La cryptologie rompt avec le secret défense

- Informatique - Sécurité Informatique -

Date de mise en ligne : vendredi 6 octobre 2006

Spyworld Actu

La médaille d'or du CNRS honore cette année Jacques Stern, pionnier reconnu mondialement de la cryptologie, une discipline longtemps soumise au secret défense qui envahit désormais la vie de tous les jours. "Vous avez tous sur vous deux processeurs cryptographiques : un téléphone portable et une carte bancaire", a lancé vendredi aux journalistes M. Stern, directeur du Laboratoire d'informatique de l'Ecole normale supérieure (LIENS).

Tout le monde utilise maintenant des liaisons sécurisées, fondées sur des protocoles cryptographiques comme SSL, pour effectuer ses paiements sur internet. Arrivent maintenant des systèmes pour la protection des contenus audiovisuels et des données personnelles, notamment médicales. Demain, ce sera le vote électronique qui, lui aussi, aura besoin de faire la preuve de sa fiabilité.

La cryptologie, parce qu'elle a pour objet d'assurer l'intégrité, l'authenticité et la confidentialité des communications, est presque aussi vieille que l'art de la guerre. Jacques Stern lui a d'ailleurs consacré un livre intitulé "La Science du secret". Les armées de Jules César chiffraient déjà de manière très efficace leurs messages. Le premier manuscrit connu sur cette science a été rédigé dès 850 par le savant et philosophe arabe al-Kindi.

Pendant la dernière guerre mondiale, le mathématicien anglais Alan Turing - l'une des sources d'inspiration citées par M. Stern - a joué un rôle déterminant dans la victoire alliée en cassant le code utilisé par les nazis.

A cette époque, la cryptologie est chasse gardée des militaires. La rupture intervient en 1976, avec l'invention de la cryptologie à clef publique. Elle permet d'éliminer tout échange préalable de code et d'instaurer une "signature" permettant de garantir que l'émetteur a bien envoyé le message.

Deux ans plus tard, la création d'un premier algorithme, baptisé RSA, peut faire basculer cette "science des secrets" dans le domaine civil. L'émergence d'internet et des transactions électroniques allait la rendre incontournable.

"La sécurité, a fait valoir M. Stern, c'est une chaîne dont la cryptologie n'est qu'un maillon, mais peut-être son maillon le plus solide", par rapport aux autres failles que sont les systèmes d'exploitation, les intrusions...

Issu des mathématiques, M. Stern est l'auteur de quelque 150 publications dans les revues scientifiques. Il siège aussi dans de nombreux comités officiels, comme l'observatoire de la sécurité des paiements électroniques, un secteur où la sécurité des transactions a été un temps mise en doute.

L'une des spécialités de l'école française de cryptologie, dont M. Stern est le maître incontesté, est l'accent mis sur la sécurité. Ce n'est pas parce qu'un algorithme a résisté aux attaques qu'il est sûr ! En 2000, son équipe a ainsi pu démontrer qu'une norme d'échange électronique était fiable, contrairement à la rumeur qui secouait le monde des utilisateurs de l'internet.

M. Stern affirme que les "hackers" ne l'empêchent pas de dormir. En revanche, les ordinateurs quantiques, sur lesquels travaillent des équipes de scientifiques dans le monde entier, seraient un "cauchemar pour les spécialistes de cryptologie, s'ils devaient voir le jour, puisqu'ils seraient capable de casser nos mécanismes de protection", redoute-t-il.

Post-scriptum :

http://fr.news.yahoo.com/06102006/2...