Record : des chercheurs de l'EPFL cassent une clé de sécurité de 768 bits

- Informatique - Sécurité Informatique -

Date de mise en ligne : vendredi 8 janvier 2010

Spyworld Actu

Une équipe de scientifiques parmi lesquels des chercheurs de l'EPFL sont parvenus à "casser" une clé de sécurité de 768 bits sur internet, battant ainsi un record mondial.

Les systèmes cryptographiques garantissent la sécurité des échanges de données sur Internet : ils sont au coeur du commerce électronique, que ce soit sur les sites "http" ou "https". S'assurer de leur fiabilité est dès lors crucial, souligne l'Ecole polytechnique fédérale de Lausanne (EPFL) vendredi dans un communiqué.

Les chercheurs de l'EPFL, de l'INRIA (France), NTT (Japon), de l'Université de Bonn (Allemagne) et CWI (Pays-Bas) sont parvenus à casser la clé RSA de 768 bits en extrayant les facteurs premiers de ses 232 chiffres. Grâce notamment à la puissance de traitement des processeurs modernes, ce nouveau record mondial a été atteint en moins de deux ans et demi de travaux.

Années de transition

Des calculs du même type ont permis de montrer la vulnérabilité des clés RSA de 512 bits en 1999, puis de 663 bits en 2005 et enfin maintenant de 768 bits. Il faut déjà s'attendre à ce que la clé RSA de 1024 bits utilisée actuellement perde son inviolabilité au cours de la prochaine décennie, relève le communiqué.

Pour Arjen Lenstra, du Laboratoire de cryptologie algorithmique à l'EPFL, ce résultat doit inciter à utiliser de plus hauts niveaux de sécurité que ceux offerts par la clé RSA de 1024 bits. Mais, rassure le professeur, les utilisateurs ne courent pas de grands risques à conserver ce système de chiffrement durant ces prochaines années de transition.

Pour cette expérience, le Laboratoire de cryptologie algorithmique a joué le rôle de coordinateur et de centre de collecte des données. Quant aux logiciels utilisés, ils se sont largement basés sur un développement effectué au début des années 2000 par l'Institut de mathématiques à l'Université de Bonn.

Post-scriptum :

http://www.tdg.ch/epfl-chercheurs-c...