



**Hervé Shauer,**  
PDG de HSC

« La cryptographie n'est pas totalement remise en question.

Il s'agit ici d'un problème lié à l'implémentation d'un algorithme cryptographique. Et ce genre de problème n'est pas rare : nombre aléatoire pas vraiment aléatoire, clés faibles, présence de la clé secrète en clair dans la mémoire, etc. Les conditions d'exploitation pour l'attaque citée ici sont difficiles à réunir : cette attaque ne peut pas toucher tous les processeurs, le programme malveillant doit fonctionner au moment précis où la clé est utilisée sur la machine cible... Pour se prémunir contre ce type d'attaque, il suffit d'utiliser une carte consacrée à la cryptographie. Mais, même dans ce cas, les entreprises n'ont pas à s'alarmer. Et le recours à une telle solution doit être réservé aux informations très sensibles. »