisant comme paramètres d’entrée la clé secrète Ki et le nombre aléatoire qui lui a été transmis. Ce résultat est ensuite retransmis du terminal mobile vers le centre d’authentification. Le centre d’authentification (AuC) qui connaît également Ki fait le même calcul et le compare au résultat reçu. Si les deux résultats sont identiques, le terminal mobile aura prouvé qu’il connaît le secret partagé Ki et est donc authentifié. Il existe une paire de clés par abonné dans chaque réseau radiomobile dont l’une est générée dans une puce SIM et l’autre dans la base de donnée d’authentification. Dès lors, on comprend toutes les précautions prises par les opérateurs pour la protection de ces données (contrôle d’accès, redondance d’architecture, sauvegardes).

La seconde phase a lieu lorsque l'identification est terminée, et dure jusqu'à la fin de la session. Le protocole est quasiment le même que celui de l’authentification à l’exception du fait que l’algorithme utilisé pour la génération de la clé de session est différent. Le nombre pseudo aléatoire qui est généré par le réseau et transmis au mobile est utilisé avec la clé Ki pour générer une clé de session. La clé de session générée est ensuite utilisée pour chiffrer les trames bit à bit en utilisant l’opérateur XOR. Le centre d’authentification qui sait également calculer la clé de session peut déchiffrer ou chiffrer les trames qu’il reçoit ou émet. Il existe un unique Ki par terminal d’abonné. En pratique le même nombre aléatoire qui a servi lors de l’authentification est simultanément utilisé pour générer la clé de session. Ceci évite l’implémentation d’un protocole spécifique et surtout l’économie de temps et de ressources dans le réseau.

Sources

Généralités

- http://www.securite-informatique.gouv.fr/

Zigbee

- http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=9436
- http://www.meshnetics.com/zigbee-faq/

Bluetooth

- http://www.symantec.com/connect/fr/articles/bluetooth-security-review-part-1
- http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf

Wifi

- http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/
- http://www.generation-nt.com/wifi-securite-cracker-cle-reseau-wep-wpa-wpa2-article-24824-1.html

Réseaux 3G

- http://freesecure.info/doc/securite-UMTS.pdf
- http://www.securiteinfo.com/attaques/phreaking/securite_reseaux_sans_fil_3G_GSM_UMTS_GPRS.shtml

Communications militaires

- http://fr.wikipedia.org/wiki/Communication_avec_les_sous-marins
- http://fr.wikipedia.org/wiki/Liaison_16