Université Paris 7 – Denis Diderot

UFR d'Informatique

Cours de **M. ROUX**

Réalisé par :

- **Ibrahim BELAID**

Introduction

Alors que l'emploi de la biométrie se développe dans les procédures de contrôle et d'identification des personnes tant dans les pays européens qu'au plan international, en France, le ministère de l'Intérieur envisage de remplacer la carte d'identité actuelle par une carte à puce intégrant empreintes digitales et photo : ces données pourraient aussi être enregistrées dans un fichier central. La CNIL sera consultée pour avis sur ce projet qui soulève des questions majeures au regard des principes de protection des données personnelles. C'est pourquoi elle a entrepris un certain nombre d'actions, et afin d'en rendre compte et de nourrir le débat de fond, a décidé d'ouvrir sur son site le dossier "biométrie et titres d'identité".

Définition

Le programme INES (identité nationale électronique sécurisée) reprend quant à lui la volonté d'instaurer une carte d'identité nationale électronique en remplaçant les titres d'identités classiques. La nouvelle carte aura le format d'une carte bancaire. Les informations écrites sur la carte seront, comme actuellement, le nom, le prénom, la date et le lieu de naissance, le sexe, l'adresse, la signature manuscrite, la préfecture qui a délivré la carte, et le numéro de la carte. Les informations contenues dans la puce seront divisées en blocs distincts et étanches (par le moyen de la cryptographie). Elle permettra à l'usager de s'identifier auprès de son administration afin de pouvoir bénéficier d'un traitement sécurisé et personnalisé. La carte nationale d'identité électronique pose plusieurs défis aux professionnels ; son utilisation et son fonctionnement nécessitent une infrastructure technique, un accès facile à la population, un portail de service élargi, des fonctionnaires formés, une grille de procédure ainsi qu'un contrôle efficace. On peut alors se demander si là encore le système français permettra d'être inter-opérable avec les autres pays et garantir ainsi une égalité de traitement entre tous les possesseurs de la nouvelle carte.

La carte vise à moderniser un système devenu obsolète. La carte permettra en effet :

- De sécuriser la diffusion des cartes d'identité et des passeports.
- Fusionner, simplifier et sécuriser les procédures de demande de passeport et de carte nationale d'identité (CNI).
- Améliorer la gestion de ces titres dans de nouvelles applications. D'améliorer la lutte contre le terrorisme en introduisant une photographie et des empreintes dans la puce de la carte.
- Délivrer des titres hautement sécurisés conformes aux exigences internationales.
- De simplifier les démarches administratives. De réduire le nombre de documents administratifs.
- Offrir aux citoyens les moyens de prouver leur identité sur Internet et de signer électroniquement, afin de favoriser le développement de l'administration électronique.

Pour cela, la Biométrie entre en jeu ; la biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu. D'autre part, comme nous allons le voir, les caractéristiques physiques sont loin d'etre si parfaites et si précises, et l'on atteint très vite des limites pour ces techniques.

Usage

Les techniques basées sur la biométrie jouissent à l'heure actuelle d'un engouement général favorisé par un phénomène de mode, principalement véhiculé par les films au cinéma et à la télévision. Ainsi, il n'est pas rare de voir des scanners rétiniens avec de superbes lasers rouges, des lecteurs d'empreintes digitales avec de très jolis voyants -clignotants-, etc... tout cela représentant le summum de la technologie du contrôle d'accès. Or, les techniques de biométrie sont belle et bien en train de se répandre dans notre vie quotidienne, et ce tout en gardant une image quelque peu trompeuse. Car le problème est bien de savoir quelles techniques existent réellement, et quelles sont leurs limites. Cet article ne se veut pas exhaustif sur un sujet aussi vaste que la biométrie, mais il a tout de même pour vocation de sensibiliser au maximum les lecteurs et de leur donner quelques bases indispensables.

Caractéristiques Physiques

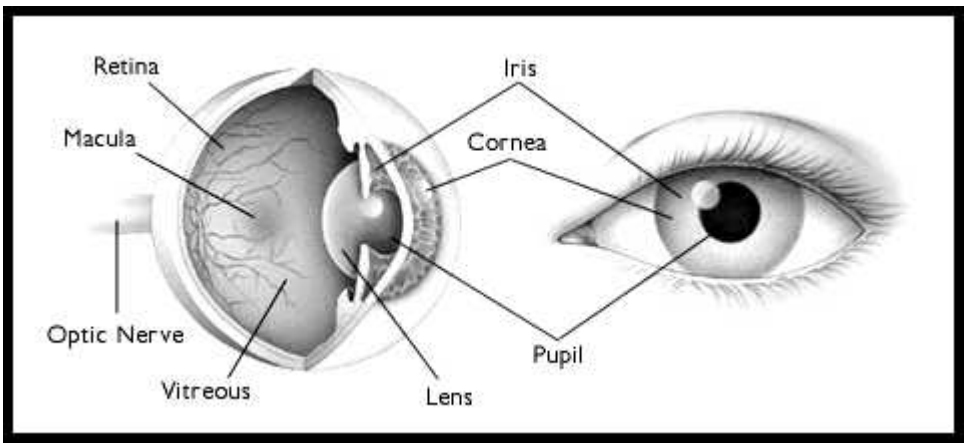
Il existe plusieurs caractéristiques physiques qui se révèlent être uniques pour un individu, et il existe également pour chacune d'entre elles plusieurs façons de les mesurer :

- **empreintes digitales (finger-scan):** la donnée de base dans le cas des empreintes digitales est le dessin représenté par les crêtes et sillons de l'épiderme. Ce dessin est unique et différent pour chaque individu. En pratique, il est quasiment impossible d'utiliser toutes les informations fournies par ce dessin (car trop nombreuses pour chaque individu), on préférera donc en extraire les caractéristiques principales telles que les bifurcations de crêtes, les "îles", les lignes qui disparaissent, etc... Une empreinte complète contient en moyenne une centaine de ces points caractéristiques (les "minuties"). Si l'on considère la zone réellement scannée, on peut extraire environ 40 de ces points. Pourtant, là encore, les produits proposés sur le marché ne se basent que sur une quinzaine de ces points (12 au minimum vis-à-vis de la loi), voire moins pour beaucoup d'entre eux (jusqu'à 8 minimum). Pour l'histoire, le nombre 12 provient de la règle des 12 points selon laquelle il est statistiquement impossible de trouver 2 individus présentants les mêmes 12 points caractéristiques, même en considérant une population de plusieurs dizaines de millions de personnes.

Les techniques utilisées pour la mesure sont diverses : capteurs optiques (caméras CCD/CMOS), capteurs ultrasoniques, capteurs de champ électrique, de capacité, de température...
Ces capteurs sont souvent doublés d'une mesure visant à établir la validité de l'échantillon soumis (autrement dit, qu'il s'agit bien d'un doigt) : mesure de la constante diélectrique relative du l'échantillon, sa conductivité, les battements de coeur, la pression sanguine, voire une mesure de l'empreinte sous l'épiderme...

- **géométrie de la main / du doigt (hand-scan):** ce type de mesure biométrique est l'un des plus répandus, notament aux Etats Unis. Cela consiste à mesurer plusieurs caractéristiques de la main (jusqu'à 90) tel que la forme de la main, longueur et largeur des doigts, formes des articulations, longueurs inter-articulations, etc... La technologie associée à cela est principalement de l'imagerie infrarouge; d'une façon générale, le système présente des FAR (False Acceptation Rate, voir plus bas) assez élevés, surtout entre personnes de la même famille ou bien encore des jumeaux.

- **iris (iris-scan):** pour les 2 techniques suivantes, il faut tout d'abord faire la distinction entre l'iris et la rétine :



Source : American Academy of Ophthalmology

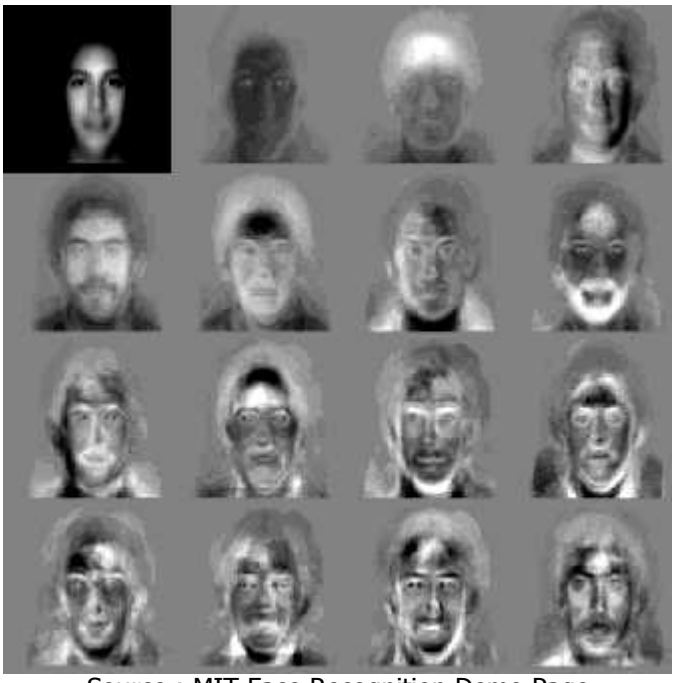
Autrement dit, l'étude de l'iris va se porter sur la partie de l'oeil visible ci-dessous :

En ce qui concerne l'iris, l'individu se place en face du capteur (caméra CCD/CMOS) qui scanne son iris. Celui-ci représente quelquechose de très intéressant pour la biométrie car il est à la fois toujours différent (même entre jumeaux, entre l'oeil gauche et le droit, etc...), indépendant du code génétique de l'individu, et très difficilement falsifiable. En effet, l'iris présente une quasi-infinité de points caractéristiques (que certains comparent en nombre à ceux de l'ADN), qui ne varient pratiquement pas pendant la vie d'une personne contrairement à la couleur de l'iris qui, elle, peut changer. Mais cela n'a aucune influence car les images d'iris obtenues par les capteurs sont en noir et blanc. Le seul problème de cette technique est liée à la mesure en elle-même, qui peut être source d'erreurs ou de problèmes. Ainsi, on peut quasiment dire que le nombre de problèmes rencontrés lors de cette mesure augmente proportionnellement avec la distance entre l'oeil etla caméra.
D'autres problèmes se posent à cause des reflets (nécessité d'avoir un éclairage restreint et maitrisé), et lors de la détection de faux yeux (photos) et autres fraudes. Pour ces dernières, on peut faire appel à certaines caractéristiques dynamiques de l'oeil qui prouveront son authenticité : réactivité de la pupille (dilatation/rétraction) par rapport à la quantité de lumière, étude de l'iris dans l'infrarouge et l'ultraviolet, etc...

- **rétine (retina-scan):** cette mesure biométrique est plus ancienne que celle utilisant l'iris, mais elle a été moins bien acceptée par le public et les utilisateurs, sans doute à cause de son

caractère trop contraignant : la mesure doit s'effectuer à très faible distance du capteur (quelques centimètres), qui effectue ensuite un balayage de la rétine. Il est physiquement impossible d'effectuer une mesure rétinienne à une distance de 30cm ou plus sur un sujet mobile comme on peut le voir dans certains films. Cette méthode requiert des sujets coopératifs et entrainés.
Pourtant cette technique semble être tout aussi fiable que celle de l'iris; elle se base sur le fait que le schéma et le dessin formé par les vaisseaux sanguins de la rétine (la paroi interne et opposée de l'oeil) est unique pour chaque individu, différent entre jumeaux et assez stable durant la vie de la personne. La mesure peut ainsi fournir jusqu'à 400 points caractéristique du sujet, que l'on peut comparer aux 30 à 40 points fournis par une empreinte digitale! En conclusion, la mesure rétinienne est la plus difficile à utiliser mais également la plus dure à contrefaire.

- **visage (facial-scan):** il s'agit ici de faire un photographie plus ou moins évoluée pour en extraire un ensemble de facteurs qui se veulent propres à chaque individu. Ces facteurs sont choisis pour leur forte invariabilité et concernent des zones du visage tel que le haut des joues, les coins de la bouche, etc... on évitera d'autre part les types de coiffures, les zones occupées par des cheveux en général ou toute zone sujette à modification durant la vie de la personne.
  Il existe plusieurs variantes de la technologie de reconnaisance du visage. La première est développée et supportée par le MIT et se nomme "Eigenface". Elle consiste à décomposer le visage en plusieurs images faites de nuances de gris, chacune mettant en évidence une caractéristique particulière :



Source : MIT Face Recognition Demo Page

Une autre technique appelée "feature analysis" se base sur la précédente en y rajoutant des informations sur les distances inter-éléments, leurs positions, etc... Elle se dit plus souple quant aux éventuelles modifications pouvant survenir : angle de prise de vue, inclinaison de la tête, etc... Viennent ensuite des techniques moins utilisées à l'heure actuelle, basée sur des réseaux neuronaux, sur des méthodes plus techniques et moins souples.

- **système et configuration des veines (vein pattern-scan):** cette technique est habituellement combinée à une autre, comme l'étude de la géométrie de la main. Il s'agit ici d'analyser le dessin formé par le réseau des veines sur une partie du corps d'un individu (la main) pour en garder quelques points caractéristiques.

Caractéristiques Comportementales

Outre les caractéristiques physiques, un individu possède également plusieurs éléments liés à son comportement qui lui sont propres :

- **dynamique des frappes au clavier (keystroke-scan):** les frappes au clavier sont influencées par plusieurs choses; tout d'abord, selon le texte que l'on tape et, de manière plus générale selon sa nature, on aura tendance à modifier sa façon de taper au clavier. C'est d'ailleurs un des moyens utilisés par certaines attaques (timing attacks) pour essayer d'inférer le contenu ou la nature du texte tapé de façon à remonter jusqu'à un mot de passe par exemple. Ces techniques sont assez satisfaisantes mais restent néanmoins statistiques. Ensuite, le facteur comportemental entre en jeu, et ce facteur va être -lui- différent pour chaque individu. Les facteurs sont à peu de chose près identiques à ceux évoqués précédemment : ce sont les durées entre frappes, la fréquence des erreurs, durée de la frappe elle-même... La différence se situe plus au niveau de l'analyse, qui peut être soit statique et basée sur des réseaux neuronaux, soit dynamique et statistique (comparaison continuelle entre l'échantillon et la référence).

- **reconnaissance vocale (voice-scan):** les données utilisées par la reconnaissance vocale proviennent à la fois de facteurs physiologiques et comportementaux. Ils ne sont en général pas imitables.

- **dynamique des signatures (signature-scan):** ce type de biométrie est à l'heure actuelle peu utilisé mais ses défenseurs espèrent l'imposer assez rapidement pour des applications spécifiques (documents électroniques, rapports, contrats...). Le procédé est habituellement combiné à une palette graphique (ou équivalent) munie d'un stylo. Ce dispositif va mesurer plusieurs caractéristiques lors de la signature, tel que la vitesse, l'ordre des frappes, la pression et les accélérations, le temps total, etc... Bref tout ce qui peut permettre d'identifier une personne de la façon la plus sure possible quand on utilise une donnée aussi changeante que la signature.

Trop beau pour etre simple

La carte d'identité électronique devrait permettre d'atteindre plusieurs objectifs. C'est ce qui fait l'intérêt du projet mais peut-être aussi sa complexité, donc sa potentielle fragilité. En forçant un peu le trait, il serait possible de soutenir que les objectifs, ou arguments, en faveur du projet carte d'identité électronique sont, de façon non exhaustive, les suivants :

- répondre aux exigences de l'OACI et des autorités américaines en matière de titres d'identité sécurisés de nouvelle génération ;
- sécuriser l'identité (contrôle des flux migratoires, lutte contre l'usurpation d'identité) ;
- offrir une clé d'accès aux téléservices sécurisés du secteur public ;
- offrir une clé d'accès sécurisé à des téléservices sécurisés du secteur privé ;
- faire un saut technologique pour rendre obsolètes les faux papiers en circulation ;
- profiter du changement de génération technologique pour rendre payant ce qui était gratuit ;
- aider l'industrie française (ou européenne) de la carte à puce ;
- aider l'industrie française (ou européenne) de la biométrie et plus spécifiquement l'industrie des solutions à base d'empreintes digitales ;

- aider l'industrie française (ou européenne) de la signature électronique ;
- faire moderne, au moins autant que les belges ou les estoniens ;
- etc.

Il sera difficile de tout faire en même temps. La diversité des objectifs du projet risque d'être à la fois un facteur de complexité (donc de délais et de surcoûts) et de susciter méfiance et confusion au sein d'une partie de l'opinion. Ce serait alors prendre le risque de fragiliser durablement une évolution souhaitable. Sans doute faudrait-il s'en tenir à un projet simplifié avec un objectif prioritaire clairement affiché, par exemple, moderniser les titres d'identité pour réduire le nombre de faux papiers en circulation (ou le nombre de « vrais » papiers en possession de « mauvaises » personnes). Pour l'accès sécurisé aux services privés en ligne, il n'est sans doute pas indispensable de mobiliser toute la puissance de l'Etat. Il a plus à perdre qu'à y gagner.

Une technologie de protection de la vie privée

Pourtant, si les promoteurs du projet acceptent de prendre en charge la complexité résultant de la diversité des objectifs, il est alors possible d'en rajouter un de plus. La future carte d'identité électronique ne pourrait-elle pas être envisagée comme une technologie de protection des données personnelles au service du citoyen ; une sorte de coffre-fort électronique portatif ?

Ce serait déjà le cas si certaines des données personnelles étaient « enfouies » dans la puce au lieu d'être exposées, comme c'est le cas aujourd'hui, à la vue de tous. Les caissières des hypermarchés, lors des paiements par chèque, ont aujourd'hui accès à la date et au lieu de naissance du porteur et à une adresse. Est-ce véritablement indispensable ? En outre, l'utilisateur de la carte pourrait disposer d'une relative maîtrises sur ses données personnelles en ayant la possibilité de procéder à des mises à jour, c'est-à-dire d'exercer son droit d'accès et de rectification prévu par la loi informatique et libertés. Cette idée figurait explicitement dans le Livre Blanc Administration électronique et protection des données personnelles de février 2002 (rapport Truche). Depuis, force est de constater que les préoccupations sécuritaires ont fait passé ce type de réflexions au second plan.

Enfin, une des options possibles pour concilier sécurité (de l'Etat et des organisation) et confiance (des citoyens) serait de faire en sorte que la carte électronique du citoyen ne soit pas systématiquement une carte d'identité mais, pour certains usages, uniquement une carte d'habilitation. On pourrait imaginer bien des cas de figure où le porteur de la carte aurait juste besoin de prouver qu'il est majeur, qu'il est ne nationalité française, qu'il possède des droits (par exemple le droit de conduire, de chasser ou de pécher) ou qu'il n'est pas déchu de certains droits (ne pas être interdit de casino, physique ou en ligne) sans avoir pour autant à justifier de son identité.

Une carte électronique du citoyen qui ne soit pas obligatoirement une carte d'identité : ce ne serait ni simple, ni économique. Mais la simplicité et la maîtrise des coûont-il véritablement des critères essentiels pour le projet ?

Inconvénient de la biométrie : égalité vs similitude

La biométrie présente malheureusement un inconvénient majeur; en effet aucune des mesures utilisées ne se révèle être totalement exacte car il s'agit bien là d'une des caractéristique majeure de tout organisme vivant : on s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins importants, bref on évolue et les mesures changent.

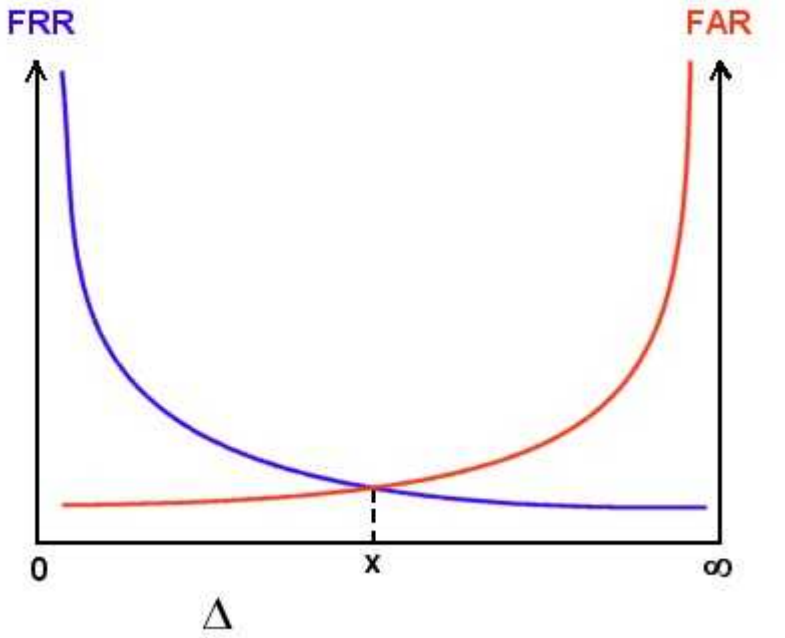
Prenons le cas le plus simple, celui des empreintes digitales (mais on notera que la même chose s'applique à toute donnée physique). Suivant les cas, nous présentons plus ou moins de transpiration; la température des doigts est tout sauf régulière (en moyenne, de 8 à 10° Celsius au-dessus de la

température ambiente). Il suffit de se couper pour présenter une anomalie dans le dessin de ses empreintes. Bref, dans la majorité des cas, la mesure retournera un résultat différent de la mesure initiale de référence. Or il faut pourtant bien réussir à se faire reconnaitre, et en réalité cela marchera dans la plupart des cas car le système autorise une marge d'erreur entre la mesure et la référence.

Le but de ce dispositif est simple : les fabricants ne recherchent nullement la sécurité absolue, ils veulent quelquechose qui fonctionne dans la pratique. Ils cherchent donc à diminuer le taux de faux rejets (False Rejection Rate, FRR), tout en maintenant un taux relativement bas de fausses acceptations (False Acceptation Rate, FAR). Explications : une FR est le fait de rejeter une personne autorisée en temps normal car sa mesure biométrique présente trop d'écart par rapport à la mesure de référence pour cette même personne. Un système fonctionnel aura un FRR le plus bas possible. D'autre part, une FA est le fait d'accepter une personne non-autorisée. Cela peut arriver si la personne a falsifié la donnée biométrique ou si la mesure la confond avec un autre personne.

Un système sûr aura un FAR le plus bas possible.

Dans la vie courante, les industriels cherchent principalement à avoir un compromis entre ces 2 taux, FRR et FAR, qui sont eux liés suivant une relation illustrée ici :



Ce graphe est purement démonstratif; delta représente la marge d'erreur autorisée par le système, variant de 0 à l'infini. Très succintement, on voit que plus la marge d'erreur autorisée est importante, plus le taux de fausses acceptations augmente, c'est-à-dire que l'on va accepter de plus en plus de personnes qui ne sont pas autorisées (et donc la sécurité du système diminue). Par contre on voit que le taux de rejet des personnes autorisées diminue également, ce qui rend le système plus fonctionnel et répond mieux aux attentes des utilisateurs. A l'autre extrémité, si l'on diminue la marge d'erreur acceptée par le procédé de mesure biométrique, les tendances des 2 taux sont inversées : on va de moins en moins accepter des individus essayant de frauder mais on va aussi, par la même occasion, avoir un taux de rejet sur des personnes autorisées qui sera trop important pour être toléré dans la plupart des cas. Le compromis habituel est de prendre la jonction des courbes, càd le point x où le couple (FAR, FRR) est minimal.

En conclusion, toute la biométrie peut se résumer pour les plus pessimistes à ce seul compromis qui fausse toute la confiance que l'on pourrait porter à cette technologie.

Limites de cette technologie

- les données biométriques ne devraient pas être utilisées seules pour de l'authentification forte car elles ne sont pas modifiables puisque par nature propres à chaque individu. On ne peut donc pas se permettre de se baser uniquement dessus, d'autant plus que nous avons vu qu'elles ne sont pas fiables à 100% (FAR/FRR). En règle générale, on préfèrera utiliser la biométrie dans le cadre d'un schéma d'identification plutôt que pour faire de l'authentification.
- les données biométriques sont comparables à tout autre système de contrôle d'accès comme des mots de passe, etc..., car du point de vue du système informatique, ce ne sont rien d'autres que des séries de bits comme toute donnée. Autrement dit, la difficulté réside dans la contrefaçon de la caractéristique physique et biologique que l'on mesure, mais en aucun cas dans sa valeur numérisée (digitale). Prenons l'exemple de notre vieil ami, le login/mot de passe. Ce système est souvent décrit comme peu sûr car une des principales attaques consiste à épier les transactions durant un processus de login pour récupérer les données utiles et les rejouer. On voit que même dans le cas des techniques basées sur la biométrie, cela reste possible! A quoi bon se compliquer la tâche en essayant de reproduire une empreinte alors que l'on peut récupérer les données numérisées directement? Ou si l'on peut attaquer les bases de données contenant toutes les données biométriques de référence?

Conclusion

On retiendra plusieurs fait marquants concernant la biométrie :

- il ne suffit pas de remplacer un login/mot de passe par une mesure de biométrie; il faut également repenser tout le système et sécuriser l'architecture complète.
- il ne faut pas utiliser une mesure biométrique seule pour procéder à une authentification; on préfera la coupler avec une carte à puce, un token sécurisé (petit élément de stockage présentant une grande résistance aux attaques, même physiques), un mot de passe voire un OTP (c.f. article concernant les OTP).
- on utilisera la biométrie de préférence pour les opérations d'identification plutôt que d'authentification.
- enfin, perdons une fois pour toute cette image de technologie ultra sûre faussement propagée par les médias. La biométrie n'est nullement une "solution miracle et universelle"!

Index des pages utilisées

- http://www.cecurity.com/site/html/article_cnie.php
- http://www.pcinpact.com/actu/news/Debat_national_sur_la_carte_didentite_electronique.htm
- http://www.securiteinfo.com/conseils/biometrie.shtml
- http://www.google.fr