USA : Mise à la retraite du DES

Les entités intéressées ont jusqu'au 9 septembre pour répondre à cet appel. En effet, il s'avère qu'à présent le DES ne répond plus aux critères de sécurité gouvernementaux édictés par cet organisme Américain. Le DES était devenu un standard gouvernemental et industriel depuis 1977, mais l'augmentation des puissances de traitement actuelles, notamment en matière de calcul parallèle, font qu'une attaque par brute force n'est désormais plus « envisageable ». Déjà le 19 janvier 1999, le groupement Distributed.Net – EFF's DES Cracker avait utilisé un peu plus de 100 000 ordinateurs connectés sur la toile pour décrypter un message DES et gagner ainsi le challenge « RSA Data Security's DES Challenge III ». Le temps nécessaire avait été à l'époque de 22 heures 15 minutes en testant 245 milliards de clefs par seconde. Ce retrait ne surprendra donc pas la communauté des spécialistes et des casseurs de codes, qui ont jeté leur dévolu sur l'AES (Advanced Encryption Standard) depuis plusieurs années, pour lequel le NIST donnait son feu vert le 4 décembre 2001. Le DES ne serait dorénavant plus toléré qu'au sein de l'implémentation du Triple-DES, même si les agences fédérales sont vivement encouragées à passer à l'AES, plus rapide et plus robuste.

Cédric Messeguer pour Vulnerabilite.com