Évaluation de la sécurité d'un système biométrique

Mohamad El-Abed et Christophe Rosenberger
Université de Caen Basse-Normandie, UMR 6072 GREYC, F-14032 Caen, France
ENSICAEN, UMR 6072 GREYC, F-14050 Caen, France
CNRS, UMR 6072 GREYC, F-14032 Caen, France
Email : {mohamad.elabed, christophe.rosenberger}@ensicaen.fr

Résumé

*Les systèmes biométriques sont vulnérables à des attaques spécifiques qui peuvent dégrader considérablement leur utilité. Afin de contribuer à résoudre cette problématique, nous proposons 1) une base commune d'attaques et de vulnérabilités des systèmes biométriques, et 2) une méthode générique (*i.e.*, indépendante de la modalité) pour évaluer quantitativement les systèmes biométriques. Deux systèmes d'authentification biométriques ont été utilisés pour illustrer l'intérêt de la méthode proposée.*

Mots clé : Biométrie ; Évaluation ; Vulnérabilité ; Attaque ; Facteur de risque

1. Introduction

La biométrie suscite une attention accrue depuis les attaques terroristes du 11 septembre 2001. L'usage de la biométrie s'est vite étendue dans de nombreuses applications destinées à gérer l'accès à des ressources physiques (aéroports, casinos, *etc.*) et logiques (ordinateurs, comptes bancaires, *etc.*). L'authentification biométrique comporte un avantage primordial sur les solutions d'authentification traditionnelles compte tenu de la relation forte entre l'authentifiant et l'utilisateur. Bien que les méthodes d'authentification biométrique promettent d'être très performantes, on ne peut pas garantir actuellement leur robustesse en pratique dans un contexte d'utilisation spécifique et une cible utilisateurs.
Les systèmes biométriques sont vulnérables à des attaques spécifiques qui peuvent dégrader considérablement leur fonctionnalité et l'intérêt de déployer de tels systèmes. Maltoni *et al.* [1] ont décrit les menaces possibles (*ex.*, *déni de service*) sur une **application générique** protégée par un système d'authentification biométrique. Schneier [2] présente deux inconvénients majeurs des systèmes biométriques que sont l'absence de secret et le problème d'irrévocabilité. Pour le premier inconvénient, tout le monde connaît nos traits biométriques (comme le visage). Tandis que pour la seconde, le trait biométrique ne peut pas être remplacé s'il est compromis. Ratha *et al.* [3] ont regroupé les attaques d'un système biométrique générique en 8 classes comme le montre la Figure 1. Un exemple d'attaque de la classe 1 consiste à présenter une fausse donnée biométrique (*ex.*, doigt prothétique) au capteur.

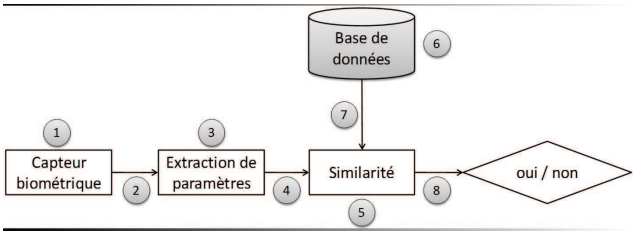

Figure 1. Emplacements des points de compromission d'un système biométrique (extrait de [3]).

Les travaux présentés par Maltoni *et al.*, Schneier et Ratha *et al.* montrent clairement la vulnérabilité des systèmes biométriques. Ainsi, l'évaluation de la sécurité des systèmes biométriques est devenue indispensable pour garantir l'opérationnalité de ces systèmes. Dans cet article, notre contribution est double. Premièrement, nous proposons une base commune d'attaques et de vulnérabilités des systèmes biométriques. Cette base pourra ainsi être utilisée par les évaluateurs pour analyser (quantitativement ou qualitativement) le niveau de sécurité d'un système biométrique. Deuxièmement, nous proposons une méthode quantitative pour évaluer

la sécurité des systèmes biométriques. La méthode proposée est indépendante de la modalité, et inspirée de la méthode d'audit de sécurité EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) [4].
Dans la suite de cet article, la Section 2 décrit la méthode proposée. La base commune d'attaques et de vulnérabilités des systèmes biométriques est donnée dans la Section 3. Les résultats expérimentaux sur deux systèmes d'authentification biométrique sont présentés dans la Section 4. Enfin, la section 5 conclut cet article.

2. Méthode développée

Selon l'Organisation Internationale de Normalisation ISO/IEC FCD 19792 [5], l'évaluation de la sécurité des systèmes biométriques est généralement composée de deux types d'évaluation complémentaires : **type 1)** évaluation du système biométrique (capteurs et algorithmes) et **type 2)** évaluation de l'environnement (est-ce que le système est utilisé en intérieur ou extérieur ?) et des conditions opérationnelles (politique d'administration telles que les mesures effectuées par les administrateurs du système pour n'enrôler que des utilisateurs légitimes, *etc.*). La méthode développée consiste à définir une méthode d'évaluation quantitative générique de **type 1** en utilisant une base commune d'attaques et de vulnérabilités, et la notion de facteur de risque. Le principe de la méthode proposée repose sur quatre étapes : 1) étude du contexte, 2) expression des besoins de sécurité, 3) appréciation des risques et 4) calcul d'un indice de sécurité.

2.1. Étude du contexte

La première étape de la démarche consiste à identifier précisément l'utilité, l'architecture et le fonctionnement du système cible. Il s'agit également de décrire précisément les différents composants et éléments essentiels du système cible (appelé également les biens), qui dépendent généralement de la modalité biométrique considérée. On en retrouve de plusieurs natures, et certains sont généralement communs à tout système d'authentification biométrique. En utilisant l'architecture d'un système biométrique générique présentée dans la Figure 1, nous avons choisi de protéger trois types de biens (information, fonction et matériel) d'un système biométrique générique. Les biens retenus sont décrits dans le Tableau 1.

2.2. Expression des besoins de sécurité

Une fois le système précisément analysé et décrit, l'étape suivante consiste à répertorier les exigences en sécurité auxquelles il doit répondre. Ces exigences pourront ensuite être rapprochées des risques que présente le système pour pouvoir définir des contre-mesures de sécurité à mettre en place. Un système d'authentification biométrique présente dans la majorité des cas des besoins de sécurité génériques, parmi lesquels figurent la confidentialité (C), l'intégrité (I), la disponibilité (D) et l'authenticité (A). L'authenticité permet de garantir que l'utilisateur qui présente la donnée biométrique est bien celui qu'il prétend être.

2.3. Appréciation des risques

Analyser les risques d'un système d'information (SI) est considéré comme un facteur indispensable à sa conception. L'analyse des risques repose sur deux phases [6] : la première consiste à identifier les causes des risques, tandis que la seconde détermine le niveau des risques identifiés (*i.e.*, dangerosité). Il existe plusieurs approches pour analyser les risques d'un SI [7], et elles sont généralement divisées en deux familles : quantitative et qualitative.
Dans cette étude, nous avons choisi d'utiliser une approche quantitative pour diverses raisons. Premièrement, c'est une approche qui permet d'estimer quantitativement les conséquences des risques identifiés, ce qui facilite nettement la comparaison des systèmes biométriques. Deuxièmement, l'approche quantitative est plus exploitable que l'approche qualitative pendant la phase de réduction des risques, puisque ces derniers sont quantitativement ordonnés selon leur degré de dangerosité. Une description détaillée des approches quantitatives et qualitatives est abordée par Rot [8], ainsi que leurs limites d'utilisation. La méthode ainsi proposée utilise la notion de facteurs de risque et la base commune d'attaques et de vulnérabilités présentée dans la Section 3. Un facteur de risque, pour chaque attaque identifiée, est considéré comme un indicateur de sa dangerosité. Nous avons utilisé les facteurs de risque pour décrire quantitativement l'importance des attaques identifiées et des vulnérabilités globales retenues du système cible. Nous présentons ci-après le calcul des facteurs de risques des attaques identifiées, tandis que dans la Section 2.3.2 sont décrits ceux liés aux vulnérabilités globales.

Référence	Type	Description
I_DONNEE_BIO	Information	Donnée biométrique de l'utilisateur qui souhaite s'authentifier
I_MODELE	Information	Modèle biométrique de l'utilisateur
I_DECISION	Information	Décision du système d'authentification (oui ou non)
F_TRAITEMENT	Fonction	Fonction de traitement des données biométriques issues du capteur biométrique
F_COMPARAISON	Fonction	Fonction de comparaison entre la donnée biométrique et le modèle biométrique
M_CAPTEUR	Matériel	Capteur biométrique
M_PROCESSUS	Matériel	Matériel sur lesquels les processus F_TRAITEMENT et F_COMPARAISON sont exécutés
M_BDD	Matériel	Support du stockage des modèles biométriques
M_CANAUX	Matériel	Canaux de transmission qui relient les différents composants du système

Table 1. Les biens d'un système d'authentification biométrique générique.

2.3.1. Facteurs de risque des attaques identifiées. Afin de calculer le facteur de risque pour chaque attaque identifiée, nous utilisons une approche quantitative inspirée de l'Analyse Multi-Critères (MCA) [9]. Plus spécifiquement, nous utilisons deux critères pour calculer un facteur de risque (f_r) pour chaque attaque identifiée :

$$f_r = c_1 \times c_2 \tag{1}$$

- La gravité (c_1) représente l'impact de l'attaque en terme de criticité. Ce facteur est défini sur une échelle entre 0 et 10 (le plus haut score 10 correspond à une attaque très critique). Il est arbitrairement fixé selon les besoins de sécurité retenus (confidentialité, intégrité, disponibilité et authenticité) sur les biens identifiés ;
- La facilité (c_2) représente la difficulté pour implémenter une attaque réussie. Ce facteur est défini sur une échelle entre 0 et 10 (le score 0 correspond à une attaque impossible, tandis que le score 10 correspond à une attaque très facile). Il est arbitrairement fixé selon les trois informations suivantes : i) la vulnérabilité du système (failles liées à l'architecture de déploiement), ii) le coût en terme d'équipements spécifiques nécessaires pour implémenter l'attaque en question et iii) le niveau d'expertise requis (l'attaquant devrait maîtriser des connaissances techniques pour développer un programme malveillant).

2.3.2. Facteurs de risque des vulnérabilités globales. Pour les trois vulnérabilités globales retenues d'un système biométrique (*cf.*, Section 3.2), nous avons développé un ensemble de règles pour estimer le facteur de risque associé comme décrit dans le Tableau 2. Pour la performance du système, nous avons multiplié le taux d'erreur par deux puisque un système biométrique possédant un taux d'erreur (selon le système cible, EER ou HTER) supérieur ou égal à 50% n'est pas possible (pour un système d'authentification). Pour de tels systèmes, nous mettons ainsi le facteur de risque associé à 100. Pour la qualité, nous avons défini quatre règles selon le niveau de mise en oeuvre d'un contrôle de qualité du système pendant la phase d'enrôlement. Pour la base des modèles biométriques, nous avons également défini un ensemble de règles selon le degré de mise en oeuvre de mécanismes de protection (chiffrement et révocabilité des modèles biométriques) du système sur cet élément essentiel. Les quantifications du facteur de risque dans ce tableau sont certes arbitraires mais nous comptons solliciter la communauté en biométrie pour obtenir un consensus des experts.

2.4. Indice de sécurité

Estimer le niveau de sécurité global d'un système biométrique (plus généralement d'un SI), est une tâche difficile puisque le nombre d'acteurs impliqué dans le processus d'authentification est important. Dès lors, il est toujours avantageux d'illustrer la sécurité globale du système cible par un indice ($0-100$) pour faciliter l'évaluation et la comparaison des tels systèmes [10]. Pour ce faire, nous avons utilisé la notion d'aire sous la courbe sur les facteurs de risque retenus pour calculer l'indice de sécurité globale du système cible. L'indice de sécurité est ainsi défini par :

$$\text{Indice} = \alpha \left(1 - \frac{AUC(f(x))}{AUC(g(x))}\right) = \alpha \left(1 - \frac{\int_1^n f(x)\,\mathrm{d}x}{\int_1^n g(x)\,\mathrm{d}x}\right) \tag{2}$$

Point	Description	Conditions	Facteur de risque (f_r)
9	Performance du système	Panel suffisant d'utilisateurs	2 × EER (limité à 100)
10	La qualité du modèle biométrique pendant l'enrôlement	- Plusieurs captures avec contrôle de qualité - Une seule capture avec contrôle de qualité - Plusieurs captures sans contrôle de qualité - Une seule capture sans contrôle de qualité	0 40 60 100
11	Mécanismes de protection de la base des modèles biométriques	- Base sécurisée et stockage local - Base sécurisée et stockage central - Base non sécurisée et stockage local - Base non sécurisée et stockage central	0 40 60 100

Table 2. Vulnérabilités globales des systèmes biométriques : les facteurs de risque.

où $\alpha = 100$, $n = r + s$, avec r le nombre d'emplacements des points de compromission (dans notre cas, $r = 8$) et s le nombre des vulnérabilités globales retenues (dans notre cas, $s = 3$). La fonction $f(x)$ représente la courbe obtenue à partir des facteurs de risque retenus sur les 11 points (le facteur de risque maximal est retenu à chaque point de compromission). Tandis que la fonction $g(x)$ représente la courbe obtenue à partir de l'ensemble des facteurs de risque le plus élevé qu'on peut avoir à chaque point de compromission (dans notre cas, ils sont égaux à 100). Plus l'indice est proche de 100, meilleure est la robustesse du système cible contre la fraude.

3. Base commune d'attaques et de vulnérabilités

La base d'attaques et de vulnérabilités prend en considération les attaques et vulnérabilités de la littérature (comme ceux présentées dans [11]), ainsi que les vulnérabilités présentées par l'Organisation Internationale de Normalisation ISO/IEC FCD 19792 [5]. Outre les attaques identifiées sur les huit emplacements de compromission présentés par Ratha *et al.*, nous avons ajouté trois vulnérabilités globales (*cf*, Section 3.2) qui nous ont paru pertinentes lors de l'évaluation de la sécurité des systèmes biométriques. Nous présentons ci-après la base commune d'attaques identifiées, tandis que les vulnérabilités globales sont données dans la section 3.2.

3.1. Attaques des systèmes biométriques

La base commune d'attaques identifiées aux huit emplacements de compromission (*cf.*, Figure 1) est donnée sous la forme suivante : «description» de l'attaque ainsi que son «atteinte» sur les besoins de sécurité retenus dans la Section 2.2. Cette illustration va nous permettre de quantifier la gravité (c_1) de chaque attaque identifiée lors de l'évaluation de la sécurité du système cible.

Point 1. Capteur

$\mathbf{A}_{11}$ - *Description* L'attaquant présente au capteur une fausse donnée biométrique (*e.g.*, doigts prothétiques) pour usurper l'identité d'un utilisateur légitime.
- *Atteintes* Authenticité sur L_DECISION.

$\mathbf{A}_{12}$ - *Description* L'attaquant exploite la similarité des données biométriques (le cas de jumeaux identiques et les systèmes biométriques utilisant des modalités spécifiques tels que le visage et l'ADN).
- *Atteintes* Authenticité sur L_DECISION.

$\mathbf{A}_{13}$ - *Description* Les utilisateurs légitimes fournissent volontairement leur donnée biométrique à l'attaquant (photo d'iris de bonne qualité).
- *Atteintes* Authenticité sur L_DECISION.

$\mathbf{A}_{14}$ - *Description* L'attaquant fournit sa propre donnée biométrique (tentative zéro effort) pour usurper l'identité d'un utilisateur légitime. En général, les attaquants choisissent des victimes ayant un faible modèle biométrique (image d'un visage de mauvaise qualité).
- *Atteintes* Authenticité sur L_DECISION.

$\mathbf{A}_{15}$ - *Description* L'attaquant récupère et exploite une donnée biométrique résiduelle (image d'une empreinte) sur le capteur afin d'usurper l'identité du dernier utilisateur authentifié.
- *Atteintes* Confidentialité sur L_DONNEE_BIO ; Authenticité sur L_DECISION.

$\mathbf{A}_{16}$ - *Description* L'attaquant dégrade le capteur biométrique pour le mettre hors d'état de fonctionnement.
- *Atteintes* Disponibilité sur M_CAPTEUR.

Points 2 et 4. Canaux de transmission

$\mathbf{A}_{241}$ - *Description* L'attaquant intercepte et rejoue

une donnée biométrique à partir d'un canal de transmission.
- *Atteintes* Confidentialité sur I_DONNEE_BIO ; Authenticité sur I_DECISION.
$\mathbf{A}_{242}$ - *Description* L'attaquant détruit le canal de transmission afin de rendre le système indisponible pour les utilisateurs légitimes.
- *Atteintes* Disponibilité sur M_CANAUX.
$\mathbf{A}_{243}$ - *Description* L'attaquant altère l'information transportée sur le canal pour empêcher les utilisateurs légitimes de s'authentifier.
- *Atteintes* Intégrité sur I_DONNEE_BIO ; Intégrité sur M_CANAUX.
$\mathbf{A}_{244}$ - *Description* L'attaquant tente en permanence de s'authentifier par le système, en injectant des données au module de traitement (image d'une empreinte) ou au module de comparaison (minuties) [12].
- *Atteintes* Authenticité sur I_DECISION.
$\mathbf{A}_{245}$ - *Description* L'attaquant injecte en permanence des données pour rendre le système inaccessible aux utilisateurs légitimes.
- *Atteintes* Disponibilité sur M_CANAUX.

Points 3 et 5. Les composants logiciels
$\mathbf{A}_{351}$ - *Description* Les composants logiciels du système peuvent être remplacés par un programme du type cheval de Troie qui fonctionne selon les spécifications de ses concepteurs.
- *Atteintes* Confidentialité sur I_DONNEE_BIO ; Confidentialité sur I_MODELE ; Disponibilité sur F_TRAITEMENT ; Disponibilité sur F_COMPARAISON.

Point 6. Base des modèles biométriques
$\mathbf{A}_{61}$ - *Description* L'attaquant accède en mode lecture à la base des modèles biométriques.
- *Atteintes* Confidentialité sur I_MODELE ; Authenticité sur I_DECISION.
$\mathbf{A}_{62}$ - *Description* L'attaquant modifie (ajout, remplacement ou suppression) les modèles biométriques de la base.
- *Atteintes* Disponibilité sur I_MODELE ; Intégrité sur I_MODELE.

Point 7. Canal de transmission
$\mathbf{A}_{71}$ - *Description* L'attaquant intercepte un modèle biométrique à partir du canal de transmission afin d'être rejoué.
- *Atteintes* Confidentialité sur I_MODELE ; Authenticité sur I_DECISION.
$\mathbf{A}_{72}$ - *Description* L'attaquant altère les modèles biométriques transportés sur le canal pour empêcher les utilisateurs légitimes de s'authentifier.
- *Atteintes* Intégrité sur I_MODELE ; Intégrité sur M_CANAUX.
$\mathbf{A}_{73}$ - *Description* L'attaquant détruit le canal de transmission afin de rendre le système indisponible pour ses utilisateurs légitimes.
- *Atteintes* Disponibilité sur M_CANAUX.

Point 8. Canal de transmission
$\mathbf{A}_{81}$ - *Description* L'attaquant altère le résultat transporté (oui/non) pour empêcher l'accès d'un utilisateur légitime, ou ouvrir l'accès d'un imposteur.
- *Atteintes* Intégrité sur I_DECISION ; Authenticité sur I_DECISION.
$\mathbf{A}_{82}$ - *Description* L'attaquant détruit le canal de transmission afin de rendre le système indisponible pour ses utilisateurs légitimes.
- *Atteintes* Disponibilité sur M_CANAUX.

3.2. Vulnérabilités globales des systèmes biométriques

Point 9. Limites de performance
En comparaison aux systèmes d'authentification traditionnels qui offrent une réponse binaire (oui ou non), les systèmes biométriques sont moins précis et sont soumis à des erreurs telles que les taux de fausses acceptations (FAR) et de faux rejets (FRR). Cette variation illustrée par les taux d'erreurs peut affecter les systèmes biométriques en terme de sécurité. Doddington *et al.* [13] divisent les utilisateurs légitimes en quatre catégories que sont les moutons, les agneaux, les chèvres et les loups. Les moutons sont ceux qui peuvent être facilement reconnus (ils contribuent à une faible valeur du FRR). Les agneaux sont ceux qui peuvent être facilement imités (ils contribuent à un FAR élevé). Les chèvres sont ceux qui peuvent être difficilement reconnus (ils contribuent à un FRR élevé). Les loups sont ceux qui ont la capacité d'usurper facilement d'autres utilisateurs légitimes (ils contribuent à un FAR élevé). Ainsi, un système biométrique peu efficient en terme de performance, peut être vulnérable face aux agneaux et loups.

Point 10. Limites de qualité pendant la phase d'enrôlement
La qualité des données acquises pendant la phase d'enrôlement est un facteur important à prendre en compte lors du développement des systèmes biométriques. L'absence d'un test de qualité augmente la possibilité d'avoir de faibles modèles biométriques. Ces modèles augmentent nettement la probabilité de réussite des attaques par zéro effort, hill-climbing et force brute [12].

Point 11. Mécanismes de protection des modèles biométriques

L'utilisation de la biométrie présente des vulnérabilités en termes de respect des droits et des libertés fondamentales. Le fait de conserver des modèles biométriques dans une base de données centrale constitue une invasion de la vie privée. Ces données sont donc des données sensibles, qui ne sont pas encore protégées de façon spécifique par une norme internationale (même si la norme ISO/IEC 27000 [14] adresse la protection des données personnelles). Ainsi, un système qui ne met pas en oeuvre de mécanismes de protection des modèles biométriques, peut être vulnérable à des attaques par rejeu.

4. Résultats expérimentaux

4.1. Étude du contexte et besoins de sécurité

Nous avons utilisé deux systèmes d'authentification biométrique pour montrer l'intérêt de la méthode proposée. Le premier système est le logiciel GREYC-Keystroke [15] basé sur la dynamique de frapper au clavier. Le deuxième, est un système commercial Fingerprint lock basé sur l'empreinte digitale. Les principales caractéristiques de ces deux systèmes sont : i) GREYC-Keystroke possède un taux d'égale erreur (EER) égal à $17,51\%$ sur une base composée de 70 individus, avec 3 vecteurs d'enrôlement et 2 pour le test ; ii) Fingerprint lock fournit un taux de fausses acceptations (FAR) égal à 0.0001% et un taux de faux rejets (FRR) égal à 0.1%. Le taux d'erreur moyen (HTER) est ainsi égal à 0.05% ; iii) L'architecture des deux systèmes n'est pas distribuée ; iv) Aucun mécanisme de protection des données ni de chiffrement sur la base des modèles biométriques est mis en oeuvre dans les deux systèmes ; v) Aucun test de qualité n'est utilisé pour contrôler la qualité des données biométriques acquises pendant la phase d'enrôlement dans les deux systèmes ; vi) Le PC utilisé pour GREYC-Keystroke est connecté sur Internet.
Nous avons choisi de comparer ces deux systèmes différents (en terme de conception) puisque les résultats de leur évaluation et leur comparaison devraient pouvoir être aussi différents que possible. Les biens ainsi que les besoins de sécurité retenus sont ceux présentés dans le Tableau 1 et la Section 2.2, respectivement.

4.2. Appréciation des risques

Afin d'analyser les risques sur les deux systèmes cibles présentés dans la section précédente, nous avons utilisé la base commune d'attaques et de vulnérabilités des systèmes biométriques (*cf.*, Section 3), et la notion de facteurs de risque (*cf.*, Section 2.3). Les deux Tableaux 3 et 4, présentent l'analyse des deux systèmes cibles GREYC-Keystroke et Fingerprint lock, respectivement. Nous avons mis le symbole «-» dans les trois dernières lignes de chacun de ces deux tableaux, puisque les facteurs de risque des vulnérabilités globales retenues sont évalués à l'aide des règles comme le montre le Tableau 2.
Pour les attaques possibles sur le capteur (point 1), nous avons identifié trois attaques possibles (A_{14}, A_{15}, A_{16}) sur le système GREYC-Keystroke, et quatre ($A_{11}, A_{13}, A_{15}, A_{16}$) pour Fingerprint lock. Pour le système cible GREYC-Keystroke, l'attaque A_{13} n'était pas possible puisque un utilisateur légitime ne peut pas donner à un imposteur sa façon de taper sur un clavier. Pour Fingerprint lock, l'attaque A_{12} n'était pas possible puisque l'empreinte digitale est unique pour chaque personne (même pour le cas de jumeaux identiques [16]). Prenons le cas de l'attaque de type écoute et rejoue (A_{15}) présente dans les deux systèmes cibles. Pour le facteur «gravité (c_1)» de l'attaque A_{15}, nous avons mis les valeurs 8 et 10 pour le système GREYC-Keystroke et Fingerprint lock, respectivement. Nous avons mis la valeur 8, puisque l'attaquant ne récupère que des événements de temps, qui n'a pas d'impact tangible sur la vie privée. Tandis que dans le cas du système Fingerprint lock, nous l'avons mis à 10 puisque l'accès à la donnée biométrique brute constitue une intrusion dans la vie privée. Pour le facteur «facilité (c_2)» de l'attaque A_{15}, nous avons mis les valeurs 3 et 6 pour le système GREYC-Keystroke et Fingerprint lock, respectivement. Nous avons plus pénalisé le système Fingerprint lock que le système GREYC-Keystroke, puisque c'est beaucoup plus facile de récupérer une image d'empreinte digitale résiduelle sur le capteur que de récupérer des événements de temps. Henniger *et al.* [17] et Marcela Espinoza [18] montrent clairement la facilité de récupérer une image résiduelle d'une empreinte digitale pour usurper l'identité d'un utilisateur légitime.
La Figure 2 illustre une étude comparative des facteurs de risque (le facteur de risque maximal est retenu à chaque point de compromission) entre les deux systèmes cibles. En utilisant cette figure, nous pouvons déduire plusieurs résultats tels que : Fingerprint lock est plus vulnérable au point 1 que GREYC-Keystroke, les deux systèmes ne sont pas vulnérables au point 4, et le système GREYC-

Keystroke est plus vulnérable que le deuxième système aux points de compromission $2, 3, 5, 6, 7, 8$ et 9. D'autre part, en utilisant les facteurs de risque ainsi calculés et l'équation 2, les indices du sécurité du système GREYC-Keystroke et Fingerprint lock sont ainsi égaux à $56,7\%$ et 86%, respectivement. Ces résultats montrent que le système GREYC-Kesytroke est globalement plus vulnérable aux attaques que le système Fingerprint lock. Ce résultat pouvait être attendu dans la mesure ou aucune mesure particulière n'a été prise pour sécuriser GREYC-Keystroke dont sa vocation est de fournir un logiciel de démonstration d'une modalité biométrique peu répandue.
Enfin, puisque le système Fingerprint lock est une boîte noire (*i.e.*, pas de documentation), nous n'avons pas pu identifier d'attaques sur quelques points de compromission. Malgré ça, un attaquant pourrait être en mesure de les trouver, grâce à du reverse engineering (matériel et logiciel). Cependant, l'utilisation du système commercial dans cette étude est retenue afin de montrer l'intérêt de la méthode proposée pour évaluer et comparer les systèmes d'authentification biométrique. D'une manière plus générale, lors de l'évaluation d'un système biométrique, les concepteurs doivent fournir tous les détails (architecture, caractéristiques, *etc.*) du système cible aux évaluateurs.

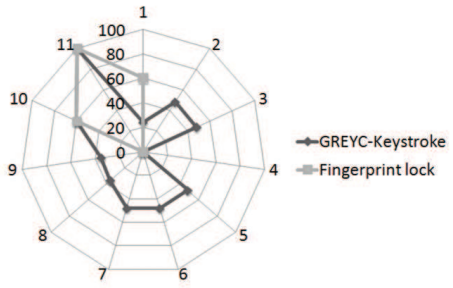

Figure 2. Une illustration comparative des deux systèmes cibles selon notre modèle d'analyse sécuritaire : huit points de compromission et trois vulnérabilités globales d'un système biométrique générique.

5. Conclusion

L'évaluation des systèmes biométriques est considérée comme un enjeu majeur en biométrie. Malgré les travaux d'évaluation existants, peu d'études se sont focalisées sur l'évaluation de ces systèmes en terme de sécurité. La principale contribution de cet article est la présentation 1) d'une base commune d'attaques et de vulnérabilités des systèmes biométriques, 2) d'une méthode générique pour évaluer quantitativement la sécurité des systèmes biométriques. Nous avons montré son intérêt pour évaluer et comparer les systèmes d'authentification biométrique.
La méthode proposée présente l'avantage d'être indépendante de la modalité biométrique considérée, et facile à utiliser puisque l'approche retenue est quantitative. Cependant, le calcul des facteurs de risque est arbitrairement fixé. Afin de résoudre cette limite, nous comptons faire une évaluation subjective de la méthode proposée. Pour cela, nous avons prévu de faire évaluer par des experts les résultats d'analyse de sécurité (notamment, les valeurs subjectives de facteurs de risque). La comparaison des résultats d'analyse sécuritaire provenant des experts avec ceux obtenus par notre méthode d'évaluation nous permettra de l'améliorer.

Références

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer-Verlag, 2003.

[2] B. Schneier. The uses and abuses of biometrics. *Communications of the ACM*, 1999.

[3] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40 :614 – 634, 2001.

[4] EBIOS. Expression des besoins et identification des objectifs de sécurité (EBIOS). Technical report, L'Agence nationale de la sécurité des systèmes d'information (ANSSI), 2004.

[5] ISO/IEC FCD 19792. Information technology – security techniques – security evaluation of biometrics, 2008.

[6] G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology system. Technical report, National Institute of Standards and Technology (NIST), 2002.

[7] R. Ortalo, Y. Deswarte, and M. Kaaniche. Experimenting with quantitative evaluation tools for monitoring operational security. *IEEE Transactions on Software Engineering*, 25 :633–650, 1999.

[8] A. Rot. IT risk assessment : Quantitative and qualitative approach. In *the World Congress on Engineering and Computer Science (WCECS)*, pages 1–6, 2008.

[9] MCA. *Multi-criteria analysis : a manual*. Department for Communities and Local Government : London, 2009.

Point	Attaque	C	I	D	A	Gravité (c_1)	Facilité (c_2)	Risque (f_r)
1	A_{14}				×	6	2	12
	A_{16}			×		2	10	20
	A_{15}	×			×	8	3	24
2	A_{245}			×		2	6	12
	A_{243}		×			2	6	12
	A_{242}			×		2	10	20
	A_{244}				×	6	4	24
	A_{241}	×			×	8	6	48
3	A_{351}	×		×		8	6	48
5	A_{351}	×		×		8	6	48
6	A_{62}		×	×		8	4	32
	A_{61}	×			×	8	6	48
7	A_{72}		×			2	6	12
	A_{73}			×		2	10	20
	A_{71}	×			×	8	6	48
8	A_{82}			×		2	10	20
	A_{81}		×		×	6	6	36
9	Performance du système				×	-	-	35.02
10	Plusieurs captures sans contrôle de qualité				×	-	-	60
11	Base non sécurisée et stockage centrale	×	×	×	×	-	-	100

Table 3. Analyse sécuritaire du système GREYC-Keystroke (C : Confidentialité, I : Intégrité, D : Disponibilité, A : Authenticité).

Point	Attaque	C	I	D	A	Gravité (c_1)	Facilité (c_2)	Risque (f_r)
1	A_{16}			×		2	10	20
	A_{11}				×	6	8	48
	A_{13}				×	6	8	48
	A_{15}	×			×	10	6	60
9	Performance du système				×	-	-	0.1
10	Plusieurs captures sans contrôle de qualité				×	-	-	60
11	Base non sécurisée et stockage centrale	×	×	×	×	-	-	100

Table 4. Analyse sécuritaire du système Fingerprint lock (C : Confidentialité, I : Intégrité, D : Disponibilité, A : Authenticité).

[10] J. Ashbourn. Vulnerability with regard to biometric systems. http ://www.eetimes.com/, 2010.

[11] C. Roberts. Biometric attack vectors and defences. *Computers & Security*, 2007.

[12] U. Uludag and A. K. Jain. Attacks on biometric systems : A case study in fingerprints. In *Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI*, volume 5306, pages 622–633, 2004.

[13] G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds. Sheep, goats, lambs and wolves : A statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation. In *International Conference on Spoken Language Processing (ICSLP)*, pages 1–4, 1998.

[14] ISO/IEC 27000. Information technology – security techniques – information security management systems – overview and vocabulary, 2009.

[15] R. Giot, M. El Abed, and C. Rosenberger. Greyc keystroke : a benchmark for keystroke dynamics biometric systems. In *IEEE Third International Conference on Biometrics : Theory, Applications and Systems (BTAS)*, pages 1–6, 2009.

[16] A. K. Jain, S. Prabhakar, and S. Pankanti. Can identical twins be discriminated based on fingerprints ? Technical report, Department of Computer Science, Michigan State University, 2000.

[17] O. Henniger, D. Scheuermann, and T. Kniess. On security evaluation of fingerprint recognition systems. In *Internation Biometric Performance Testing Conference (IBPC)*, pages 1–10, 2010.

[18] M. Espinoza, C. Champod, and P. Margot. Vulnerabilities of fingerprint reader to fake fingerprints attacks. *Forensic Science International*, 204 :41–49, 2010.