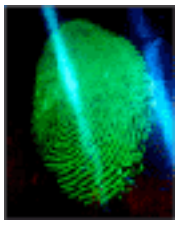
Biométrie : des chercheurs américains améliorent la sécurité des technologies

- Technologie -



Date de mise en ligne : vendredi 4 avril 2008

Spyworld Actu

Le Nist a présenté deux modèles d'authentification destinés à l'accès sécurisé des personnels fédéraux.

Les chercheurs de l'US National Institute of Standards and Technology (Nist) ont mis au point une technologie d'identification par empreintes digitales qui répond aux critères de précision standard pour les cartes d'identification fédérales.

Homeland Security Presidential Directive 12 stipule que la plupart des employés et sous-traitants d'organismes fédéraux devront utiliser des cartes PIV (Personal Identification Verification) d'ici l'automne prochain. Les cartes PIV seront nécessaires pour "authentifier" l'identité des utilisateurs à l'entrée des bâtiments fédéraux.

Le Nist a publié en 2006 une norme pour les nouveaux identifiants qui spécifie que les cartes stockent une représentation des caractéristiques clés ou "points caractéristiques" des empreintes digitales de l'utilisateur afin d'établir son identification biométrique.

Sous la norme actuelle, un utilisateur cherchant à pénétrer dans un point d'accès à contrôle biométrique doit insérer la carte PIV dans un dispositif et placer ses doigts sur un scanner.

L'authentification s'effectue en deux étapes : le détenteur de la carte saisit un code PIN pour permettre la lecture de ses caractéristiques digitales à partir de la carte, et le lecteur de carte vérifie la concordance des données stockées avec la nouvelle image scannée des empreintes digitales.

Au cours de tests récents, les chercheurs du Nist ont évalué la précision et la sécurité de deux variations sur ce modèle qui, s'ils sont acceptés pour un usage gouvernemental, offriraient des fonctionnalités améliorées.

Dans le premier modèle, les données biométriques stockées sur la carte transitent par une interface sans fil sécurisée, ce qui évite d'avoir à insérer la carte dans un lecteur.

Le second modèle utilise une technique d'authentification alternative appelée 'match-on-card' dans laquelle les données biométriques provenant du scanner d'empreintes digitales sont envoyées vers la carte PIV afin d'évaluer leur concordance grâce à un processeur intégré dans la carte.

Les données caractéristiques stockées ne quittent jamais la carte. Selon l'informaticien Patrick Grother, cette technique présente l'avantage d'éviter toute copie du modèle d'empreinte en cas de perte de la carte.

Les tests réalisés par le Nist ont répondu à deux questions majeures relatives à l'utilisation de la technologie match-on-card. La première était de savoir si les 'clés' électroniques de la carte pouvaient maintenir une transmission de données sans fil sécurisée entre le lecteur d'empreintes et la carte et vérifier la concordance des données en 2,5 secondes.

La seconde question consistait à déterminer si l'opération match-on-card produirait autant d'acceptation et de refus erronés que les techniques match-off-card traditionnelles où la puissance de calcul disponible est supérieure.

Selon les chercheurs, 10 cartes utilisant une clé 128 octets standard et sept cartes utilisant une clé 256 octets plus sécurisée ont passé avec succès les tests de sécurité et de rapidité via une transmission sans fil.

Sur le plan de la précision, une équipe a répondu aux critères établis par le Nist et deux autres les ont manqués de peu. Les informaticiens ont prévu une nouvelle campagne de tests afin d'élargir la participation.

Traduction de l'article US boffins boost fingerprint recognition security de Vnunet.com en date du 3 avril 2008.

Post-scriptum :

http://www.vnunet.fr/fr/news/2008/0...