Des chercheurs prouvent que le standard AES n'est pas inviolable

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 22 août 2011

L'algorithme utilisé pour sécuriser la plupart des transactions en ligne peut être compromis.

Les chercheurs de Microsoft et des chercheurs néerlandais de l'Université Catholique de Louvain, basée en Belgique, ont découvert comment casser l'algorithme de cryptage Advanced Encryption Standard (AES) utilisé pour sécuriser la plupart des transactions en ligne et les communications sans fil. « Le mode d'attaque mis au point par ces chercheurs est capable de récupérer la clé AES secrète trois à cinq fois plus vite que ce l'on pensait jusqu'ici », a fait savoir l'Université de Louvain. Les chercheurs ont précisé que le mode d'attaque était complexe et qu'il ne pouvait être réalisé facilement avec les technologies existantes. « En pratique, la méthodologie utilisée prendrait des milliards d'années de temps d'ordinateur pour briser l'algorithme AES », précisent-ils.

Lire la suite

Post-scriptum :

http://www.lemondeinformatique.fr/a...