Nouveau protocole de sécurité WLAN chez Cisco

La sécurisation des accès aux réseaux sans fil est d'actualité. Cisco Systems apporte sa pierre à l'édifice en cours de construction.

Après avoir publié une alerte sur le protocole du système d'authentification LEAP (*Lightweight extensible authentification protocol*) pour les mots de passe non cryptés, en août dernier, Cisco propose aujourd'hui un nouveau protocole de protection contre les attaques de type 'dictionnaires', qui consistent à tester en masse des mots afin de repérer les mots clés. Le protocole EAP-FAST (*Extensible Authentification Prototocol – Flexible Authentification via Secure Tunneling*) a été développé par Cisco; il est destiné aux réseaux sans fil Wireless LAN ou WLAN, donc Wi-Fi inclus. La solution proposée consiste à envoyer un mot de passe d'authentification entre le client WLAN et l'accès LAN sans fil au travers d'un 'tunnel' sécurisé et crypté. L'intérêt du protocole EAP-FAST va au delà: il permet de se passer de serveurs déportés pour la manipulation des certificats numériques provenant d'autres systèmes de sécurité WLAN, le *Protected Extensible Authentification Protocol* ou PEAP. Cependant pour Cisco, EAP-FAST se place plutôt en complément de LEAP et de PEAP qu'en remplacement. Ce nouveau protocole pourrait être disponible gratuitement sur le site de Cisco avant la fin mars. Il pourrait être intégré au futur protocole de sécurité ***802.1x wireless*** en cours de développement par l'IETF. Et il sera validé dans le programme de partenariat du constructeur, CCX.