CASES LUXEMBOURG Guide pratique

Les réseaux sans fil

Attaques possibles

Pour plus de sécurité, adoptez les réflexes CASES !

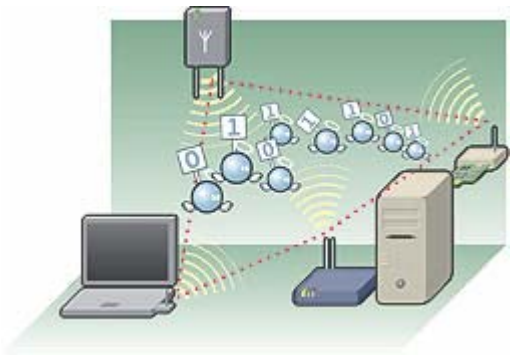

Table des matières

1 Introduction
2 Les attaques
3 Comment protéger son réseau sans fil ?
4 Glossaire et abréviations
5 Sources

1 Introduction

Pour s'introduire dans un réseau filaire, il faut s'y relier « physiquement ». En revanche, dans un réseau sans fil, cette action est beaucoup plus discrète : tout voisin ou passant se trouvant dans la zone de couverture du réseau peut potentiellement s'y raccorder. Cette faculté est d'autant plus gênante qu'à l'inverse de ce qui se passe en filaire, l'intrus n'est pas forcément visible. De ce fait, libre à lui donc de fouiner sur les disques durs des PC raccordés au réseau ou d'utiliser la connexion Internet à mauvais escient.

2 Les attaques

2.1 Bluetooth

La quasi-totalité des GSM (ainsi qu'un certain nombre de PDA, laptops, etc.) ont la faculté de se connecter à un réseau Bluetooth. Cette fonctionnalité très pratique permet, par exemple, d'échanger très rapidement des données entre 2 appareils. Elle est ainsi très couramment utilisée pour connecter un GSM à une oreillette sans fil.

Ainsi, si une personne malintentionnée utilise la fonctionnalité Bluetooth d'un appareil, elle peut aisément profiter des tous les contacts du téléphone, lire les messages échangés, écouter les conversations, voire même passer des appels gratuitement. Les ordinateurs et PDA communiquent souvent en Bluetooth, des informations peuvent alors être échangées comme les coordonnées de contacts ou des messages e-mail. Il serait alors possible de les intercepter. Un autre exemple peut être l'utilisation de clavier Bluetooth avec des possibilités d'interception des frappes sur le clavier par un attaquant externe et faisant alors office de keylogger très dangereux.

De fait, de nombreux logiciels permettant d'exploiter les failles Bluetooth sont disponibles sur Internet, permettant d'espionner les communications, de passer des communications au nom de voir de l'équipement vulnérable ou d'en prendre le contrôle à distance.

2.2 Wifi

L'attaque probablement la plus utilisée est le Wardriving. Cette attaque facile et très répandue consiste à rechercher les réseaux sans fil détectables et accessibles depuis la voie publique.

Pour ce faire, un wardriver se promène équipé d'un terminal mobile WiFi (ordinateur portable, PDA, smartphone), avec une antenne sans fil et éventuellement une sonde GPS permettant la géo localisation des réseaux détectés, ceci afin de capter les réseaux wireless existant dans les environs et de les cartographier. Le terme Warchalking désigne quant à lui le fait de "tagger" les lieux où des réseaux WiFi ont été découverts par wardriving.

On peut cartographier les accès WiFi dans le but de trouver des accès non sécurisés pouvant être exploités afin de détourner une connexion réseau à son avantage, et éventuellement de pouvoir surfer gratuitement sur Internet ou écouter ce qui se passe sur le réseau pour notamment y voler des informations. Plusieurs logiciels permettent d'effectuer cette recherche très facilement, en indiquant par exemple de quel type est la borne sans fil et si le chiffrement / l'encryption est activée.

Lorsqu'une borne sans fil est détectée, des outils disponibles sur Internet permettent d'écouter (et de capturer) les communications entre le client sans fil et la borne. Grâce à cette capture et à d'autres outils de diagnostic, on peut lire des données (mots de passe, comptes E-mail, documents envoyés), "rejouer" la communication (pour voler la session de l'utilisateur et récupérer ses données), etc. Une fois la clé de cryptage (WEP - Wired Equivalent Privacy - par exemple) découverte, l'outil travaille en mode « autonome » et capture puis déchiffre les données en temps réel…

3 Comment protéger son réseau sans fil ?

3.1 Le Bluetooth et la sécurité

La principale faiblesse de la sécurité Bluetooth réside dans l'insuffisance du code personnel à 4 chiffres qui est entré lors de la mise en connexion de 2 appareils Bluetooth.

Un sérieux danger réside dans le fait que souvent la gestion des mises à jour n'est que rarement mise en œuvre pour les outils Bluetooth (téléphones mobiles, smartphones) et que des vulnérabilités exploitables ne sont pas corrigées, même si des patchs sont disponibles.

Une autre faille, inhérente à tous les appareils mobiles, réside dans le déni de services. En effet, les appareils Bluetooth fonctionnant sur batterie, une forme d'attaque peut consister à surcharger de travail un dispositif ciblé de manière à épuiser ses batteries. Ainsi le GSM attaqué se retrouvera très vite sans batterie et sera inutilisable pour son propriétaire. Les concepteurs de Bluetooth travaillent actuellement sur des parades à ces limitations.

Ainsi pour protéger efficacement son appareil disposant d'une connexion Bluetooth il suffit de :

- Ne pas « coupler » son appareil à un périphérique inconnu ou dont on n'est pas sûr de l'identité de l'émetteur, surtout si l'on doit entrer son code PIN
- Mettre à jour le système d'exploitation de son appareil
- Désactiver la fonctionnalité Bluetooth lorsqu'elle n'est pas utilisée.

Pour plus d'informations consultez le dossier (In)sécurité Bluetooth : http://www.cases.public.lu/fr/publications/dossiers/bluetooth/bluetooth-insecurite.pdf

3.2 WLAN

Les dernières normes du Wifi (802.11) intègrent désormais des moyens de protection.

De plus, voici les quelques précautions à prendre pour sécuriser son réseau Wifi :

- Une infrastructure adaptée

La première chose à faire lors de la mise en place d'un réseau sans fil consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir.

Il n'est toutefois pas rare que la zone de couverture soit largement plus grande que souhaitée, auquel cas il est possible de réduire la puissance de la borne d'accès afin d'adapter sa portée à la zone à couvrir.

- Changer les valeurs par défaut

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur. Il est impératif de se connecter à l'interface d'administration (généralement via une interface Web sur un port spécifique de la borne d'accès) pour notamment changer le mot de passe d'administration.

- Protéger le SSID

D'autre part, afin de se connecter à un point d'accès il est indispensable de connaître l'identifiant du réseau (SSID – Service Set Identifier)). Ainsi, il est vivement conseillé de modifier le nom du réseau par défaut et de désactiver la diffusion (broadcast) de ce dernier sur le réseau.

Le changement de l'identifiant réseau par défaut est d'autant plus important qu'il peut donner aux pirates des éléments d'information sur la marque ou le modèle du point d'accès utilisé. On peut aussi cacher la diffusion du SSID et ne fournir le nom qu'aux personnes de confiance. Cela évite qu'il soit découvrable facilement par tout le monde.

- Le filtrage des adresses MAC

Chaque adaptateur réseau possède une adresse physique qui lui est propre (appelée adresse MAC).

Cette adresse est représentée par 12 chiffres hexadécimaux groupés par paires et séparés par des tirets ou des doubles points. Les points d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès (ACL – Access Control List) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil. Cette précaution quelque peu contraignante permet de limiter l'accès au réseau à un certain nombre de machines. Par contre, cela ne résout pas le problème de la confidentialité des échanges.

- Utilisation d'un protocole sécurisé

Un moyen d'augmenter la sécurité au niveau de la confidentialité et de l'authentification, est d'utiliser la notion de protocole sécurisé WEP (Wired Equivalent Privacy) ou WPA (WiFi Protected Access).

Le WEP est un protocole chargé de chiffrer les paquets Wifi qui transitent entre les équipements. Le principe du WEP consiste à définir dans un premier temps une clé secrète. Cette clé doit être déclarée au niveau du point d'accès et des clients. Elle entre en jeu pour chiffrer les données. La clé de session partagée par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations WiFi il est nécessaire de les configurer en utilisant la même clé de session. Ainsi, la connaissance de la clé est suffisante pour déchiffrer les communications.

Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données mais il est vivement conseillé de mettre au moins en œuvre une protection WEP 128 bits afin d'assurer un niveau de confidentialité minimum si l'on ne peut rien choisir d'autre. En effet, certains appareils Wifi ne disposent pas encore de moyen de s'authentifier au WPA (consoles de jeux portables par exemple)

Le WPA est appelée à remplacer le protocole WEP, elle est présente aujourd'hui dans la quasi-totalité des équipements Wifi… La différence entre WEP et WPA réside principalement dans l'utilisation de clés dynamiques, renouvelées très régulièrement. Ceci constitue un pas dans la sécurité, car s'il demeure théoriquement possible d'écouter le trafic, la mise en place de clés dynamiques rend beaucoup plus difficiles, voire impossibles, les attaques par force brute. Le WPA est préférable au WEP d'un point de vue sécurité mais tous les équipements ne sont pas toujours compatibles.

Le WPA2 est une évolution du WPA qui permet de sécuriser les réseaux wifi aussi bien en mode « Ad-hoc »

qu'en mode « Infrastructure ». CASES Luxembourg recommande l'utilisation de WPA2 si le matériel le supporte.

Bien sur, les moyens de protection des réseaux filaires s'appliquent aussi ici :

- Mise en œuvre d'un VPN

Pour toutes les communications nécessitant un haut niveau de sécurisation, il est impératif de recourir à un chiffrement fort des données et de mettre en place un réseau privé virtuel (VPN – Virtual Private Network).

Les réseaux privés virtuels peuvent employer la cryptographie et d'autres mécanismes de sécurité pour aménager un "tunnel" sécurisé et par l'intermédiaire duquel s'effectuent les transmissions de données entre des utilisateurs habilités à les employer.

Cette sécurisation de bout en bout ne permet l'accès au réseau qu'aux utilisateurs habilités et évite l'interception des données pendant leur transmission, quel que soit le média utilisé pour transporter les données.

Les réseaux VPN servent également à sécuriser les connexions des utilisateurs nomades demandant une connexion distante. L'utilisation d'une technologie unique est évidemment un avantage au niveau de la facilité de gestion et de la maîtrise technique.

- Firewall

Il est important de considérer par défaut, qu'un réseau WiFi est un réseau auquel on ne peut faire confiance : il est préférable d'utiliser une barrière logique (firewall) pour isoler un réseau filaire d'un réseau WiFi.

Installer et configurer un pare-feu (firewall), même peu coûteux, entre les points d'accès et le réseau filaire ainsi que sur les postes clients, permet de déployer des fonctions d'identification et d'authentification suffisantes pour dissuader la majorité des pirates. Il existe de nombreux types de pare-feu, logiciels ou bien matériels, le niveau de protection variant de l'un à l'autre.

3.3 Réseaux cellulaires / téléphones portables

Dans la norme GSM, la protection des données est assurée par les algorithmes de chiffrement A5/1 et A5/2.

Le système GSM a donc recours aux procédés suivants :

- Authentification de chaque abonné avant de lui autoriser l'accès à un service,
- Utilisation d'une identité temporaire,
- Chiffrement (ou cryptage) des communications.

3.4 Wimax

Le Wimax étant très similaire au Wifi, les conseils pour l'architecture sont les mêmes que pour le Wifi.

Le trafic Wimax est encrypté (DES3 et AES) et pour l'authentification point à point, c'est PKM-EAP (Extensible Authentication Protocol) qui est utilisé.

4 Glossaire et abréviations

EDGE - Enhanced Data rate for GSM Evolution

GPRS - General Packet Radio Service

GPS - Global Positioning System

GSM - Global System for Mobile Communications - Groupe Spécial Mobile

HSDPA - High Speed Downlink Packet Access

MAN - Metropolitan Area Network

UMTS - Universal Mobile Telecommunications System

WAP - Wireless Access Protocol

WEP - Wired Equivalent Privacy

WIFI - Wireless FIdelity

WLAN - Wireless Local Area Network

WPAN- Wireless Personal Area Network

5 Sources

- WiFi Planet - http://www.wifiplanet.com
- WiFi Alliance - http://www.wi-fi.org/
- The Official Bluetooth Web-site - http://www.bluetooth.com/
- WiMaxxed - http://wimaxxed.com/
- WIMAX forum - http://www.wimaxforum.org/home
- GuideInformatique.com - http://www.guideinformatique.com/fiche-telephone_mobile-735.htm
- Wikipédia – http://www.wikipedia.org
- L'aménagement numérique des territoires - http://extranet.ant.cete-ouest.equipement.gouv.fr/article.php3?id_article=9
- What is the WiMAX Security scheme/protocol? - http://www.wimax.com/education/faq/faq29