Biométrie et sécurité des installations sensibles

Franck Rousset

La sécurité des installations sensibles - civiles et militaires - impose la mise en place d'un ensemble cohérent de dispositions juridiques, organisationnelles, humaines, techniques et matérielles. Ces installations présentent de fortes disparités en termes de nature et d'importance pour la réalisation et la poursuite des activités. Elles doivent donc faire l'objet de mesures de protection adaptées à leur environnement, leur personnel, aux activités et aux moyens matériels et immatériels contre les différentes formes de menaces. La complémentarité des fonctions et des dispositifs de protection doit tenir compte du principe de la défense en profondeur et d'une équation de protection.

Franck Rousset est ingénieur chargé d'études au département Moyens de protection de la Direction de la protection des installations, moyens et activités de la Défense (DPID) du ministère des Armées. À ce titre, il contribue à l'élaboration des politiques ministérielles et des standards des dispositifs de protection des emprises et des systèmes d'information concourant à la défense-sécurité et s'assure de leur mise en application. Auparavant, en tant que *project manager* **au sein de l'agence de communication et de l'information de l'OTAN, il a dirigé le déploiement de la pleine capacité de réaction aux incidents cyber de cette l'organisation internationale.**

Franck Rousset nous présente dans cet article comment la biométrie et ses différentes techniques peuvent contribuer au renforcement des fonctions et dispositifs de protection des installations sensibles, sous réserve d'être attentif aux modalités de mise en œuvre juridique et technique.

La biométrie

La biométrie regroupe l'ensemble des techniques informatiques permettant d'identifier un individu à partir de caractéristiques morphologiques, biologiques, physiologiques ou comportementales qui lui sont propres, comme la forme de la main ou du visage, le dessin de l'iris ou du doigt, les mouvements de l'écriture manuscrite, la signature vocale, etc.

La biométrie est souvent présentée comme une alternative aux identifications plus traditionnelles. Cependant, elle est le plus souvent employée en association avec les différents critères du contrôle d'accès que l'on classe de la façon suivants :

- ce que l'on sait (un code),
- ce que l'on a (un badge, une clé),
- ce que l'on est (la biométrie - cela inclut également ce que l'on sait faire).

Les applications de la biométrie sont nombreuses ; elles vont au-delà du seul domaine de la sécurité des installations sensibles dont le contrôle d'accès et de la détection intrusion et touchent différents domaines : police, travail, domestique, etc.

Champ d'application de la biométrie : identification et authentification

L'identification permet d'associer une identité à une personne (qui elle est !). L'authentification permet d'apporter la preuve de l'identité d'une personne (est-elle vraiment celle qu'elle dit être ?).

L'authentification implique l'identification. L'authentification renforcée nécessite plusieurs méthodes d'identification de nature différente. L'identification complémentaire (notion nouvelle utilisée dans ce document) renforce la confiance dans l'identification d'une personne, sans apporter la preuve de son identité (ce n'est pas une authentification).

Quelques définitions

• **Élément biométrique :** toute caractéristique morphologique, biologique, physiologique ou comportementale qui permet de s'assurer de l'identité d'un individu.

• **Échantillon biométrique :** donnée représentant une caractéristique biométrique capturée par un système biométrique.

• **Gabarit (en anglais « template ») :** représentation numérique après traitement de l'élément biométrique. Le gabarit biométrique désigne les mesures qui sont mémorisées lors de l'enregistrement des caractéristiques morphologiques (empreinte digitale, forme de la main, iris...), biologiques (ADN, urine, sang...) ou comportementales (démarche, dynamique de tracé de signature...) de la personne concernée. On dit que les personnes maîtrisent leur gabarit lorsqu'on leur confie le support de stockage de ces mesures ou lorsque ce support est conservé dans les serveurs du responsable du système sous une forme le rendant inexploitable en l'absence d'intervention de la personne concernée. Au contraire, on dit que les personnes ne maîtrisent pas leur gabarit lorsque le support de stockage de ces mesures est conservé dans les serveurs du responsable du système sous une forme exploitable même en l'absence d'intervention de la personne concernée. La taille et le format du gabarit dépendent des éléments biométriques capturés et du traitement effectué par le lecteur biométrique (algorithme de transformation et de compression) afin de permettre au système biométrique d'effectuer correctement les comparaisons.

• **Comparaison :** processus d'évaluation de la correspondance d'un échantillon biométrique avec un ou plusieurs modèles de référence précédemment stockés.

• **Correspondance :** processus de comparaison positive d'un échantillon biométrique avec une référence stockée et d'évaluation du degré de similitude.

• **1 à 1 (dite vérification/correspondance) :** la formule 1 à 1 est utilisée lorsqu'une comparaison est réalisée entre le gabarit de l'utilisateur et le gabarit sauvegardé (correspondant à l'utilisateur). L'échantillon biométrique sauvegardé peut être stocké soit dans un support (badge) ou dans une base de données (confinée dans le lecteur ou délocalisée sur un serveur distant). Lorsqu'il est stocké dans une base de données, l'utilisateur fournira un code pour permettre au système de récupérer le gabarit.

•**1 à N (dite recherche) :** la formule 1 à N est utilisée lorsqu'une comparaison est réalisée entre le gabarit de l'utilisateur et un nombre plus ou moins grand de gabarits sauvegardés dans la base de données. Lors de la comparaison, on vient rechercher le gabarit sauvegardé qui correspond le plus au gabarit de l'utilisateur capturé par le lecteur biométrique (dans les limites de tolérances intrinsèques ou paramétrées de ce lecteur biométrique).

Système biométrique

Un système biométrique met généralement en œuvre les principales étapes suivantes :

Étape d'enrôlement / enregistrement :

1/ capture de l'échantillon biométrique,

2/ extraction des points caractéristiques,

3/ traitement (calcul du gabarit par la sélection, combinaison et/ou agrégation des points caractéristiques pertinents, puis compression, signature et/ou chiffrement du résultat),

4/ enregistrement du gabarit sur un support ou en base de données (confinée dans le lecteur biométrique ou sur un serveur délocalisé).

Étape de recherche (1 à N) ou de vérification/correspondance (1 à 1) :

1/ capture de l'échantillon biométrique,

2/ extraction des points caractéristiques,

3/ traitement,

4/ comparaison avec le gabarit (stocké sur un support ou en base de données).

Étape de comparaison :

Cette étape consiste à vérifier l'identité de la personne. Pour cela, le lecteur réalise une comparaison entre deux ensembles de points caractéristiques. Le premier est extrait de l'élément biométrique capturé par le lecteur, le second est issu de celui stocké sur un support ou en base de données.

Figure 1 - Système biométrique : étape d'enrôlement / enregistrement

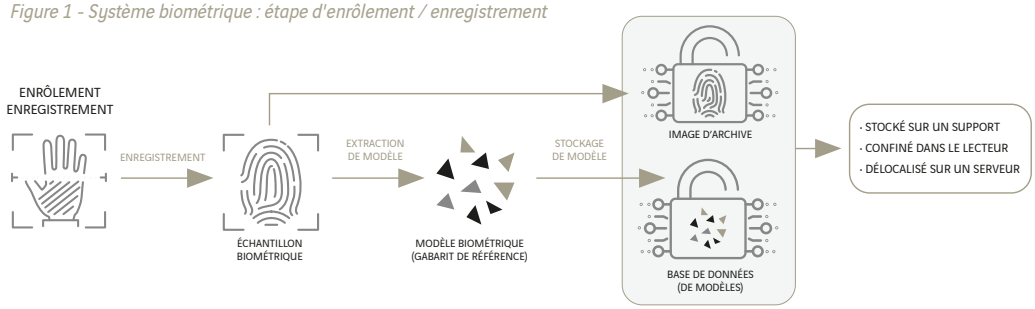
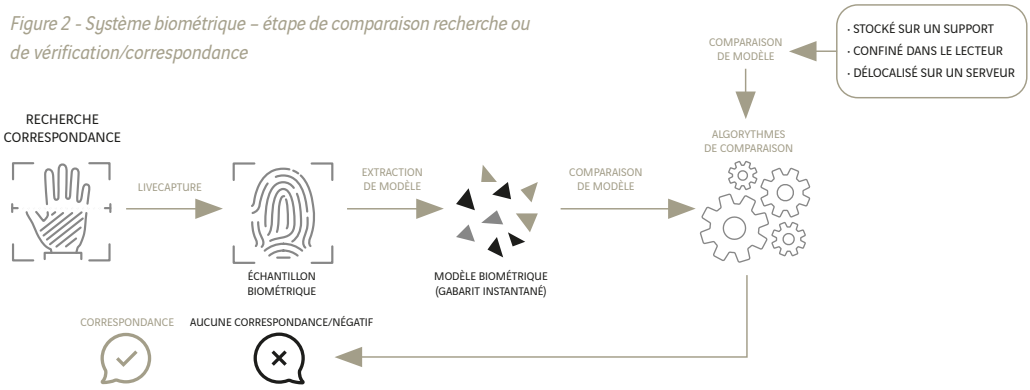


Figure 2 - Système biométrique – étape de comparaison recherche ou de vérification/correspondance



La méthode de comparaison utilisée doit tenir compte des translations, rotations et déformations présentes lors de l'étape d'enrôlement et surtout lors de celle de vérification. La comparaison ne peut donc pas donner une ressemblance à 100%. Cette tolérance d'erreur (due aux algorithmes utilisés ET au positionnement de l'élément biométrique capturé à l'enrôlement et à la vérification) offre des possibilités de fraude de substitution. La fiabilité du système biométrique dépend donc de la qualité cette étape de comparaison.

Risques de fraudes et fausse acceptation

Bien que vecteur d'amélioration de la sécurité, l'usage de la biométrie comporte des risques pouvant porter atteinte au fonctionnement des systèmes, et donc de manière intrinsèque, à la protection d'une installation.

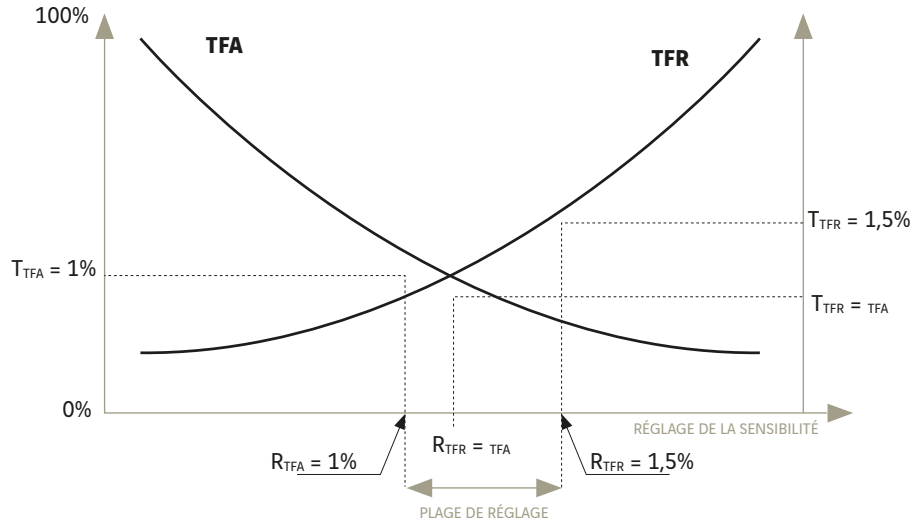
Il existe deux types de fraudes sur les solutions biométriques qu'il convient de prendre en compte dans l'analyse de risques des systèmes (ou des dispositifs de protection) sur lesquels ces solutions sont mises en œuvre :

- La fraude par substitution, qui consiste à tromper le lecteur à l'aide d'un clone d'élément biométrique ;
- La fraude cyber, qui consiste à piéger ou attaquer un des constituants du système biométrique : algorithme de transformation, base de données, mécanismes cryptographiques, interface de communication, réseau, etc.

Bien que n'étant pas une fraude volontaire, le taux de fausse acceptation (à tort d'une personne non autorisée) est un facteur également important à prendre en compte dans l'analyse de risques liée à la biométrie.

Taux de fausse acceptation versus taux de faux rejet

Le taux de fausse acceptation (TFA) traduit l'incertitude liée à l'utilisation d'un lecteur biométrique acceptant à tort une personne non autorisée. Il est exprimé en pourcentage d'acceptation à tort. On parle aussi de *False Acceptation Rate* (FAR) ou encore de Taux d'acceptation à tort (TAT). Le taux de faux rejet (TFR) traduit l'incerti-



tude liée à l'utilisation d'un lecteur biométrique refusant à tort une personne autorisée. On parle aussi de False Reject Rate (FRR) ou de taux de rejet à tort (TRT). Le réglage choisi doit permettre un TFA inférieur à 1% et un TFR inférieur à 1,5%. La solution idéale recherchée consiste à obtenir un TFR égal au TFA, le plus faible possible. L'analyse de risques doit explicitement évaluer l'impact du TFA retenu sur la sécurité offerte par système biométrique, et proposer des mesures compensatoires.

Quelques exemples de solutions biométriques

> Empreinte digitale

L'empreinte digitale est l'une des techniques les plus connues du grand public. Elle a été développée pour permettre aux policiers d'identifier les criminels récidivistes. Les arrêts de lignes, bifurcations, lacs, ilots et points représentent les points caractéristiques du dessin digital. Ces points sont aussi appelés minuties. La combinaison de ces minuties est pratiquement infinie, ce qui permet de considérer qu'une empreinte digitale est unique.

> Visage

La reconnaissance du visage est la technologie biométrique la plus naturelle. En effet, c'est celle qu'utilise tout individu pour reconnaître un autre individu.

La reconnaissance du visage en 2D consiste, à partir d'une photographie du visage de l'individu se présentant devant une caméra, à en mesurer les caractéristiques faciales qui se modifient peu avec le temps : forme du visage, emplacement des lèvres, du nez, écartement des yeux, etc.

La reconnaissance du visage en 3D consiste, à partir d'une ou plusieurs caméras et d'un projecteur infrarouge, à restituer un modèle 3D du visage et à en mesurer les caractéristiques faciales mentionnées supra.

> Iris

L'iris est la partie colorée de l'œil. Cette couleur est déterminée par la présence d'un pigment, la mélanine, le même composé chimique qui donne aussi leurs couleurs aux cheveux et à la peau. L'iris est constitué d'un réseau très dense de tubes très fins, dont le diamètre est inférieur à celui d'un cheveu. L'enchevêtrement des tubes de l'iris est propre à chaque œil et le rend unique.

> Volumétrie de la main

La géométrie de la main était une méthode fréquemment utilisée aux États-Unis. Le système prend une photo en 3D de la main posée sur une plaque avec ergots (afin d'aider l'utilisateur à positionner correctement sa main). De cette photo, il sélectionne les points caractéristiques de la main (longueur des doigts, forme des articulations). Comme la forme de la main se modifie avec le temps, il est nécessaire d'actualiser régulièrement les données enrôlées.

> Réseau veineux

L'analyse du réseau veineux du doigt ou de la main est plus récente. Le lecteur biométrique utilise certaines propriétés du sang pour pouvoir visualiser à l'aide d'une caméra le réseau veineux. Lorsqu'il est soumis à une forte lumière extérieure couplée à une source infrarouge, le sang apparait en sombre sur l'image visualisée, que ce soit dans les veines ou dans les artères. Cette technologie est sans contact et ne laisse pas de trace.

Utilisation de la biométrie pour la sécurité des installations sensibles

Juridiquement et techniquement, la biométrie peut être utilisée dans plusieurs contextes radicalement distincts et non comparables entre eux.

Pour la sécurité des installations sensibles, on identifie deux scénarios principaux. Vu les contraintes juridiques, techniques et financières, le besoin de protection de l'installation sensible doit être avéré et la plus-value de cet usage de la biométrie doit être démontrée avant sa mise en œuvre.

Scénario 1 - Authentification renforcée (enjeu sécuritaire : contrôle d'accès)

Lorsque les besoins de protection sont très élevés, mais que la fréquentation est faible ou moyenne, alors il est possible de coupler le système de contrôle d'accès avec de la biométrie pour disposer d'un facteur d'identification supplémentaire du porteur, et ainsi contribuer à son authentification renforcée. C'est le cas d'usage correspondant à la lecture d'un identifiant chiffré dans un badge d'accès, complété soit par la saisie d'un code mémorisé par le porteur ou soit par une comparaison biométrique du porteur. La marge d'erreur doit être la plus infime possible, car les enjeux sont stratégiques et financièrement souvent difficilement chiffrables.

Scénario 2 - Identification complémentaire pour le contrôle visuel comparatif (enjeu sécuritaire : détection intrusion)

Indépendamment des flux de passage (fréquentation), à chaque contrôle d'accès, il est nécessaire de garantir l'identité des « accédants » afin de prévenir tout risque d'usurpation d'identité (vol ou usage non autorisé du badge d'accès), en effectuant de manière graduée, un contrôle visuel comparatif du porteur et du badge présenté pour le contrôle d'accès, en particulier par un examen comparatif de la photo (présente sur le badge ou connue par des systèmes d'information). Cet examen peut être facilité et rendu plus performant en utilisant certaines techniques biométriques (en particulier la reconnaissance faciale). Ces techniques n'offrent pas de garanties d'identification pour le contrôle d'accès, mais contribuent à la détection d'éventuels intrus.

Scénario exclu - Identification de confort (enjeu : économique ou personnel)

Lorsque les besoins de protection sont moindres, voire faibles, mais que la fréquentation est très élevée, alors il est possible de s'appuyer sur la biométrie (dite de confort) pour identifier simplement des personnes et ainsi leur faciliter l'utilisation de services n'ayant pas forcément un enjeu de sécurité particulier, mais présentant plutôt un intérêt économique ou personnel : accès à des services facturés tels que la restauration, le suivi du consommateur lors de son parcours d'achat, le déverrouillage d'un équipement électronique personnel, etc. Une marge d'erreur peut être admise sous réserve d'être financièrement acceptable par l'institution proposant ce service.
L'utilisation de la biométrie dans ce scénario « identification de confort » est exclue pour des systèmes (ou des dispositifs de protection) contribuant à la sécurité des installations sensibles.

Scénario spécifique - Identification d'une personne par ses empreintes génétiques (enjeu : juridique)

Ce scénario correspond aux exigences de l'alinéa 4 de l'article 16-11 du Code civil (modifié par la loi n°2016-731 du 3 juin 2016 - art. 116) précise que l'identification d'une personne par ses empreintes génétiques ne peut être recherchée que [...] dans les conditions prévues à l'article L. 2381-1 du Code de la défense (modifié par la loi n°2017-258 du 28 février 2017 - art. 7). Ce contexte d'utilisation n'entre pas le périmètre de cet article.

Conditions de mise en œuvre

Sur le plan juridique

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés publiques telle que modifiée par la loi relative à la protection des données personnelles de juin 2018 s'applique aux traitements de données à caractère personnel qu'ils soient ou non automatisés. Les données sensibles (dont biométriques) constituent une catégorie particulière de données à caractère personnel, obéissant à un régime de protection particulier. Par principe, les données sensibles ne doivent pas figurer dans un traitement. Leur utilisation doit rester exceptionnelle. Elle doit être limitée et strictement nécessaire à la finalité du traitement. Entrant dans le cadre d'une dérogation, ce traitement peut justifier la réalisation d'une analyse d'impact, et reste soumis – pour les systèmes d'information mis en œuvre par l'État – à un régime d'autorisation préalable. Le secteur privé obéit à un autre régime. Ainsi, l'utilisation de données biométriques nécessaires à l'authentification ou au contrôle de l'identité de personnes accédant à une installation sensible de l'administration devra être autorisée par décret en Conseil d'État pris après avis motivé et publié de la CNIL dès lors qu'un tel traitement intéresse la Défense nationale (article 26 de la loi informatique et libertés).

Sur le plan technique

Il convient de distinguer :

- les dispositifs biométriques permettant aux personnes de garder la maîtrise de leur gabarit biométrique : cela suppose de stocker le gabarit biométrique sur un support détenu par la seule personne concernée ou en base de données sous une forme inexploitable, car illisible sans un secret détenu par la seule personne concernée ;
- les dispositifs biométriques ne garantissant pas cette maîtrise : cela sous-entend que le gabarit biométrique est stocké en base de données (serveurs distants ou terminal de lecture comparaison).

Dans les deux cas, l'installation et l'exploitation de ces dispositifs sont soumises à des conditions strictes. Des mesures de sécurité portant sur les données, les matériels, les logiciels et les éventuels canaux informatiques doivent être adoptées par le responsable de traitement pour préserver la sécurité et la confidentialité des données traitées :

- **les risques pour la vie privée doivent être minimisés.** En conséquence, les données traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles ont été collectées.
- **Le recours à un traitement biométrique doit être justifié.** Par exemple, le contrôle d'accès biométrique ne doit pas devenir courant et se substituer à d'autres dispositifs standards moins intrusifs pour les personnes (badge, clé, gardiennage, etc.), sans véritable justification.
- **Les systèmes biométriques garantissant la maîtrise des personnes sur leur gabarit doivent être privilégiés.** À défaut, la conservation des gabarits en base doit être justifiée et assortie de garanties fortes. Une étude d'impact est nécessaire pour vérifier et documenter le respect des mesures de protection sur les données.

Dans la pratique : faire le compromis juridique et technique

Dans le contexte de la sécurité des installations sensibles (contrôle d'accès et détection intrusion), les fonctions et dispositifs de protection requièrent une authentification (voire renforcée) de l'individu, à défaut une identification complé-

mentaire. La biométrie permet d'identifier un individu à partir d'éléments biométriques qui lui sont propres. Les systèmes biométriques comparent des données biométriques enrôlées à celles présentées au moment de la vérification. Les techniques sont nombreuses, hétérogènes et n'offrent que des réponses parcellaires aux besoins globaux. Cependant, ces techniques biométriques peuvent être combinées afin d'améliorer la confiance et la performance des dispositifs.

En parallèle, l'usage de la biométrie comporte des risques (fraude par substitution ou fraude cyber) pouvant porter atteinte aux personnes ainsi qu'au fonctionnement des systèmes et donc aux installations, sans oublier les problèmes de performances liés à l'équilibre entre le taux de fausse acceptation et le taux de faux rejet.

Le cadre juridique (RGPD et CNIL) sur le traitement des données à caractère personnel impose des mesures de protection, avec un objectif de résultats, pour en préserver la sécurité et la confidentialité.

Conclusion

Étant donné les contraintes existantes dans les domaines juridiques, techniques et financiers, l'usage de la biométrie pour la sécurité des installations sensibles doit être justifié et n'intervenir qu'en complément, l'ensemble conférant alors au système (ou dispositif de protection) une fonction de sécurité renforcée.

Sachant que, malgré une explosion de l'offre de solutions biométriques, celles-ci restent encore de qualité hétérogène et souffrent de l'absence de normes et de certifications communément reconnues, il incombe donc aux responsables de la sécurité de mener en premier un travail d'évaluation complet avant de faire appel à de telles techniques. ■

Franck Rousset,
Ingénieur chargé d'études au département Moyens de protection de la Direction de la protection des installations, moyens et activités de la Défense (DPID) du ministère des Armées.

Bibliographie

[RGPD] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données)

[CNIL] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[IM 1544] Instruction ministérielle 1544/DEF/CAB/DR du 17 janvier 2017, relative à la défense-sécurité des activités, moyens et installations relevant du ministre de la Défense

[MinARM RGPD] Instruction ARM/SGA/DAJ/D2P relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère de la Défense du 19 juillet 2018