Vers une plus grande protection des données chiffrées

- Informatique - Sécurité Informatique -

Date de mise en ligne : jeudi 19 fÃ©vrier 2009

Le chiffrement des données sensibles est indispensable pour assurer leur protection lorsqu'elles sont stockées sur des supports mobiles (ordinateurs portables, clés USB, CD, DVD...). Dans certains cas, au prix de manipulations sophistiquées, on peut cependant récupérer les clés de chiffrement stockées dans la mémoire d'un ordinateur en veille, en hibernation ou qui vient d'être éteint.

Des chercheurs développent donc une technique stockant les clés de chiffrement dans le cache du processeur, et non plus en mémoire.

Source "presse" Counter measure for cold Boot attack - The Register - 19 janvier 2009

Source "doctrine" LestWe Remember : Cold Boot Attacks on Encryption Keys, J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson_, William Paul, oseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten, 21 février 2008, Proc. 2008 USENIX Security Symposium (Lien de téléchargement - http://citp.princeton.edu/pub/coldb...)

[En plus de chiffrer les données sensibles, les utilisateurs doivent assurer une surveillance physique des ordinateurs portables stockant de telles données lorsqu'ils ne sont pas complètement éteints. Lors d'un passage en douane, les ordinateurs portables doivent avoir été éteints plusieurs minutes avant le contrôle pour éviter tout risque que les clés de chiffrement soient récupérées.]

Post-scriptum :

http://www.intelligence-economique....