

Transactions via Internet: des chercheurs de l'EPFL font sauter le verrou de sécurité

Des chercheurs de l'EPFL ont trouvé une faille dans le système le plus répandu de sécurisation des transactions effectuées via Internet. Ils ont démontré qu'il est possible de reconnaître en moins d'une heure le mot de passe utilisé par un internaute pour se connecter à un service de vente commercial ou à son compte en banque en ligne. En devançant les pirates, ils offrent les moyens de se prémunir contre une telle attaque !

Nous sommes les premiers à avoir découvert cette faiblesse du protocole SSL, le procédé de sécurisation le plus couramment utilisé pour les transactions via Internet, précise le professeur à l'EPFL Serge Vaudenay. SSL ou Secure Socket Layer était pourtant réputé inviolable. Les chercheurs de l'EPFL ont imaginé une attaque qui fonctionne quand l'algorithme de chiffrement utilisé est de type CBC et que le pirate se trouve dans le voisinage du serveur de messagerie.

Mot de passe intercepté Concrètement, explique le professeur Vaudenay, nous avons développé un programme qui nous a permis d'intercepter le mot de passe d'une personne utilisant un logiciel de communication sécurisé par SSL. Les scientifiques sont ensuite parvenus à se connecter au logiciel en se faisant passer pour l'utilisateur. Ils auraient ainsi pu lire ses mails ou effectuer des transactions financières en son nom.

Faut-il dorénavant s'abstenir d'utiliser Internet pour effectuer ses paiements ? Evidemment, rassure le professeur Vaudenay, nous avons transmis le résultat de nos recherches aux personnes qui mettent à jour le SSL. La nouvelle version d'openssl (0.9.7a) apporte une protection contre l'attaque imaginée par les chercheurs de l'EPFL.

Pôle de recherche national Le projet qui a mis en évidence la faille du protocole SSL a été réalisé dans le cadre du Pôle de recherche national sur les réseaux mobiles MICS. Outre Serge Vaudenay, directeur du Laboratoire de sécurité et de cryptographie, les personnes ayant participé aux travaux sont le chercheur à l'EPFL Brice Canvel, un étudiant de la section Systèmes de communications Martin Vuagnoux et un responsable de la cryptographie dans une grande banque Alain Hiltgen.

Un programme SSL est transparent pour l'utilisateur. Ce dernier peut donc l'utiliser en toute ignorance. Ceci-dit, un serveur sécurisé par SSL possède une adresse commençant par https://... Le **s** signifie secured (sécurisé). Secure Socket Layer peut se traduire par couche de Socket sécurisée. Socket est un anglicisme désignant une interface permettant de faire communiquer les logiciels entre eux. Le SSL est ainsi un protocole qui protège cette interface de toute utilisation pirate ou non autorisée en assurant la confidentialité des opérations.