Le protocole SSL de paiement à distance désormais piratable

SSL (Secure Socket Layer), le protocole de sécurité d'échanges de données le plus utilisé sur la toile, jusqu'à présent sans faille connue, vient d'être cassé par une équipe de l'Ecole Polytechnique Fédérale de Lausanne (EPFL, Suisse). Alors question, est-ce que nos paiements par CB sont toujours aussi sûr ?

En moins d'une heure, les attaquants, le professeur Serge Vaudenay et un étudiant, Martin Vuagnoux sont parvenus à obtenir le mot de passe d'un utilisateur d'Outlook Express 6. Une fois les paramètres de l'utilisateur en main il leur était possible d'utiliser le compte afin d'envoyer des mails sous son identité, de passer des transactions financières ou autres.

Ces faux pirates ont réussi à s'emparer du mot de passe grâce à un algorithme de chiffrement appelé cipher block chaining (CBC) et utilisé, parmi d'autres, dans le protocole SSL. Par un jeu d'aller-retour de messages d'erreurs, les deux "chercheurs" ont réussi à obtenir le mot de passe de la victime.

Il est bon de rappeler que le système SSL permet de crypter des données afin qu'elle ne puisse pas être déchiffrées durant leur parcours sur le reseau, entre le serveur et le client. L'utilisation de SSL est signalée soit par un petit cadenas fermé sur le navigateur ou soit par une adresse web commençant par https://.

Faut-il arrêter de consulter ses mails en ligne et arrêter d'acheter par Internet ? La réponse est non car avant d'annoncer publiquement la faille du protocole SSL, le jeudi 20 février 2003, le professeur Serge Vaudenay et Martin Vuagnoux ont bien avant signalé leur découverte aux développeurs du SSL. Ces derniers ont sorti dans les plus brefs délais une nouvelle version du protocole (OpenSSL 0.9.7a) jusqu'à la prochaine faille qui sera trouvée.

Par

Publié sur Cafeduweb - Archives le samedi 22 février 2003
Consultable en ligne : http://archives.cafeduweb.com/lire/2801-protocole-ssl-paiement-a-distance-desormais-piratable.html