

Gare aux vampires du haut débit!

SANS FIL Les réseaux wi-fi risquent de devenir la cible des «tricheurs», préviennent trois chercheurs de l'EPFL. Qui ont breveté une invention pour résoudre le problème.

Pour qu'un protocoleienne, il faut que tout le monde en respecte les règles. C'est vrai pour les mondanités, et c'est vrai pour le protocole du wi-fi. D'où la menace qui plane sur les «hotspots», les réseaux wi-fi qui fleurissent un peu partout, dans les hôtels et les centres commerciaux: il devient de plus en plus facile de contourner les règles et des «tricheurs» pourraient en profiter pour tirer à eux la couverture du haut débit. Un peu comme certains remontent à toute berzingue, sur la voie d'urgence, une autoroute embouteillée...

C'est une équipe de trois chercheurs de l'EPFL qui a mis le doigt sur le problème: il suffirait à des hackers de changer une seule ligne de code pour vampiriser la bande passante d'un réseau sans fil, avertit le professeur Jean-Pierre Hubaux.

Le problème provient du Multiple Access Control (MAC), le protocole qui définit la répartition de la bande passante entre les utilisateurs d'un même point d'accès wi-fi. Normalement, la répartition se fait de façon aléatoire. Ces taux sont constamment réassignés, ce qui fait que chaque utilisateur bénéficie en moyenne du même débit.

Mais, en 2003, de nouvelles cartes wi-fi sont arrivées sur le marché. La gestion du MAC n'y est plus assurée par le hardware, mais par le logiciel. Ce qui change tout: les cartes sont de plus en plus programmables et il devient possible de «tricher»

avec le protocole. Pour peu qu'on travaille sous Linux, on peut, en modifiant une ligne du protocole, fixer un taux de transfert élevé en sa faveur. Pourquoi sous Linux? Parce que, à l'inverse de Windows, son code-source est ouvert, donc manipulable.

Mieux vaut prévenir que guérir

La «faille» a été démontrée en laboratoire par l'équipe du professeur Hubaux. Et alors que des standards ont été développés, comme le 802.11i, pour renforcer la sécurité et la confidentialité des «hotspots», rien n'a encore été fait pour empêcher la fraude au MAC. Certes, aucun cas de «tricherie» n'a encore été rapporté dans le monde réel, en dehors des labos feutrés de l'EPFL. Mais, avec la multiplication des «hotspots», des réseaux commerciaux, mieux vaut ne pas prendre l'avertissement à la légère.

Jusqu'ici, les réseaux sans fil étaient cantonnés aux campus et aux entreprises: la vocation originelle du wi-fi était de remplacer les réseaux locaux filaires (Ethernet), qui constituaient autant de pièges pour les secrétaires pressées... Mais, aujourd'hui, les opérateurs — Swisscom en tête — s'y intéressent de plus en plus pour des applications commerciales. Cela d'autant plus que beaucoup sont tombés de haut avec l'UMTS... Or, quand on sait que certains hôtels chargent plus de 1 franc la minute pour

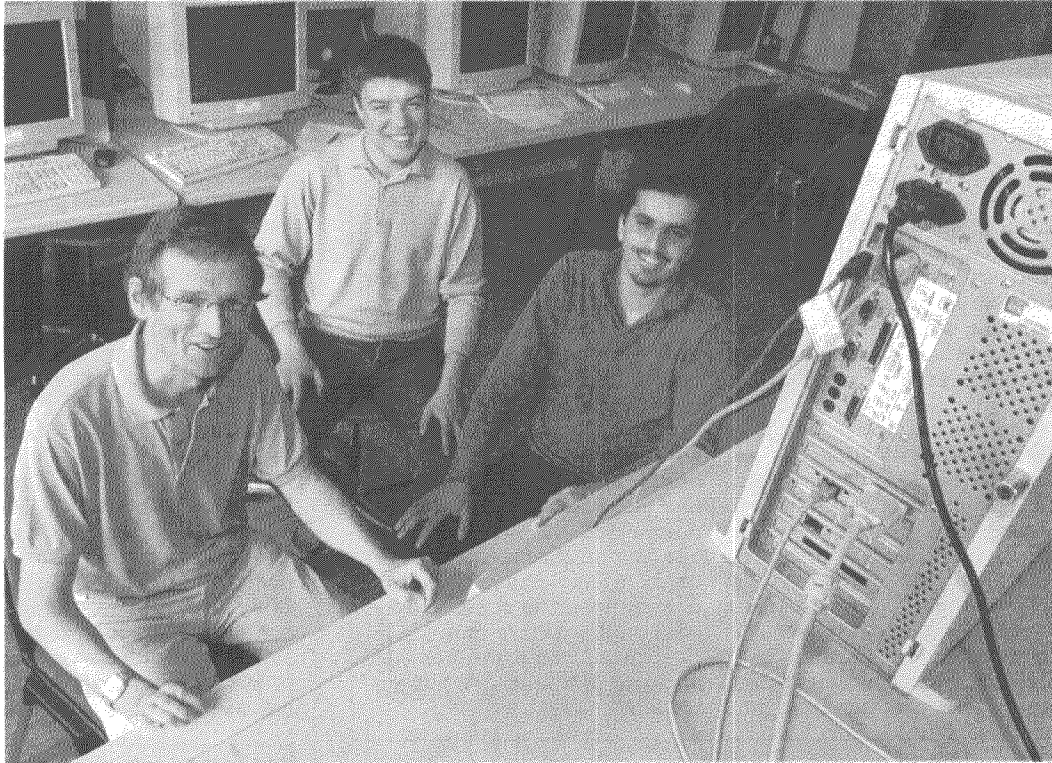
l'utilisation de leur «hotspot», on comprend que la tentation de tricher soit grande. «D'habitude, on traite les problèmes après coup, argumente Maxim Raya, le doctorant qui a initié le projet. Mais notre objectif est de sensibiliser les entreprises concernées avant qu'ils n'apparaissent.»

L'effet Domino

Pour ce faire, les trois collègues, le professeur Hubaux, Imad Aad et Maxim Raya, ne viennent pas les mains vides: ils ont développé un logiciel, baptisé Domino, pour couper l'herbe sous les pieds des pirates. «Domino détecte les anomalies du réseau sur la base d'une série de moyennes statistiques», explique Jean-Pierre Hubaux. Les «tricheurs» sont identifiés en une fraction de seconde et Domino peut aussi être configuré pour les bloquer automatiquement.

Un brevet a été déposé aux Etats-Unis et les trois chercheurs espèrent breveter leur invention. Ils ont déjà démarché des industriels, en se concentrant sur les sociétés spécialisées dans la sécurisation des réseaux, sur les opérateurs télécoms et sur les constructeurs, comme Cisco ou Hitachi. Toutefois, reconnaît Imad Aad, «nous n'en sommes qu'au début». Et aujourd'hui, plusieurs scénarios sont possibles: la commercialisation de Domino peut passer par le franchisage, mais aussi — pourquoi pas? — par la vente du brevet.

NICOLAS BERLIE



Le professeur Jean-Pierre Hubaux, Maxim Raya et Imad Aad (de gauche à droite) entendent bien damer le pion aux «tricheurs» du wi-fi.

Philippe Maeder