BIOMÉTRIE

FÉVRIER 2020

ITSAP.00.019

La biométrie désigne la mesure et l'usage de caractéristiques corporelles uniques (comme les empreintes digitales, une rétine, la structure faciale, les caractéristiques linguistiques et les réseaux veineux). En effet, grâce à vos empreintes digitales, vous pouvez par exemple vous authentifier pour déverrouiller votre dispositif mobile. Si vous recourez à l'authentification biométrique, nous vous recommandons toutefois d'utiliser également un mot de passe ou un numéro d'identification personnel (NIP) afin d'ajouter une protection supplémentaire (ce que l'on appelle l'authentification à facteurs multiples). Il faut toutefois savoir que la biométrie apporte son lot d'avantages et d'inconvénients de même que des vulnérabilités qui sont mis de l'avant dans le présent document.

Voici des exemples d'appareils de biométrie :

- Un lecteur d'empreintes digitales permet de mesurer des courants électriques ou d'émettre des ultrasons qui reproduisent les motifs de vos empreintes digitales;
- Un système de reconnaissance faciale photographie votre visage et compare la photo prise aux images qui vous correspondent;
- Un système de reconnaissance de l'iris photographie votre œil à l'aide d'une lumière infrarouge et compare la photo prise aux caractéristiques de votre iris;
- Un système de reconnaissance des réseaux veineux comportant un lecteur émet une lumière infrarouge afin de créer une image des veines apparaissant dans votre main;
- Un système d'identification du locuteur analyse une combinaison de sonorités de votre voix ainsi que d'autres caractéristiques individuelles (p. ex. votre accent, votre rythme, votre vocabulaire).

QUELLES SONT LES UTILITÉS ASSOCIÉES À LA BIOMÉTRIE?

La biométrie s'avère utile pour vous authentifier. En effet, plutôt que d'avoir à entrer un mot de passe ou une phrase de mots, vous pouvez aisément recourir à vos caractéristiques biométriques.

Les organismes peuvent se servir de la biométrie dans différentes circonstances, notamment les suivantes :

- gérer l'accès aux installations d'un édifice (p. ex. les salles de serveurs);
- déverrouiller les actifs et les dispositifs de TI;
- procéder à des paiements à partir de téléphones intelligents.

COMMENT PUIS-JE COMMENCER À UTILISER LA BIOMÉTRIE?

La première fois que vous utilisez la biométrie sur un dispositif, vous devez enregistrer votre caractéristique unique dans le cadre du processus d'inscription. À titre d'exemple, le lecteur d'empreintes procède au balayage de vos empreintes digitales plusieurs fois afin que le dispositif puisse analyser et conserver un code de hachage associé à votre caractéristique biométrique unique. Ce code représente en fait vos empreintes digitales chiffrées et est vraiment difficile à déchiffrer pour les acteurs malveillants. Un dispositif n'enregistre donc jamais l'image de vos empreintes digitales comme telles.

Avant d'utiliser un système biométrique (comme un dispositif mobile), nous vous recommandons d'effectuer des recherches pour vous assurer que les mécanismes de sécurité du système cadrent avec les exigences de votre organisme.

SÉRIE SENSIBILISATION

QUELLES SONT CERTAINES DES MENACES ASSOCIÉES À LA BIOMÉTRIE?

Malgré le caractère unique de vos caractéristiques biométriques, des auteurs de menace peuvent tout de même les reproduire, les copier ou les imiter afin de déjouer des systèmes. Ils peuvent par exemple faire ce qui suit :

- copier vos empreintes digitales (p. ex. des empreintes digitales synthétiques servant de clés maîtresses);
- utiliser une photo tirée de votre profil de médias sociaux pour déjouer un système de reconnaissance faciale;
- obtenir une image de votre iris pour tromper un système de reconnaissance de l'iris (p. ex. des verres de contact sur lesquels apparaît une image de votre iris);
- enregistrer ou métamorphoser votre voix pour tromper un système d'identification du locuteur (p. ex. extraire votre voix pour la superposer sur la voix d'un acteur malveillant).

Il est à noter que les menaces propres aux médiaux sociaux ne cessent d'augmenter. De fait, grâce à vos comptes de médias sociaux, les auteurs de menace peuvent accéder facilement aux photos et aux vidéos que vous partagez publiquement. N'oubliez donc pas que les éléments que vous publiez peuvent servir à imiter vos caractéristiques biométriques.

QUELS SONT CERTAINS DES PROBLÈMES ASSOCIÉS AUX SYSTÈMES BIOMÉTRIQUES?

Les systèmes biométriques peuvent être défaillants et refuser (faux négatif) ou autoriser l'accès (faux positif) à un système ou à un dispositif.

On entend par ***faux négatif*** les situations où un système biométrique ne reconnaît pas la personne réelle et bloque ses accès. Un cas de faux négatif peut représenter une menace pour votre organisme. En effet, si une infrastructure de serveurs est par exemple hors service et si le personnel autorisé ne peut pas y accéder, votre organisme perd tous ses accès jusqu'à ce que le problème de faux négatif se règle ou qu'une personne réussisse finalement à accéder à l'infrastructure.

En revanche, on entend par ***faux positif*** les situations où un système biométrique fait correspondre par erreur les justificatifs d'identité de deux personnes différentes. Ainsi, si une personne ne détenant pas d'autorisation se trouve dans une situation de faux positif, votre organisme et la personne détenant les justificatifs d'identité utilisés sont à risque. Par exemple, si votre téléphone intelligent octroie un accès à une personne autre que vous à la suite d'une mauvaise reconnaissance faciale, vos renseignements personnels risquent d'être compromis.

Comme les cas de faux négatifs et de faux positifs sont possibles, nous recommandons l'utilisation d'un mot de passe ou d'un NIP associée à l'utilisation d'un facteur biométrique (en d'autres mots, le recours à l'authentification à facteurs multiples) afin d'ajouter une protection supplémentaire.

QUEL EST LE DEGRÉ DE SÉCURITÉ DES NOUVELLES STRUCTURES?

Dans la foulée des récents progrès technologiques, on observe l'amélioration des mesures de sécurité protégeant les caractéristiques biométriques contre les cyberattaques courantes grâce, entre autres, aux nouvelles fonctions et technologies suivantes :

- Les systèmes de reconnaissance faciale s'appuient désormais sur des méthodes utilisant des points de lumière infrarouge qui créent un schéma 3D du visage d'un utilisateur (ce qui rend donc peu probable le fait qu'une photo prise sur un compte de médias sociaux donne accès à un dispositif);
- Le balayage des veines de la paume représente une méthode d'authentification biométrique assurant une protection considérable. En effet, les veines ne sont pas aussi facilement visibles que votre visage ou vos empreintes digitales, ce qui complique le vol de votre motif veineux par un acteur malveillant.

QUELS ENJEUX RELATIFS À LA VIE PRIVÉE ASSOCIE-T-ON À LA BIOMÉTRIE?

Bien que la biométrie puisse constituer une méthode d'authentification utile, il s'agit également d'une forme de renseignement personnel. Par conséquent, si votre organisme souhaite recourir à la biométrie dans le cadre d'une authentification à facteurs multiples, il doit s'assurer que ce type de données est recueilli, traité et utilisé conformément à des exigences juridiques et réglementaires (notamment la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*). Les employés doivent par exemple donner leur consentement à l'organisme avant que celui-ci recueille et utilise leurs caractéristiques biométriques.

QUELLES MESURES DE PROTECTION POUVEZ -VOUS PRENDRE?

Nous vous recommandons en fait de jumeler l'authentification biométrique à un autre mécanisme d'authentification (p. ex. des phrases de passe), car l'authentification à facteurs multiples permet de renforcer le niveau de sécurité. Ainsi, en cas de compromission de l'un des mécanismes d'authentification, l'autre mécanisme utilisé continuera de protéger l'accès à vos dispositifs ou à vos comptes.

Contrairement à d'autres mécanismes d'authentification (comme les mots de passe ou les cartes à puce), il est impossible de deviner ou de voler une caractéristique biométrique. Or, si une caractéristique biométrique particulière (comme les empreintes digitales de l'index de votre main droite) est imitée ou copiée, il sera impossible d'en obtenir de nouvelles, contrairement à un mot de passe ou à un NIP. Il faudra donc remplacer cette caractéristique biométrique par une autre (comme les empreintes digitales d'un autre doigt) pour empêcher des acteurs malveillants d'accéder à des systèmes et à des dispositifs.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.