EcoRéseau

PAYS : France
PAGE(S) :58,59
SURFACE :104 %
PERIODICITE : Bimestriel

JOURNALISTE : Jean-Marie Benoist

► **1 décembre 2016 - N°36**

Focus sur un sujet high tech dans l'air du temps

À l'aube de la révolution

La créativité parle dans le monde du paiement, entraînant de nouveaux challenges en matière de sécurisation, qui pourraient bien aboutir à réorganiser le marché.

Le marché du paiement est en pleine ébullition : il semble que tous les mois de nouvelles façons de payer fassent leurs débuts, toutes plus «ésotériques» les unes que les autres. Récemment, Mastercard annonçait tester le paiement par selfie ! Ce foisonnement d'innovations est en fait motivé par deux facteurs : une sécurisation croissante des transactions, et une demande – aussi bien des commerçants que des utilisateurs – de simplification toujours plus poussée de l'acte en lui-même. Un vrai jeu d'équilibriste – en fait, « *il s'agit d'arriver à un équilibre entre la facilité d'usage et un niveau de sécurité acceptable* », résume Loïc Dequay, chef de produit Innovation Paiement mobile Acceptation chez Monext.

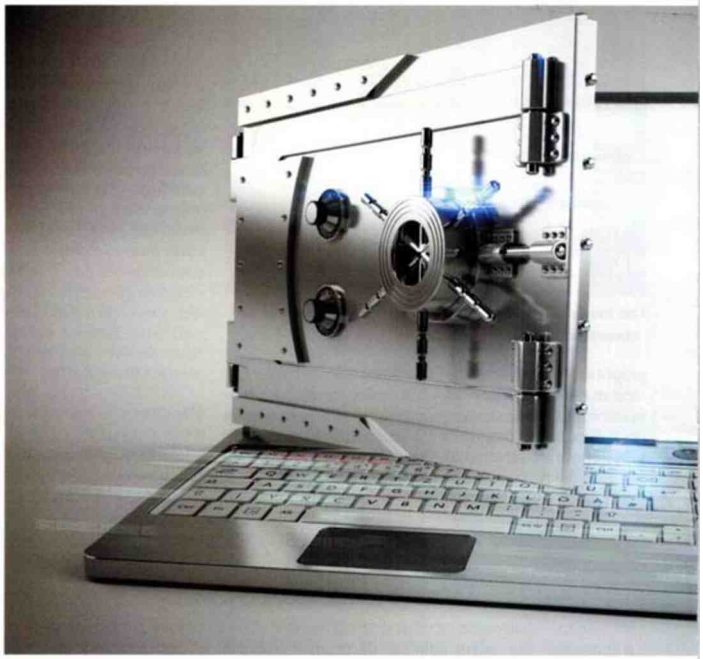
L'IDENTIFICATION PAR LE CORPS

Les innovations les plus excitantes ont recours à la biométrie, basée sur les caractéristiques corporelles. Iris, fond d'œil, réseaux veineux, empreinte digitale, voix, voire selfie… les idées ne manquent pas. Et elles ont l'énorme avantage d'être facilement adoptées par les utilisateurs. « *Néanmoins, toute forme d'identification biométrique a ses faiblesses* », souligne Richard Lack, directeur des ventes EMEA chez Gigya. Une photo suffisait à tromper l'identification d'iris (il faut maintenant cligner des yeux) ; de la pâte à modeler suffit à passer outre des capteurs d'empreinte digitale (ou simplement le vrai doigt du propriétaire, endormi ou ivre). C'est une des raisons pour lesquelles « *il n'existe pas encore de réglementation sur l'utilisation de critères biométriques pour l'identification chez les grands réseaux de paiement, à l'exception de l'empreinte digitale pour les wallet mobiles (ApplePay, SamsungPay, AndroidPay…)* », rappelle Vincent Ducrohet, directeur Next Generation Offering / LABS chez Ingenico. Tous ces projets sont donc des pilotes.

> *Les moyens d'authentification implicites sont une demande récurrente de la part des commerçants*

PAR L'OBJET

L'autre type majeur d'innovation se concentre sur les objets connectés utilisant le NFC, comme les bracelets (tels qu'expérimentés par Gemalto lors de l'Euro 2016). Plus facile à sécuriser (la technologie est mieux maîtrisée), ils posent cependant des problèmes de distribution et de gestion (perte, casse…). Mais Visa et Mastercard ont ouvert leur plateforme de *tokenisation* (qui utilise un numéro généré au hasard au lieu des coordonnées bancaires) aux fabricants. Autrement dit, n'importe quel objet connecté peut être doté de capacités de paiement. Ce qui n'est pas forcément une bonne nouvelle : régulièrement, des objets connectés se font pirater, de la voiture au frigo. Un objet en particulier sort du lot : le smartphone. Il possède à la fois les ca-



Dans ce domaine, les solutions radicales et indestructibles n'existent pas.

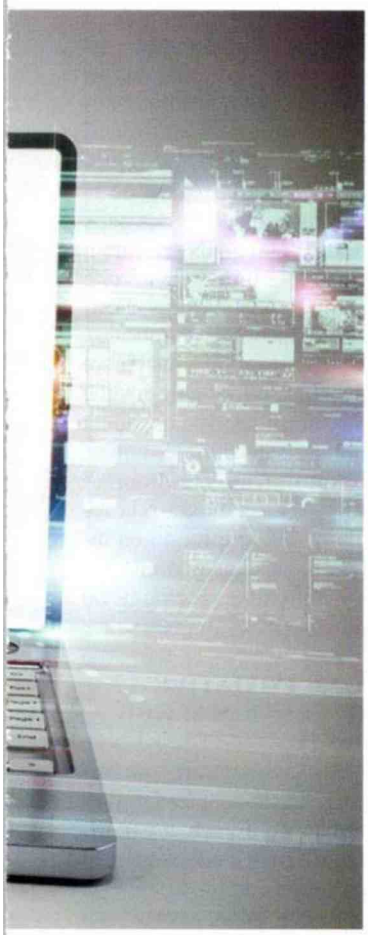
EcoRéseau

PAYS : France
PAGE(S) :58,59
SURFACE :104 %
PERIODICITE : Bimestriel

JOURNALISTE : Jean-Marie Benoist

► **1 décembre 2016 - N°36**

pacités techniques pour procéder à différentes identifications (SMS, appareil photo, NFC…), est omniprésent, et d'un maniement aisé pour l'utilisateur, dont il a une très (certains diraient trop) bonne connaissance. C'est d'ailleurs ce que cherche



à exploiter Google, avec son projet Abacus. « *Pendant que vous utilisez votre téléphone, l'application tourne, et rassemble des données sur vous et vos habitudes d'utilisation : comment vous tapez, vos endroits habituels, votre vitesse, votre empreinte vocale…* », explique Richard Lack. Puis elle utilise ces données pour vous identifier. Les résultats sont, paraît-il, bluffants.

Par les habitudes

Abacus va en fait bien au-delà de l'objet connecté, même s'il en utilise un : il s'agit plutôt d'une solution dite implicite. L'idée est, grâce à une connaissance client approfondie, de détecter les comportements inhabituels et de ne déclencher les authentifications fortes qu'à ce moment-là. C'est notamment la position prise par Amazon, qui ne veut pas se débarrasser de son fameux « one-click ». C'est le top de la fluidité – et du coup, « *les moyens d'authentification implicites sont une demande récurrente de la part des commerçants* », explique Loïc Dequay. Outre les habitudes de consommation, d'autres solutions implicites pratiquent le « device fingerprinting », en identifiant l'utilisateur grâce à son environnement réseau (les adresses mac des appareils connectés, leur système d'exploitation…).

Les favoris

Parmi ce fourmillement d'innovations, deux mé-

EcoRéseau

PAYS : France
PAGE(S) :58,59
SURFACE :104 %
PERIODICITE : Bimestriel

JOURNALISTE : Jean-Marie Benoist

► **1 décembre 2016 - N°36**

thodes sortent du lot. Apple Pay, avec l'empreinte digitale, qui rentre déjà bien dans les mœurs ; et la reconnaissance vocale, qui commence à être expérimentée dans le monde du paiement. « *Comme pour l'empreinte digitale, le grand public, grâce aux assistants personnels virtuels (Cortana, Siri…), est déjà familiarisé avec la technologie* », souligne Vincent Ducrohet.

De fait, si l'évolution est inéluctable, il est difficile de prédire quelle sera l'innovation qui se hissera au-dessus du lot et deviendra la nouvelle norme – ou du moins le moyen de paiement majoritaire. C'est l'utilisateur qui décidera, et tous les jours arrivent des nouveaux systèmes, des nouveaux moyens de contrôle biométriques ou logiciels… Et, tous les jours ou presque, des problèmes de sécurité apparaissent, des brèches – et aujourd'hui, un seul incident peut entacher la réputation d'un produit suffisamment longtemps pour lui faire perdre sa chance. ●

Détecter les comportements inhabituels et ne déclencher les authentifications fortes qu'à ce moment-là

Jean-Marie Benoist