Détection du vivant : pour une authentification biométrique encore plus sûre

Face à la multiplication des attaques informatiques et à l'usurpation d'identité, Morpho élève encore d'un cran la fiabilité de ses systèmes d'authentification biométrique. Comment ? En détectant le vivant pour déjouer les fausses empreintes, les photos ou autres données biométriques artificielles.

 # IDENTITÉ

POSTÉ LE 05.03.16

La biométrie est aujourd'hui sans conteste la méthode à la fois la plus pratique et la plus sûre pour authentifier une personne. Elle permet de confirmer que l'utilisateur est bien celui qu'il prétend être tout en apportant un confort d'utilisation quotidien optimal. Parmi toutes les biométries, la reconnaissance d'empreinte digitale d'abord, popularisée par le TouchID d'Apple, puis la reconnaissance faciale se sont rapidement développées sur le marché du mobile. De la même manière, dans les applications les plus sensibles telles que le contrôle d'accès, l'authentification des paiements ou le passage aux frontières, ces deux biométries sont devenues LE facteur clé de l'authentification. Cependant, les systèmes biométriques peuvent devenir vulnérables face à des attaques au moyen de faux échantillons biométriques comme la photo d'un visage ou l'utilisation de faux doigt.

Comment parer à ces nouvelles tentatives ? En incluant une nouvelle technologie aux capteurs biométriques ; la **reconnaissance du vivant**.

En effet, la capacité à détecter le vivant renforce considérablement la sécurité et la fiabilité des systèmes biométriques. Depuis plusieurs années, Morpho développe ces technologies. Dès 2013, Morpho était le premier à certifier sa technologie de reconnaissance de faux doigts, capable de mesurer les caractéristiques spécifiques de la peau humaine.

Aujourd'hui, Morpho innove pour accompagner le déploiement de la reconnaissance faciale dans les applications grand public en présentant la détection du vivant appliquée à la reconnaissance faciale. Installée par exemple sur un smartphone équipé d'un capteur vidéo, elle permet à l'utilisateur de s'authentifier rapidement et naturellement de manière sécurisée. C'est le « **selfie-check** ». Mais à la différence d'autres technologies du marché, ce selfie-check ne peut être trompé par l'emploi d'une photo.

Comment ça marche ? Au moment de l'authentification, les algorithmes vont vérifier que le selfie réalisé par l'utilisateur du smartphone correspond à la biométrie préalablement enregistrée par son propriétaire et si elle est réalisée en « live ». La technologie va alors s'aider par exemple des mouvements de l'arrière-plan pour reconstituer le visage de l'utilisateur en 3D. Anne Bouverot a récemment participé au Mobile World Congress au cours duquel elle a effectué, en direct, une démonstration de reconnaissance faciale sur smartphone avec cette technologie.

Dans le cadre d'applications très critiques, combinée à d'autres facteurs d'authentification biométrique, « ce que l'utilisateur possède » (un smartphone, un token sécurisé) et « ce que l'utilisateur sait » (un code PIN), cette nouvelle

technologie représente un gain considérable en matière de sécurité.