Les serveurs Bull établissent un record en cryptographie

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 21 novembre 2005

Une équipe de chercheurs français, issue de la Direction Générale de l'Armement (DGA/CELAR et DGA/SPOTI) et de l'Université de Versailles-Saint Quentin en Yvelines, a établi un nouveau record dans le calcul de logarithmes discrets. Celui-ci a été atteint à l'aide du supercalculateur TeraNova, un cluster constitué de serveurs NovaScale de Bull. La possibilité de calculer des logarithmes discrets est directement liée à la capacité de trouver les clés de chiffrement utilisées dans l'algorithme de Diffie-Hellman. Cet algorithme à clé publique est couramment utilisé lorsque deux personnes souhaitent échanger des messages confidentiels sans partager initialement de secret. Pour définir leur clé commune de chiffrement, elles échangent, par le biais d'un réseau, deux nombres qui sont l'exponentiation d'une information qui doit rester secrète. Une personne capable de calculer le logarithme discret de ces nombres pourrait remonter à l'élément secret et connaître la clé de chiffrement utilisée. Ce record a été établi sur TeraNova, un cluster de 16 serveurs NovaScale. Malgré la difficulté qu'il représente, il n'a fallu que 13 jours de traitement continu à 64 processeurs pour résoudre ce problème. Cet exploit illustre l'efficacité des processeurs Itanium® 2 pour ces calculs cryptographiques. D'une puissance de 2 teraflops, ce cluster composé de 20 serveurs de 16 processeurs Itanium 2 d'Intel a été déployé dans le cadre du projet TER@TEC qui fait partie du pôle de compétitivité SYSTEMA@TIC. Il est destiné à promouvoir l'utilisation de la simulation numérique et de l'informatique à haute performance au travers de coopération scientifique entre partenaires du monde de la recherche et de l'industrie parmi lesquels Bull et l'Université de Versailles-Saint Quentin.