

Le code de la NSA cassé par des chercheurs français

Le code SHA-0 de la très puissante agence américaine NSA (National Security Agency) spécialisée dans l'écoute des communications électroniques vient d'être cassé. Et par des chercheurs français. Il s'agit d'une première mondiale.

Ces chercheurs, issus de la Direction centrale de la sécurité des systèmes d'information (DCSSI) et de l'Université de Versailles-Saint-Quentin ont utilisé le supercalculateur TeraNova, un ordinateur constitué de grappes de serveurs Bull, ou « cluster ». Ce calculateur, d'une puissance de 1,3 téraflops (1.300 milliards d'opérations par seconde) et composé de 16 serveurs utilisant 16 processeurs Itanium 2 d'Intel, a été installé au centre DAM-Ile-de-France (Direction des applications militaires) du Commissariat à l'énergie atomique (CEA). Il aura fallu trois semaines de calculs ininterrompus, soit 80.000 heures de temps processeurs pour venir à bout de ce code créé en 1990.