Windows et chiffrement BitLocker : une méthode d'attaque

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 7 dÃ©cembre 2009

Spyworld Actu

Les chercheurs allemands de l'institut Frauenhofer pour la sécurité de l'information ont mis au jour une méthode d'attaque à l'encontre de la fonctionnalité de chiffrement des données BitLocker proposée dans Windows Vista et 7.

Le très sérieux institut Frauenhofer va-t-il mettre le feu aux poudres ? Avec les éditions les plus onéreuses de Windows Vista (Professionnelle, Entreprise, Intégrale) et Windows 7 (Entreprise, Intégrale), ainsi que Windows Server 2008, Microsoft propose la fonctionnalité de sécurité dénommée BitLocker. Cette dernière permet le chiffrement de l'intégralité d'un lecteur où résident Windows et les données.

Ce chiffrement de disque utilise les fonctions de la plateforme Trust Computing si un module TPM (Trusted Platform Module) est présent dans l'ordinateur. TPM chiffre les données via une clé stockée à l'intérieur du module. Une lecture des données nécessite donc le même TPM et un état particulier des composants essentiels, explique Frauenhofer. Cet état est vérifié lors de la séquence d'amorçage (boot) avec le BIOS, le chargeur d'amorçage et TPM qui travaillent de concert.

Selon Frauenhofer, un attaquant peut remplacer le code de boot BitLocker initial avec un code remanié et dérober les informations liées à l'interaction avec l'utilisateur. Pendant, le processus de démarrage, BiLocker nécessite en effet une interaction avec l'utilisateur pour obtenir un mot de passe ou/et une clé contenue sur un périphérique USB.

" Ce code de boot modifié ne peut pas permettre de poursuivre la séquence d'amorçage après l'obtention des clés de l'utilisateur. Par contre, il peut restaurer l'état initial du chargeur d'amorçage et provoquer un redémarrage de manière qui semble plausible pour l'utilisateur. Si l'attaquant peut continuer avec ce reboot forcé, une seconde attaque lui permettra de voler les données de l'ordinateur "

, indique Frauenhofer.

L'institut a décrit plusieurs méthodes d'attaque qui entrent dans le cadre de l'espionnage industriel, et l'utilisateur doit avoir accès (physique) à l'ordinateur pris pour cible. Du reste, il n'est pas question de l'exploitation d'un bug dans BitLocker.

Post-scriptum :

http://www.generation-nt.com/bitloc...