Gouvernement en ligne

Recherche

>>

e-Veille

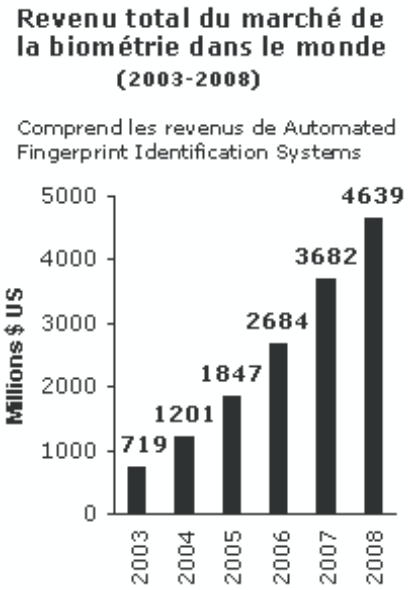
À la rencontre des gouvernements en ligne du globe

Novembre 2004

La biométrie pour authentifier l'identité des citoyens. De la science-fiction à la réalité.

Biométrie : le mot de passe de demain ?

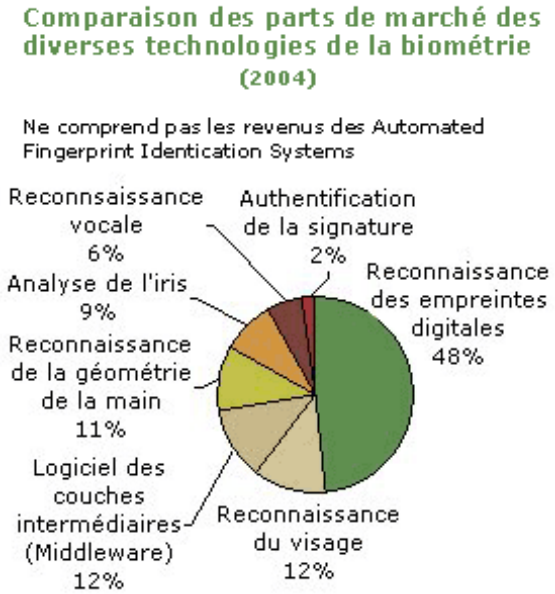
Identifier une personne de manière irréfutable, voilà le rêve de bien des organisations dont les services se fondent sur des données sensibles et confidentielles. La biométrie se définit comme l'analyse mathématique des caractéristiques biologiques ou comportementales d'une personne, destinée à déterminer son identité. Parmi les techniques les plus connues, notons la reconnaissance de l'empreinte digitale ou l'analyse de l'ADN.



La question demeure : les technologies biométriques sont-elles réellement infaillibles ? La réponse : non. D'abord, certaines caractéristiques physiques peuvent être falsifiées. Pensons notamment à l'ajout de prothèses qui changent la forme d'un visage ou le port d'une lentille qui imite le dessin d'un iris. Certaines caractéristiques peuvent aussi être altérées dans le temps (vieillissement, maladie, changement de comportement, etc.) ou quelque peu modifiées par des conditions environnementales (saleté, humidité ou autres). Une coïncidence absolue, c'est-à-dire 100 % de similitude entre le fichier « signature » créé lors de l'enregistrement de la personne et le fichier utilisé lors de la vérification, s'avère donc impossible. Les performances des systèmes d'authentification se mesurent par deux taux :

- le taux de faux rejets (T.F.R.) : pourcentage de personnes rejetées par erreur ;
- le taux de fausses acceptations (T.F.A.) : pourcentage d'acceptations qui n'auraient pas dû être retenues.

Ces taux varient selon la qualité des systèmes, mais aussi selon le niveau de sécurité désiré.



Malgré ces imperfections, il n'en reste pas moins que l'utilisation de technologies biométriques est en plein essor, surtout depuis les évènements du 11 septembre 2001. L'International Biometric Group prévoit, d'ailleurs, une forte croissance du marché de cette technologie dans les années à venir. Les revenus globaux de la biométrie, qui sont passés de 719 millions de dollars américains en 2003 à 1,2 milliard en 2004, atteindraient les 4,6 milliards en 2008. La reconnaissance des empreintes digitales, qui génère à elle seule près de la moitié des revenus mondiaux du domaine de la biométrie, représente, sans conteste, la plus grande part du marché actuel de la technologie biométrique.

La biométrie, en permettant de sauvegarder l'identité et l'intégrité des données, peut être l'alliée de la vie privée, mais, comme nous le verrons plus loin, elle comporte également son lot d'enjeux à l'égard de la sécurité des renseignements recueillis et de leur utilisation.

Rédactrice : Isabelle Vachon, analyste-conseil, Enquêtes et Veille stratégique, CEFRIO
Sources : International Biometric Group. *Biometrics Market and Industry Report 2004-2008*, 2004, 272 pages. Faits saillants disponibles gratuitement.
Office québécois de la langue française. « Biométrie », « Biométrie comportementale » et « Biométrie physiologique », *Grand dictionnaire terminologique*, 2004.
Securiteinfo.com. « La biométrie », « Les technologies biométriques », 2004.

Obéir plus qu'au doigt et à l'œil : les diverses technologies biométriques

La mesure biométrique peut reposer sur deux types de caractéristiques propres à chaque individu, soit les caractéristiques physiologiques et comportementales. D'une part, la biométrie physiologique s'appuie sur diverses données corporelles. Parmi les caractéristiques physiques particulières à chacun, on retrouve les empreintes digitales, l'iris, la rétine et l'ADN. D'autre part, certains comportements permettent d'identifier les personnes, tels que la façon de signer, de marcher ou de taper sur les touches d'un clavier. Il s'agit alors de mesures dites comportementales, fondées sur la reconnaissance d'une façon d'exécuter une action acquise au fil du temps. Chaque mesure, physiologique ou comportementale, comporte des avantages et des inconvénients. Le choix de l'une ou l'autre des technologies repose sur le degré de sécurité souhaité, le budget disponible et le contexte de son utilisation.

Biométrie physiologique

La *reconnaissance des empreintes digitales* constitue la technique biométrique de type physiologique la plus ancienne et la plus répandue. Elle est, en outre, largement utilisée par la CIA depuis les années 1960. Cette mesure est obtenue d'après le dessin représenté par les crêtes et les sillons de l'épiderme d'un doigt. Des capteurs optiques, des capteurs ultrasoniques ainsi que des capteurs de champ électrique ou de température permettent d'obtenir diverses données sur les empreintes digitales. La *reconnaissance de la forme de la main ou des doigts* figure également parmi les techniques biométriques les plus répandues, notamment aux États-Unis. Elle consiste à mesurer plusieurs caractéristiques de la main, telles que sa forme, la longueur et la largeur des doigts ou la forme des articulations. Elle s'appuie sur une image en trois dimensions obtenue par imagerie infrarouge. Ces deux techniques — soit la reconnaissance des empreintes digitales et de la forme de la main et des doigts — sont surtout utilisées pour contrôler l'accès à des locaux, à des machines, à des équipements spécifiques ou encore à des systèmes d'information. De plus, la reconnaissance de la forme de la main a été utilisée lors des Jeux olympiques d'Atlanta et est actuellement en cours d'utilisation pour offrir aux voyageurs un accès rapide aux aéroports. Environ 60 000 personnes seraient inscrites à ce service dans les aéroports des États-Unis et du Canada.

Deux composantes de l'œil peuvent également servir à l'identification des individus, soit l'iris et la rétine. Considéré comme le « fleuron de la biométrie », le *balayage de l'iris* obtient un taux d'erreur pratiquement nul. L'iris, anneau visible coloré de l'œil, comporte un dessin unique à chaque personne. Plus encore, les deux yeux d'une même personne présentent des dessins distincts. On obtient un cliché de ce dessin en utilisant un capteur d'image sous un éclairage artificiel calibré (diodes électroluminescentes [DEL]), l'éclairage ambiant étant atténué le plus possible. L'accès rapide des voyageurs aux aéroports et le passage accéléré aux douanes, le contrôle de l'accès à des distributeurs de billets de banque, à des locaux ou à des systèmes informatiques ne sont que quelques-unes des applications possibles de la reconnaissance de l'iris comme instrument biométrique. Quant à la *reconnaissance de la rétine*, elle repose sur le dessin formé par la vascularisation près de la rétine. Ce schéma veineux est propre à chaque personne et permet même une différenciation entre jumeaux. Une lumière infrarouge de forte intensité scanne la rétine de l'œil. Cette technique, plus ancienne que celle du blayage de l'iris, n'obtient pas la même cote de popularité. Elle requiert que la mesure soit prise à quelques centimètres seulement de l'appareil, ce qui en rebute plusieurs. Quoi qu'il en soit, la rétine demeure la caractéristique physique qui s'altère le moins au cours de la vie. On utilise surtout cette technique pour contrôler l'accès à des distributeurs automatiques de billets.

Moins fiable que les techniques décrites précédemment, l'*analyse de la forme du visage* croît néanmoins en popularité. Cette mesure s'obtient à partir de diverses photographies plus ou moins évoluées du visage. De ces photos sont extraits des éléments propres à chaque individu, choisis pour leur forte invariabilité, tels que le haut de la joue ou les coins de la bouche. Des facteurs comme les cheveux, les parties du visage couvertes par les cheveux ou tout autre élément pouvant changer avec le temps ne sont pas pris en considération dans la mesure et l'analyse. Le balayage de la forme du visage pour l'identification des individus est davantage utilisé pour vérifier les passeports dans les aéroports, pour reconnaître les criminels ainsi que pour contrôler l'accès à certains services (banque, coffre-fort ou autres) ou à des

systèmes ou des réseaux informatiques (intranet, extranet, portail en ligne ou autres).

Le tableau ci-dessous présente les divers avantages et inconvénients que comportent les techniques biométriques qui reposent sur des caractéristiques physiques.

Tableau 1. Avantages et inconvénients des principales techniques biométriques physiologiques

Techniques	Avantages	Inconvénients
Reconnaissance des empreintes digitales	• La technique la plus éprouvée et la plus connue du grand public. • La petite taille du lecteur facilite son intégration dans la majorité des applications (ordinateurs, téléphones, etc.). • Faible coût des lecteurs grâce aux nouveaux capteurs. • Traitement rapide. • Bon compromis entre le taux de rejets et le taux de fausses acceptations.	• Difficulté de lecture : sensibilité aux altérations pouvant survenir au cours de la vie (égratignure, cicatrice, vieillissement ou autres) et à certaines variations (température, humidité, saleté, etc.). • Besoin de la coopération de l’utilisateur pour la pose correcte du doigt sur le lecteur.
Reconnaissance de la forme de la main ou des doigts	• Technique moins capricieuse que la reconnaissance des empreintes digitales : insensibilité à la poussière, aux coupures au doigt, etc. • D'utilisation très simple.	• Taux très élevé de fausses acceptations (les appareils ne peuvent distinguer les jumeaux ou les personnes de la même famille sur cette base). • La forme de la main ou des doigts se modifie avec le vieillissement, ce qui nuit à la mesure à long terme. • Lecteur trop encombrant pour l'utiliser dans une voiture ou sur un téléphone.
Analyse de la forme du visage	• Seule une opération chirurgicale modifiant la forme du visage (ajout de prothèses, transformation du cartilage, etc.) peut affecter la fiabilité. • Seule technique utilisable sans le consentement de la personne. • D’utilisation facile.	• Technique qui ne permet pas d'identifier des personnes en mouvement. • Impossibilité de différencier des jumeaux. • Peu d'efficacité. • Sensibilité à la variation de l’éclairage et au changement de la position du visage.
Balayage de l'iris	• Grande quantité de renseignements contenus dans l’iris. • Iris très difficilement falsifiable. • Dessin de l'iris indépendant du code génétique. • Iris différent entre jumeaux. • L'iris ne varie presque pas au cours d’une vie.	• Des problèmes peuvent survenir lors de la mesure (reflet, variation de la taille de la pupille, etc.). • Une photo ou une lentille de contact reproduisant l’image de l’iris peut affecter la fiaibilité. • Aspect invasif de la méthode.

Balayage de la rétine	• Technique la plus difficile à falsifier. • Technique très efficace. Taux faibles de faux rejets et de fausses acceptations. • Carte vasculaire propre à chaque individu et différente, même entre jumeaux • Haute sécurité. • La rétine est stable dans le temps. Elle est peu exposée aux blessures.	• Technique contraignante pour les participants (mesure à courte distance [quelques centimètres] du capteur). • Technique invasive et peu acceptée par le public. • L'aspect des vaisseaux sanguins peut être modifié par la maladie ou l'âge

Source : OCDE (2004), Securiteinfo.com (2004) et Six (2002).

Biométrie comportementale

Parmi les technologies biométriques de type comportemental, celles qui reposent sur la dynamique des frappes sur clavier, la dynamique de la signature et la reconnaissance vocale sont les plus connues. D'abord, la reconnaissance des personnes à leur *façon unique de frapper les touches du clavier* repose sur l'analyse du rythme des frappes, de la durée entre les frappes, de la fréquence des erreurs, de la durée de la frappe elle-même. Cette technique d'identification des individus s'avère surtout utile pour contrôler l'accès à un système d'information. La mesure de la *dynamique des signatures* s'effectue, quant à elle, à l'aide d'une palette graphique et d'un stylet. Cette technique tient compte, notamment, de la vitesse d'exécution de la signature, de la pression, de l'accélération, du temps total, de l'inclinaison du stylet et du nombre de fois que le stylet est enlevé de la palette. Parmi les applications possibles de cette technique, on compte l'authentification de l'identité des personnes qui signent des documents électroniques, des contrats ou des rapports. Enfin, la *reconnaissance vocale* a pour assise une combinaison de données physiologiques et comportementales de la voix. Elle sert surtout à protéger des immeubles d'habitation (contrôle de l'entrée par un portail), à exercer un contrôle frontalier et à sécuriser l'accès à des services banquiers.

Le tableau suivant propose une synthèse des avantages et des inconvénients possibles de chacune des mesures biométriques comportementales.

Tableau 2. Avantages et inconvénients des principales techniques biométriques comportementales

Techniques	Avantages	Inconvénients
Dynamique de frappe sur clavier	• Permet d'identifier une personne à distance, à partir de son ordinateur.	• L'état de santé et la fatigue peuvent altérer la façon de frapper les touches. • Sensibilité à la différence entre les claviers.
Dynamique des signatures	• Facile à utiliser. • Très acceptée par les usagers.	• Technique peu utilisée jusqu'à maintenant. • La signature étant changeante, une combinaison de données (vitesse d'exécution ou autres) est nécessaire.
Reconnaissance vocale	• Une des seules techniques permettant de reconnaître quelqu'un à distance et la seule utilisée pour la reconnaissance par téléphone.	• Il est très facile d'enregistrer ou de reproduire la voix. • Nécessite une excellente qualité audio. Sensible aux bruits ambiants. • La voix change dans le temps et peut être altérée (rhume, fatigue, forte émotion, etc.). • Faible niveau de différenciation entre deux voix. • Taux élevés de faux rejets et de fausses acceptations.

Source : OCDE (2004), Securiteinfo.com (2004) et Six (2002).

À ces diverses techniques, s'ajoutent les mesures biométriques s'appuyant sur la géométrie de l'oreille, les odeurs corporelles, les pores de la

peau, la thermographie et l'ADN. Chacune des techniques biométriques existantes peut répondre à un besoin particulier et convenir à un contexte d'utilisation précis. La biométrie « multimodalité » — soit la combinaison de diverses techniques biométriques — assure également un meilleur niveau de sécurité en réunissant les avantages de chacun et en éliminant certaines limites.

Rédactrice : Isabelle Vachon, analyste-conseil, Enquêtes et Veille stratégique, CEFRIO

Sources : Drothier, Yves. « La recherche envisage la biométrie multimodalité », *Journal du Net*, 2 novembre 2004.
Hope-Tindall, Peter; OCDE. Direction de la science, de la technologie et de l'industrie. Comité de la politique de l'information, de l'informatique et des communications. *Working Party on Information Security and Privacy : Biometric-Based Technologies*, 30 juin 2004, 66 p.
Securiteinfo.com. « La biométrie », « Les technologies biométriques », 2004.
Six, Nicolas. « Biométrie : six moyens d'identifier un utilisateur », *Journal du Net*, 26 août 2002.

Quelques applications gouvernementales de la biométrie dans le monde

Plusieurs pays, dont le Canada, ont mis en place des systèmes de reconnaissance biométrique afin de sécuriser et de faciliter certaines activités de leurs citoyens. Passons en revue quelques-unes des initiatives en matière de biométrie appliquées récemment ou en voie de l'être par des autorités gouvernementales.

Passeports biométriques

Certains pays vont de l'avant en instaurant l'usage de passeports biométriques. Le Danemark (reconnaissance faciale), les Pays-Bas (reconnaissance faciale et lecture des empreintes digitales), la Belgique (reconnaissance faciale, probablement combinée à la lecture d'empreintes digitales) et les États-Unis sont les précurseurs dans ce domaine. De son côté, l'Australie prévoit fournir à ses ressortissants un passeport biométrique d'ici dix ans.

Aéroports

Aux Pays-Bas, il est possible, pour les citoyens, d'obtenir une carte contenant des données biométriques de leurs deux iris en adhérant à un programme. Moyennant une certaine somme, les usagers des aéroports peuvent ainsi accélérer les processus d'embarquement et éviter les longues files d'attente.

À partir du 15 novembre 2004, le Canada offrira à ses citoyens une carte facilitant l'accès aux zones réglementées dans les 29 principaux aéroports du pays, dont l'aéroport Montréal-Trudeau. Les voyageurs qui auront une telle carte en leur possession devront subir un balayage de l'iris ou des empreintes digitales.

Santé

Six hôpitaux du Tennessee aux États-Unis utilisent un système de reconnaissance d'empreintes digitales limitant l'accès aux dossiers-patients aux seules personnes autorisées à les consulter.

Circulation à l'intérieur d'un édifice

Le ministère de l'Agriculture du Mexique a mis en place un système pour contrôler l'accès à certaines zones dans ses édifices. L'utilisation de données biométriques permet en plus de gérer les déplacements des 1 500 employés du ministère.

Immigration et demandes d'asile

Les pays de l'Union européenne se sont dotés d'une base de données commune d'empreintes digitales et d'un système qui permet d'échanger entre eux de l'information sur les demandeurs d'asile et les immigrants illégaux.

Carte d'identité nationale

Un projet pilote de carte d'identité nationale aux Pays-Bas a été lancé en septembre 2004. Cette carte d'identité biométrique contient de l'information sur les empreintes digitales et sur l'iris.

Grâce au progrès dans le domaine de la biométrie, nous pouvons croire qu'à moyen terme, des technologies permettront d'authentifier l'identité des citoyens à distance et de leur donner l'accès à des services gouvernementaux en ligne. Déjà, des souris munies d'un capteur d'empreintes digitales, la reconnaissance de la forme du visage à partir d'une image de webcaméra ou encore l'analyse de la dynamique de frappe sur clavier démontrent l'usage potentiel de la biométrie à cette fin.

Rédactrice : Caroline Jacob, analyste-conseil, Enquêtes et Veille stratégique, CEFRIO
Source : Anonyme. « Bioscrypt selected by Mexican government », *TMCnet.com*, 23 janvier 2004.
Anonyme. « West Tennessee healthcare benefits from integrated biometric security solution using Trusted Space ® software and Zvetco Biome-trics Verifi™ fingerprint readers », *TMCnet.com*, 17 juin 2004.

Commission européenne, *eGovernment News* :

- 9 juin 2004, « Dutch biometric passport trials taking shape ».
- 6 mai 2004, « EU biometric identification system for asylum seekers is a success, says report ».
- 18 mai 2004, « Belgium unveils biometric passport program ».
- 10 mars 2004, « US Government to start issuing biometric passports in October 2004 ».
- 18 février 2004, « Danish Government to start issuing biometric passports by the end of 2004 ».

Transports Canada. « Utilisation de la biométrie aux aéroports canadiens –lancement de deux projets d'amélioration à la sûreté », communiqué de presse, 15 octobre 2004.

Favorables ou non? Perception des Canadiens et des Américains quant à l'usage de la biométrie

Si la biométrie apparaît sécurisante parce qu'elle offre la possibilité de vérifier – pratiquement sans erreur – l'identité des personnes, elle peut aussi effrayer en raison de son caractère intrusif. Qu'en pensent les citoyens canadiens et américains ? Comment perçoivent-ils l'utilisation de la biométrie pour lutter contre le vol d'identité et pour améliorer la sécurité ? Deux études ont tenté de cerner les perceptions des Canadiens et des Américains à ce propos.

Au Canada

Selon une étude réalisée par Citoyenneté et Immigration Canada en septembre 2003, les Canadiens semblent très peu sensibilisés à la question de l'utilisation de la biométrie. En effet, selon les résultats de l'étude, plus de huit citoyens sur dix (83 %) ne savent pas, savent peu ou très peu, ce qu'est la biométrie. Cependant, après avoir pris connaissance de la définition de la biométrie, 54 % des Canadiens ont affirmé avoir déjà entendu ou lu quelque chose sur ce sujet.

Malgré leur faible niveau de connaissance en matière de biométrie, il appert que les Canadiens sont tout de même favorables à son utilisation. D'ailleurs, les résultats indiquent que plus du tiers des Canadiens (35 %) considèrent que la biométrie peut être très efficace pour lutter contre l'usage frauduleux de documents d'identité. Aussi, plus des deux tiers (68 %) se disent en faveur de l'utilisation de la biométrie par le gouvernement fédéral pour réduire ces fraudes. Précisons que les Québécois se montrent plus enclins que les autres Canadiens à appuyer cette idée (73 %). Les habitants des provinces de l'Atlantique sont, pour leur part, ceux qui appuient le moins cette idée (62 %).

Les résultats du sondage révèlent également que plus de la majorité des Canadiens croient que la biométrie permettra de :

- diminuer les fraudes d'identité par les immigrants illégaux (76 %) ;
- réduire l'abus des programmes gouvernementaux (74 %) ;

- rendre plus difficile l'entrée de terroristes au pays (67 %);
- rendre plus difficiles les activités terroristes au pays (66 %) ;
- faciliter l'entrée des citoyens canadiens aux États-Unis (63 %).

Le sondage montre aussi que de nombreux Canadiens ont des inquiétudes concernant certains aspects de l'utilisation de la biométrie, particulièrement à l'égard :

- du coût de mise en œuvre (49 %) ;
- de la réduction importante de la protection de la vie privée, étant donné le risque que le gouvernement puisse suivre les mouvements des citoyens (48 %) ;
- de la possibilité que les criminels puissent contourner la technologie (46 %) ;
- de la possibilité que le gouvernement fasse un mauvais usage ou un usage abusif de la biométrie (45 %) ;
- du fait que la biométrie va à l'encontre des valeurs canadiennes fondamentales de liberté et d'équité (37 %).

Enfin, une forte proportion de Canadiens pensent que, d'ici la fin de la présente décennie, le gouvernement mettra probablement en place un indicateur biométrique afin de vérifier l'identité des citoyens (80 %).

Aux États-Unis

Une étude réalisée chez nos voisins du sud en octobre 2004 relève que les deux tiers des répondants (69 %) semblent favorables à l'idée d'utiliser la biométrie. Environ un Américain sur dix (12 %) s'est prononcé contre son utilisation et un sur cinq (19 %) a dit être ambivalent sur la question. Les moyens les plus populaires auprès des répondants américains sont les empreintes digitales (85 %) et la reconnaissance de la voix (84 %). Les analyses des mains (57 %), de l'iris (46 %) et du visage (45 %) ont obtenu un appui plus faible. Enfin, en ce qui a trait aux avantages de la biométrie perçus par les personnes interrogées, notons l'élimination des mots de passe (88 %), l'accélération des transactions (69 %) et l'accroissement de la sécurité de l'information (56 %).

Rédactrice : Caroline Jacob, analyste-conseil, Enquêtes et Veille stratégique, CEFRIO
Sources : EDS. *Consumer Mistakes Continue To Aid Identity Theft According to Nationwide Survey : Survey Finds Consumers Open to the Use of Innovative Identification Methods Such as Biometrics*, communiqué de presse, 27 octobre 2004.
EDS. *Privacy and Identity Management Survey : Summary of Results and Findings*, octobre 2004, 13 p.
Ministère Citoyenneté et Immigration Canada (CIC). *Perceptions du public sur la biométrie*, septembre 2003.
Ministère Citoyenneté et Immigration Canada (CIC). « Les Canadiens sont toujours grandement favorables à l'utilisation de la biométrie pour combattre l'usurpation d'identité », communiqué de presse, octobre 2003.

Biométrie, sécurité et protection de la vie privée

Lorsqu'il est question d'authentification électronique, les technologies qui s'appuient sur la biométrie ont le vent dans les voiles, notamment parce qu'elles sont souvent pressenties comme infaillibles. Mais attention! Aussi sophistiqués qu'ils soient, ces systèmes d'identification demeurent vulnérables à divers types d'attaques informatiques. Or, ces effractions représentent autant de menaces à la sécurité et à la protection des renseignements personnels transmis par ces technologies.

Poursuivant l'objectif de présenter les avantages ainsi que les limites des technologies d'authentification qui s'appuient sur la biométrie, l'Organisation de coopération et de développement économiques (OCDE) a publié en juin 2004 un rapport intitulé *Working Party on Information Security and Privacy : Biometric-Based Technologies*. En plus de présenter les divers types de mesures relatives à la biométrie, le document démontre que des mécanismes et des procédures doivent être associés à ces mesures pour assurer la sécurité.

Selon l'OCDE, trois grands champs d'inquiétude sont liés à l'utilisation de la biométrie :

1. L'utilisation inappropriée des renseignements personnels qui sont échangés ou qui sont conservés dans les systèmes, ou leur utilisation à des fins autres que celles ayant présidé à leur collecte ;
2. Le risque que ces systèmes en viennent à constituer des infrastructures de surveillance et de contrôle social ;
3. Le fait que le consentement des usagers et la transparence des processus soient des éléments optionnels plutôt qu'obligatoires, lors

de l'implantation de mécanismes biométriques.

Pour répondre à ces préoccupations, le rapport propose différentes techniques ou méthodes susceptibles de renforcer la sécurité des systèmes de mesures biométriques :

1. La voie légale : les lois et la réglementation en vigueur doivent être comprises et utilisées comme des outils dans le design des systèmes ;
2. L'élaboration de politiques organisationnelles associées à la sécurité et à la protection des renseignements personnels : tout comme dans le cas des lois, ces politiques doivent être prises en considération lors de l'implantation de la biométrie ;
3. L'utilisation de protection logicielle : les dispositifs inviolables (*tamper-proof hardware*) peuvent par exemple être utilisés pour gérer les opérations du système et s'assurer qu'une personne mal intentionnée ne puisse facilement déjouer les mécanismes de sécurité.

En bref...

Si les technologies associées à la biométrie représentent assurément des solutions d'avenir, il faut, malgré tout, savoir reconnaître leurs limites et repérer leurs faiblesses. Enfin, quelles que soient les mesures retenues, des méthodes destinées à assurer la sécurité du processus d'authentification ainsi que la protection des renseignements personnels transmis doivent idéalement présider au développement des systèmes.

Rédactrice : Catherine Lamy, directrice adjointe, Enquêtes et Veille stratégique, CEFRIO
Sources : OCDE. Direction de la science, de la technologie et de l'industrie. Comité de la politique de l'information, de l'informatique et des communications. *Working Party on Information Security and Privacy : Biometric-Based Technologies*, 30 juin 2004, 66 p.

Pour en savoir plus

Commission nationale de l'informatique et des libertés (CNIL). *Biométrie : la position de la CNIL*, 18 octobre 2004.

Anil K. Jain et al. « Biometrics : A Grand Challenge », *International Conference on Pattern Recognition*, actes de colloque, Cambridge, Royaume-Uni, Août 2004.

Le **bulletin e-Veille** est produit sous la coordination du Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles du Secrétariat du Conseil du trésor, en collaboration avec le CEFRIO.

Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles du Secrétariat du Conseil du trésor
1500H, rue Jean-Talon Nord
Sainte-Foy (Québec) G1N 4T5
Téléphone : (418) 528-5505
Télécopieur : (418) 528-5506

Gestion et supervision
Pascal Doucet, conseiller en ingénierie documentaire et veille stratégique, Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles, Secrétariat du Conseil du trésor
Éric Lacroix, directeur des enquêtes et de la veille stratégique, CEFRIO

Réalisation et rédaction
Isabelle Vachon, analyste-conseil, Direction des enquêtes et de la veille stratégique, CEFRIO

Avec la collaboration de :
Catherine Lamy, directrice adjointe des enquêtes et de la veille stratégique, CEFRIO
Caroline Jacob, analyste-conseil, Direction des enquêtes et de la veille stratégique, CEFRIO

Recherche documentaire
Isabelle Poulin, documentaliste, Direction des enquêtes et et de la veille stratégique, CEFRIO

Révision linguistique
Diane Lambert-Tésolin, conseillère en rédaction, Direction des communications, Secrétariat du Conseil du trésor

Publications précédentes >>

- | Ministres |
- Ministère |
- Au service des citoyens |
- Au service des ministères et des réseaux |

- | Publications du Québec |
- Gouvernement en ligne |
- Documentation |
- Pour nous joindre |

Dernière modification de cette page : 2005-08-05

Québec