

La biométrie: de James Bond à la porte de votre garage

INTERVIEW DE MOHAMMED SALAH OKA, CO-DIRECTEUR DE KALYSS S.A.

«**U**n homme habillé de noir s'approche de la porte blindée de la chambre forte où les secrets de la super bombe sont enfermés. Il passe son badge devant un scanner puis présente son œil devant un rayon laser qui scrute le fond de sa rétine. Après quelques secondes, la porte s'ouvre et l'homme pénètre dans le saint des saints.»

Le Chênois: Une telle scène relève-t-elle du roman policier?

Mohammed Salah Oka: Non, pas vraiment! La reconnaissance par l'œil est de plus en plus utilisée, mais pas exactement comme dans le passage que vous venez de citer! Cela fait partie des systèmes de sécurité qu'utilise la biométrie.

Qu'est-ce au juste que la biométrie?

Le terme "biométrie" désigne l'ensemble des procédés de reconnaissance automatique d'une personne par certaines de ses caractéristiques physiques (morphologiques, biologiques). Le mot "biométrie" est en réalité un anglicisme dérivé du terme *biometrics*. La langue française avait bien "anthropométrie", mais, limité aux mesures du corps humain; il a été écarté au profit de "biométrie", plus moderne et qui inclut la notion de traitement informatique.

Les caractéristiques physiques peuvent-elles changer avec le temps?

Oui et c'est pourquoi le choix des caractéristiques physiques est important. Il faut qu'elles soient tout à la fois: discriminantes, pour différencier les personnes sans équivoque; invariables, pour assurer leur permanence; universelles, pour être appliquées à tout le monde; faciles à exploiter et acceptables culturellement par les utilisateurs et difficilement falsifiables. C'est le cas de l'ADN, de l'iris, des empreintes digitales, de la reconnaissance faciale, de la géométrie de la main, de la rétine, des veines... Ces éléments ont l'avantage d'être plus ou moins stables dans la vie d'un individu et ne subissent pas autant les effets du stress que la signature par exemple.

Pourquoi utiliser des systèmes aussi complexes?

Tout d'abord, il faut bien mettre les choses au clair: ces systèmes sont de plus en plus courants et pour certains de moins en moins coûteux: pour quelques francs, vous avez actuellement des clés USB qui "reconnaissent" vos empreintes digitales. D'autre part, la biométrie répond à une demande effective. Vous avez, j'en suis certain, plusieurs cartes dans votre portefeuille: à chaque carte correspond un code pin. Pour entrer chez vous vous avez besoin d'un autre code, de même pour utiliser



Photo: J. M. Jakobowicz

vos téléphone portable. De plus, dans les entreprises, l'accès aux ordinateurs se fait à l'aide de codes qui doivent être changés fréquemment. Ce qui veut dire que soit vous êtes obligé de mémoriser une dizaine, voire une vingtaine de codes, soit vous utilisez toujours le même relativement simple donc aisément reproductible. En plus, rien ne garantit que lorsque vous consultez votre compte en banque sur Internet, c'est bien vous qui êtes devant votre écran; il peut s'agir de n'importe qui, qui usurpe votre identité. L'avantage de la biométrie c'est qu'à la fois la machine est certaine que c'est de vous qu'il s'agit parce que certains critères physiques sont présents devant la caméra ou le scanner et en plus vous n'êtes plus obligé d'avoir une banque de données à la place du cerveau pour emmagasiner tous vos codes!

Mais ces critères sont-ils vraiment uniques?

Une empreinte digitale est le dessin formé par les lignes de la peau des doigts, son caractère quasi-unique en fait un outil biométrique très utilisé pour l'identification des individus. En effet, la probabilité pour que deux personnes aient la même empreinte est très faible, même à l'échelle de l'humanité. On estime à 1/64 milliards la probabilité pour que deux individus aient les mêmes empreintes digitales. Il faut bien avouer que ce n'est pas un système très nouveau puisque l'empreinte du pouce servait déjà de signature lors d'échanges commerciaux à Babylone (-3000 av. J.-C.)! Quant à l'iris, il n'y en a pas deux identiques même au niveau d'une seule personne: les iris des deux yeux sont différents. Ce qui permet à certaines banques d'offrir un service un

peu spécial à certains clients: suivant que le client présente l'œil droit ou l'œil gauche devant la caméra il aura accès à ses comptes ou à des comptes fictifs. Ainsi, un client qui serait contraint par la force de dévoiler ses comptes aurait comme ultime ressource de déclencher une alarme en présentant le mauvais œil devant la caméra sans pour autant éveiller les soupçons de son agresseur.

Qui utilise la biométrie?

De plus en plus d'entreprises ont un besoin énorme de sécurité, car leurs employés deviennent de plus en plus "nomades", soit qu'ils travaillent à la maison ou carrément dans d'autres pays; il faut à tout prix que les échanges qu'ils ont entre eux ou avec la maison-mère soient sécurisés. Le secteur financier qui travaille lui aussi de plus en plus avec Internet a ce même besoin de sécurité. Les personnes privées utilisent, elles aussi, la biométrie et là les applications sont multiples: elles vont depuis la porte du garage que l'on peut ouvrir avec les empreintes digitales jusqu'au coffre-fort ou les dossiers dans l'ordinateur individuel. D'ailleurs, à ce niveau, la biométrie va non seulement permettre de mettre en marche l'ordinateur et de consulter un dossier sécurisé, mais aussi de crypter certains documents dont l'utilisateur est le seul à posséder la clé. Les gouvernements utilisent eux aussi la biométrie.

En imposant des passeports biométriques à leurs citoyens?

C'est en effet l'une des utilisations. Ces passeports sont infalsifiables et ils associent certains critères physiques avec le détenteur du document. Ce qui fait qu'un nom est associé avec des critères biométriques et à un document. Ainsi, les trois sont indisso-

ciables. Si une personne présentant certains critères biométriques arrive à la frontière avec un passeport et un nom différents, il sera immédiatement repéré. Pour certains pays qui ont des problèmes de sécurité, ce sont des "armes" imparables. Si vous prenez, par exemple, les pays du Golfe qui connaissent une très forte immigration de travailleurs en provenance d'Asie, s'ils renvoient certains d'entre eux pour une raison ou pour une autre, la personne indésirable ne pourra plus jamais y revenir, même avec de faux papiers. Un détail: la biométrie, surtout la méthode de reconnaissance de l'iris, présente un intérêt certain pour les pays où les femmes sont voilées: elles peuvent être identifiées sans avoir besoin d'enlever leur voile...

Tout cela fait un peu peur!

Effectivement, ce système peut faire penser à "Big Brother". Heureusement, il existe dans de nombreux pays des lois qui régissent la détention de ces données biométriques. Ainsi, en France, leur stockage est interdit. Et certaines données sont interdites d'accès en particulier dans le domaine de la santé. C'est pourquoi je vous disais au début que le laser qui scrute le fond de l'œil n'était pas réaliste, car c'est une technologie intrusive qui permettrait de connaître certaines caractéristiques vitales. Mais n'oubliez pas que le but final est d'accroître notre sécurité à tous!

Que fais Kalyss, votre entreprise?

Nous conseillons et mettons en place ces systèmes parfois très sophistiqués. Que ce soit au niveau des personnes privées, mais plus généralement au niveau des entreprises. Mais nos compétences ne se limitent pas à ça, puisque nous sommes un groupe d'ingénieurs et de consultants spécialisés dans le développement et l'implémentation de logiciels basés sur les "technologies O.O." (Java/J2EE) qui requièrent un niveau d'expertise de plus en plus élevé. Nous proposons une expertise pour effectuer les bons choix technologiques et définir une architecture adéquate et évolutive. Nous sommes tout particulièrement compétents dans les technologies de Développement Objet et Distribué, nous maîtrisons la conception et l'implémentation de logiciels Internet-Intranet-Extranet sur mesure.

Jean Michel Jakobowicz

Kalyss S.A.
Rue Peillonex, 39
1225 Chêne-Bourg
<http://www.kalys.com/>