La reconnaissance faciale, c'est bidon

- Informatique - Sécurité Informatique -

Date de mise en ligne : vendredi 20 fÃ©vrier 2009

Spyworld Actu

C'est la conclusion à laquelle sont parvenus des chercheurs vietnamiens lors du Black Hat. Ils ont montré que l'on pouvait berner ce système avec de simples photos imprimées.

A l'occasion de la conférence de sécurité Black Hat, qui a eu lieu du 16 au 19 février, une équipe de chercheurs du centre vietnamien Bach Khoa Internetwork Security (Bkis) ont démontré la faible sécurité des systèmes de reconnaissance faciale installés sur certains PC portables Lenovo, Asus et Toshiba.

Ces dispositifs permettent aux utilisateurs de s'authentifier sur Windows simplement en présentant leur visage à la webcam intégrée de l'ordinateur. Un logiciel numérise le visage de l'utilisateur et, grâce à un algorithme, en extrait les points remarquables pour les comparer aux empreintes numériques précédemment répertoriées dans sa base de données.

Pratique, mais inefficace

Comme tous les systèmes d'authentification biométriques, la reconnaissance faciale est pratique, rapide et confortable. Pas besoin de se souvenir d'un mot de passe. Pas de temps perdu à taper de longues séries de chiffres, de lettres ou de caractères spéciaux. Le problème, selon les chercheurs vietnamiens, c'est que la reconnaissance faciale ne vaut pas un clou.

Pour duper les logiciels, ils ont imprimé le visage de l'utilisateur sur une feuille de papier et tendu celle-ci face à la webcam. Bingo ! Les portes de Windows se sont ouvertes. Les chercheurs ont immortalisé leur piratage dans une vidéo, disponible sur le site du centre de recherche (notez que le temps de téléchargement est plutôt long). Une présentation peut également être téléchargée sur le site de la conférence Black Hat.

Toutefois, les trois logiciels testés ne sont pas aussi inefficaces les uns que les autres. Le moins sécurisé est celui de Lenovo, Veriface III. Une photo imprimée en noir et blanc suffit pour s'authentifier. Pour Asus SmartLogon, les chercheurs ont dû modifier la luminosité ainsi que l'angle de la prise de vue. Le logiciel le plus difficile à tromper a été Toshiba Face Recognition, qui contraint systématiquement à tester une série d'impressions avec des effets de lumière et des angles de vue différents avant de pouvoir pénétrer le système.

En rester au bon vieux mot de passe

Cette démonstration de piratage biométrique rappelle celle de l'association allemande Chaos Computer Club, qui, en 2004, avait piraté un système d'authentification par empreinte digitale, simplement grâce à un peu de bricolage.

Pour les experts d'Hervé Schauer consultants, le piratage de la reconnaissance faciale n'est pas si étonnant. « C'est une technologie encore assez récente, qui doit mûrir. Pour une entreprise, le mieux, c'est la politique de sécurité basique : avoir des mots de passe longs, de dix caractères au moins, et qui changent fréquemment. En cas de besoin, on peut éventuellement associer au mot de passe une carte d'authentification », estime Matthieu Hentzien, responsable commercial.

Post-scriptum :

http://www.01net.com/editorial/4038...