IDEMIA

Vous avez vu ? Le PIN a disparu !

(Article 2/3) - Par Philippe Le Pape, expert sécurité et identité, Vice-Président du développement international et des partenariats au sein de la division Digital Security & Authentication de Safran Identity & Security (ex Morpho).

IDENTITÉ

POSTÉ LE 06.30.16

Aborder le thème de l'**authentification à deux facteurs**, c'est se pencher sur ce qui renforce l'authentification : quelque chose que l'utilisateur connait, quelque chose qu'il possède ou dont il est inséparable. Nous pourrions revoir la notion de « quelque chose dont il ne peut se séparer » et parler de « ce qu'il est », le corps humain offrant d'excellentes possibilités d'identification. Les empreintes digitales, par exemple, sont utilisées depuis la fin du XIXe siècle par les services de police du monde entier pour identifier des suspects.

L'authentification biométrique s'appuie sur des identifiants physiologiques (empreintes digitales, visage, iris) pour confirmer l'identité d'une personne. Un système biométrique est un système de reconnaissance des formes : les données biométriques d'une personne sont comparées à celles enregistrées. Fondamentalement, la biométrie est la seule manière de relier l'identité physique d'une personne à son identité numérique.

Un système biométrique type se compose de cinq éléments majeurs : un capteur pour saisir et numériser les données, des algorithmes de traitement des signaux pour former le modèle biométrique, une unité de stockage des données, un algorithme de correspondance pour comparer de nouveaux modèles à ceux déjà enregistrés et stockés, et un processus de décision qui s'appuie sur les résultats de l'algorithme de correspondance pour accepter ou rejeter le profil étudié.

Le type d'**authentification biométrique** utilisé dépend de l'application visée, notamment du niveau de sensibilité et des risques en matière de sécurité dans le cadre de la transaction numérique concernée. La gestion de la confidentialité des données revêt un caractère encore plus essentiel lorsque l'authentification de l'utilisateur a lieu dans le Cloud. Tout système biométrique, en particulier celui qui suppose l'interconnectivité, doit être soigneusement conçu afin d'éviter la perte ou l'interception des données biométriques de l'utilisateur. D'une manière générale, ces systèmes prévoient des protections cryptographiques pour prévenir l'interception des données biométriques lors de la transmission. De la même manière, lorsqu'un modèle biométrique est stocké dans un appareil, il est protégé par des outils de cryptographie et de cryptage.

Le processus d'identification qui s'appuie sur des caractéristiques biométriques est plus performant que les méthodes traditionnelles reposant sur l'association de mots de passe et codes PIN, et ce pour plusieurs raisons :

1. Simplicité d'utilisation :

- L'identification grâce aux techniques biométriques exclut la nécessité de se souvenir d'un mot de passe ou d'avoir un objet sur soi. Le logiciel et le matériel sont par ailleurs conçus pour être simples d'utilisation. Même dans des conditions de forte luminosité où les écrans sont difficiles à lire, les techniques biométriques sont simples à utiliser, tandis qu'il est difficile de saisir son mot de passe.
- Si la technologie biométrique offre des résultats précis, elle est également peu invasive. En règle générale, un scan ou une photo suffisent.
- Autre avantage par rapport aux mots de passe traditionnels, en particulier sur les outils mobiles dotés de petits claviers, l'identification biométrique est extrêmement rapide.

2. Sécurité renforcée :

- Les caractéristiques morphologiques, comme les **empreintes digitales** ou l'**iris**, sont le fondement de méthodes d'identification précises et uniques. Elles sont difficiles à dupliquer et ne peuvent être exploitées directement pour usurper une identité. Elles assurent un rempart de sécurité élevé, car le système reconnait uniquement la personne autorisée.

La technologie biométrique a évolué, depuis les applications militaires très ciblées jusqu'à une utilisation plus large dans la justice criminelle et, plus récemment, dans le domaine des solutions d'identité civiles abondamment utilisées. Aujourd'hui, les données biométriques sont déjà utilisées pour gérer et protéger l'identité unique des personnes et lutter contre les escroqueries. À titre d'exemple, au Royaume-Uni, Safran accompagne le nouveau programme GOV.UK Verify, mis en place par les autorités publiques afin de permettre aux citoyens de prouver leur identité en ligne et d'accéder en toute sécurité à divers services publics, du renouvellement du permis de conduire à la déclaration de revenus en ligne. Le processus de **vérification de l'identité** comprend différents niveaux de garantie déterminés en fonction du type d'informations à fournir par l'utilisateur. Le niveau de garantie le plus élevé (niveau 4) fait appel à des outils particuliers, comme la biométrie, afin de renforcer la protection contre les risques d'usurpation ou de fabrication d'identité.

Un programme similaire, baptisé Idensys, est actuellement mis à l'essai aux Pays-Bas.

Pour conclure cette série de publications, découvrez dans l'article ci-dessous, **La Planète du tout mobile (3/3)**, comment la technologie mobile peut devenir la solution pour les problématiques liées à d'identité civile.