Beaucoup de bruit autour de Bitlocker

- Informatique - Sécurité Informatique -

Date de mise en ligne : mercredi 9 dÃ©cembre 2009

L'Institut Fraunhofer s'offre un joli coup de publicité signé Sven Türpe, Andreas Poller, Jan Ste an, Jan-Peter Stotz, et Jan Trukenmüller. Dans une étude de 14 pages, ces spécialistes se sont penchés sur les moyens de contourner Bitlocker, ce système de chiffrement de disque intégré à Vista, Windows 7, et compatible en lecture avec les noyaux XP grâce à Bitlocker-to-go.

Plutôt que de tenter de s'attaquer directement au mécanisme de chiffrement lui-même -lequel est toujours inviolé-, les chercheurs ont tenté de trouver des failles dans l'intégration du système de protection. Et le résultat final est assez convaincant, car il démontre comment contourner un bitlocker reposant sur un TPM, attaque réputée impossible jusqu'à présent. La méthode rappelle par certains aspects celle utilisée par la chambrière diabolique de Joanna Rutkowska. Il y a, derrière cette démonstration, plus de psychologie que de subtil usage de la science informatique, mais seul le résultat compte. Il reste qu'un Bitlocker utilisant un composant TPM et exploité par des usagers méfiants vis-à-vis des clefs USB vagabondes a statistiquement peu de chances de se faire pirater dans l'état actuel des connaissances.

Mais ce que le Fraunhofer présente comme un sujet de recherche, d'autres l'envisagent comme une « suite logicielle commerciale ». Car le Kit Forensic 9.5 de Passware, commercialisé pour la modique somme de 795 $, prétend casser du Bitlocker (entre autres choses) aussi aisément que le L0pht moissonnait de l'authentification NTLM. Il s'agit en fait d'une « attaque en mémoire » nécessitant un accès physique sur la machine protégée. Le logiciel indiscret est disponible en version de démonstration, limité aux trois premiers caractères des mots passe et autres sésames binaires. A noter que cet éditeur offre une version limitée mais gratuite de son analyseur de chiffrement.

Le fait que quelques outils et techniques perfectionnés ou coûteux s'attaquent à cette protection Microsoft ne doit pas faire passer Bitlocker pour une piètre protection. Cet utilitaire peut être employé sur tout ce qui ressemble à un disque, y compris une unité virtuelle au format vhd. Cette astuce permet d'utiliser cet outil de chiffrement pour protéger un ou plusieurs fichiers « contenus » appelés à être transmis par email, ftp etc. Eviter cependant de communiquer le mot de passe ou la clef principale dans le même courrier que celui contenant le fichier protégé.

Post-scriptum :

http://www.cnis-mag.com/beaucoup-de...