Protection des données informatiques stockées sur un ordinateur portable

- Informatique - Sécurité Informatique -

Date de mise en ligne : mercredi 28 janvier 2009

Des chercheurs en sécurité informatique de l'Université de Princeton ont proposé une contre-mesure permettant de se défendre contre la technique dite du « cold boot attack ». Cette attaque permet de récupérer les clés de chiffrement stockée dans la mémoire DRAM d'un ordinateur en veille, en hibernation ou qui vient d'être éteint. Ces scientifiques ont donc développé une technique stockant les clés de chiffrement dans le cache du processeur, c'est à dire du matériel dédié et non plus en mémoire.

Cette vulnérabilité informatique peut être exploitée à des fins malveillantes afin d'accéder à des informations sensibles contenues dans des ordinateurs portables. Dans la mesure où les collaborateurs d'entreprise sont de plus en plus nomades dans la gestion de leurs données et leurs transports, si l'un de leurs ordinateurs venait à être dérobé ou examiné dans un court laps de temps, le fait que ces données soient, même, cryptées n'offre pas toutes les garanties pour en assurer leur confidentialité.

C'est pourquoi, il est vivement recommandé, d'une part, de garder une surveillance physique sur votre ordinateur et, d'autre part, d'éteindre votre ordinateur plusieurs minutes avant le contrôle lors d'un passage en douane.

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/coldboot.pdf)

Post-scriptum :

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