

**6, Boulevard Maréchal Juin - 14050 Caen Cedex**

**Tél. +33 (0)2 31 45 27 50 Fax +33 (0)2 31 45 27 60**

**Site web : www.ensicaen.fr**

**TP Analyse sécurité**

**Analyse de sécurité d’un système utilisant**

**les veines de la main**

**Olivier Brizai / Maxime Thoraval**

Table des matières

[1) Introduction 3](#_Toc285190914)

[2) Présentation du contexte de mise en place du système d'authentification 3](#_Toc285190915)

[3) Présentation générale du système 3](#_Toc285190916)

[a) Structure informatique 3](#_Toc285190917)

[i. Les domaines 3](#_Toc285190918)

[ii. Les modules 3](#_Toc285190919)

[iii. Architecture 4](#_Toc285190920)

[b) Utilisateurs 4](#_Toc285190921)

[4) Expression des besoins de sécurité 5](#_Toc285190922)

[a) Choix des critères de sécurité 5](#_Toc285190923)

[Détermination de l'échelle des besoins 6](#_Toc285190924)

[5) Vulnérabilités du système 8](#_Toc285190925)

[6) Evènements redoutés 8](#_Toc285190926)

[7) Menaces 9](#_Toc285190927)

[a) Menaces possibles 9](#_Toc285190928)

[b) Menaces du système à analyser 9](#_Toc285190929)

[i. Le(s) capteur(s) 9](#_Toc285190930)

[ii. Lien(s) entre capteur(s) et extracteur(s) d’informations 10](#_Toc285190931)

[iii. L’extracteur(s) d’informations 10](#_Toc285190932)

[iv. Lien(s) entre l’extracteur(s) et le module(s) de calcul 10](#_Toc285190933)

[v. Le(s) module(s) de calcul 11](#_Toc285190934)

[vi. La(es) base(s) de données 11](#_Toc285190935)

[vii. Lien(s) entre la(es) base(s) de données et le(s) module(s) de calcul 11](#_Toc285190936)

[viii. Le(s) module(s) de décision 12](#_Toc285190937)

[1) Croisement des évènements redoutés et des scénarios de menaces 12](#_Toc285190938)

[2) Contre-mesures 13](#_Toc285190939)

[3) Identification des objectifs de sécurité 14](#_Toc285190940)

[4) Conclusion 14](#_Toc285190941)

# Introduction

Ce document propose une étude d’un système utilisant la biométrie à base des veines de la main.

# Présentation du contexte de mise en place du système d'authentification

Nous ne présenterons pas d’entreprise dans ce contexte. Mais nous pouvons supposer que celle-ci nécessite de restreindre l’accès à une salle d’un batîment contenant des informations sensibles.

# Présentation générale du système

Le système utlise les veines de la main de personnes afin de vérifier leur identité.

## Structure informatique

### Les domaines

On définit tout d'abord 3 grands domaines :

* Le système centrale d'identification : Le système informatique générale qui contrôle et organise l'authentification des utilisateurs dans l’entreprise. Celui-ci est situé près du lieu nécessitant l’utilisation du système biométrique.
* Les points d'acquisition : les points d'acquisition est un lecteur des veines de la main.
* Le domaine de l'utilisateur : Le domaine de l’utilisateur ici est « sa main ». En effet, c’est seulement lui qui possède cette information.

Le point d’acquisition et le système centrale sont reliés dans les murs cachés dans des gaines sécurisées.

### Les modules

**1– Les capteurs**

Un seul capteur est nécessaire pour notre système, celui permettant de lire les veines de la main. L’entreprise le créeant est de source fiable (grand entreprise réputée dans ce domaine). De plus, il est considéré comme très fiable (pas de bugs).

**2 – La base de données**

La base de donnée est de type Oracle. Elle est enregistrée au sein du système générale.

**4 – L'extracteur des données**

L’extracteur de données est située au sein du système générale.

**5 – Un module de calcul**

Le module de calcul est situé dans la même salle que le système générale. Il est renfermé au sein d’HSM.

**6 - Module de prise de décision**

Comme pour le module de calcul, il est dans la même salle que le système générale. Il est, lui aussi, contenu dans un HSM qui lui est propre.

### Architecture

Ci-dessous l’architecture du système (basé sur une des génériques proposés).

Toutes les informations utilisateurs sont contenues au sein d’une base de données gérée par un système centrale. L’extracteur est lui aussi géré par ce même système.

Le système biométrique et de décision sont, quand à eux, contenu dans deux HSM distinctes.

L’architecture du système correspond à celle présentée ci-dessous avec la partie **Service** + la base de données qui sont située dans la même salle. Et le **Local station** avec le capteur situé à distance de la salle.



## Utilisateurs

Les utilisateurs du sytème seront des personnes haut gradés :

* président de l’entreprise
* vice président

Ainsi que les administrateurs le gérant.

# Expression des besoins de sécurité

## Choix des critères de sécurité

Les besoins de sécurité sont les mêmes que ceux proposés. C’est à dire Confidentialité, Disponibilité, Intégrité et Authenticité.

|  |  |
| --- | --- |
| **Confidentialité** | |
| Description | Propriété des éléments essentiels de n'être accessibles qu'aux utilisateurs autorisés.  Pour une fonction : protection des algorithmes décrivant les règles de gestion et les résultats dont la divulgation à un tiers non autorisé porterait préjudice ; absence de divulgation d'un traitement ou mécanisme à caractère confidentiel.  Pour une information : protection des données dont l'accès ou l'usage par des tiers non autorisés porterait préjudice ; absence de divulgation de données à caractère confidentiel. |
| **Disponibilité** | |
| Description | Propriété d'accessibilité au moment voulu des éléments essentiels par les utilisateurs autorisés.  Pour une fonction : garantie de la continuité des services de traitement ; absence de problèmes liés à des temps de réponse au sens large.  Pour une information : garantie de la disponibilité prévue pour l'accès aux données (délais et horaires) ; il n'y a pas de perte totale de l'information ; tant qu'il existe une version archivée de l'information, l'information est considérée comme disponible ; pour étudier la disponibilité d'une information, on suppose l'existence d'une version archivée, et on évalue la disponibilité qui correspond à la fonction d'archivage de cette information. |
| **Intégrité** | |
| Description | Propriété d'exactitude et de complétude des éléments essentiels.  Pour une fonction : assurance de conformité de l'algorithme ou de la mise en œuvre des traitements automatisés ou non par rapport aux spécifications ; absence de résultats incorrects ou incomplets de la fonction.  Pour une information : garantie d'exactitude et d'exhaustivité des données vis-à vis d'erreurs de manipulation ou d'usages non autorisés ; non-altération de l'information. |
| **Authenticité** |  |
| Description | Propriété assurant une authenticité des destinataires et des origines.  Pour une fonction : La fonction a bien été mise en place par la bonne personne.  Pour une information : l’information provient bien de la source attendue ou est bien envoyée au bon destinataire. |

## Détermination de l'échelle des besoins

On décline ici les critères de sécurité précédemment choisis sur plusieurs niveaux :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Confidentialité** | **Disponibilité** | **Intégrité** | **Authenticité** |
| **0** | *Public* | *Court terme* | *Aucun besoin d'intégrité* | *Falsifié* |
| L'élément essentiel est accessible à tous sans aucune restriction. | L'élément essentiel doit être disponible dans la journée. | Il n'y a aucun besoin de garantir l'intégrité de l'élément essentiel. | La source ou la destination ne sont pas les bonnes |
| **1** | *Supposé Restreint à l'utilisateur* | *Très court terme (temps réel)* | *Parfaitement intègre* | *Authentique* |
| L'élément essentiel est supposée accessible seulement par la l'utilisateur du système mais cet élément peut être facilement récupérable. | L'élément essentiel doit être disponible en temps réel. | L'élément essentiel doit être parfaitement intègre. | On reçoit bien les données de la bonne source et on envoie bien les données au bon destinataire. |
| **2** | *Restreint à l'utilisateur* |  |  |  |
| L'élément essentiel est accessible seulement par la l'utilisateur du système. |  |  |  |
| **3** | *Confidentiel* |  |  |  |
| L'élément essentiel est accessible seulement aux personnes accréditées |  |  |  |

Critères d'évaluation

Après avoir décrit les critères qui nous intéressent dans la recherche de sécurité pour notre système, il faut maintenant décrire les critères d'évaluation du système. Nous proposons ici une méthode basée sur la gravité des risques ainsi que sur la vraisemblance des menaces auquel le système peut-être soumis. Les métriques suivantes sont ainsi définies.

**La vraisemblance**

A chaque menace on associe un niveau de vraisemblance :

|  |  |
| --- | --- |
| **Niveaux de l'échelle** | **Description détaillée de l'échelle** |
| **1 - Minimale** | Cela ne devrait pas se (re)produire |
| **2 - Significative** | Cela pourrait se (re)produire |
| **3 - Forte** | Cela devrait se (re)produire |
| **4 - Maximale** | Cela va certainement se (re)produire |

**La gravité**

A chaque risque on associe un niveau de gravité :

|  |  |
| --- | --- |
| **Niveaux de l'échelle** | **Description détaillée de l'échelle** |
| **1 - Négligeable** | Le système surmontera les impacts sans difficulté |
| **2 - Limité** | Le système surmontera les impacts malgré quelques difficultés. |
| **3 - Importante** | Le système surmontera les impacts avec de sérieuses difficultés. |
| **4 - Critique** | La survie du système est menacée. |

Présentation des biens du système

Toujours dans l'expression du besoin de sécurité, nous nous intéressons ici à la description des biens du système. Il y a les biens essentiels du système, c'est à dire les biens essentiels du système biométrique. Ces biens reposent sur les biens supports. Les biens supports ont pu être présentés dans la partie *1 - Présentation générale du système*.

**Les biens essentiels au système**

Le bien essentiel du système est l’empreinte des veines des mains des utilisateurs autorisés à accéder à la salle, ainsi que les informations liées (données extraites de cette empreinte, …)

|  |  |  |
| --- | --- | --- |
| **Processus généraux** | **Processus essentiels** | **Informations essentielles concernées** |
| **Capture de la donnée biométrique** | | |
| La capture de la veine de la main | Aposer la main  Detection d’une demande d’authentification  Capture des veines de la main | Veines de la main |
| **Extraction de l’information biométrique** | | |
| Traitement de l’acquision | Traitement de l’empreinte lue à partir du capteur. Pour se faire, il faut envoyer celle-ci à l’extracteur d’information. | Les données transmises par le capteur |

**Liens entre biens essentiels et biens supports**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Biens supports |  | Biens essentiels | Aposer la main | Detection d’une demande d’authentification | Capture des veines | Transfert des données |
| Domaine utilisateur | | | | |  |  |
| [Aucun dans notre cas] | | |  |  |  |  |
| Point d’acquisition | | | | |  |  |
| Le point de capture de l’info biométrique | | | X |  |  |  |
| Le capteur des veines | | |  | X | X |  |
| Lien entre capteur et extracteur | | |  |  |  | X |
| Lien entre système générale et HSMs | | |  |  |  | X |

# Vulnérabilités du système

Ce schéma présente l’architecture d’un système biométrique, chaque point correspond à un site plausiblement vulnérable à différentes menaces. Par la suite, il faudra définir la liste des menaces pouvant atteindre le système, les différents risques qu’il encourt et enfin, lier ces menaces aux risques.

# Evènements redoutés

On identifie les évènements redoutés par le système d’authentification biométrique. Voici une liste d’évènements redoutés scuceptibles d’apparaître sur le système :

* Module indisponible
* Vol des données
* Modification des données
* Authentification d’un imposteur
* Non authentification d’un utilisateur
* Système HS

|  |  |  |  |
| --- | --- | --- | --- |
| **Evènements redoutés** | **Besoin de sécurité** | **Impact** | **Gravité** |
| Module indisponible | Disponiblité à court terme | Impossibilité d’accéder à la salle | Limité |
| Vol des données d’authentification | Confidentiel | Modifier les informations essentielles pour permettre à un imposteur de s’authentifier  Divulgation des informations | Importante |
| Altération, Destruction des données d’authentification | Données intègres  Données authentiques | Impossiblité d’accéder à la salle  Imposteur peut y accéder | Limité |
| Authentification d’un imposteur | Confidentiel  Données authentiques | Imposteur peut accéder à la salle | Importante |
| Non authentification d’un utilisateur | Données intègres  Disponibilité à court terme | Impossibilité d’accéder à la salle | Importante |

# Menaces

L’architecture d’un système à base d’authentification biométrique possède différentes cibles d’attaques.

## Menaces possibles

Voici la liste des menaces que le système est susceptible de subir.

* Utilisation illicite du matériel
* Utilisation de modules contrefaits
* Altération du module
* Altération des données
* Traitement illicite des données
* Pannes matérielles
* Dysfonctionnement du matériel
* Espionnage à distance
* Ecoute passive
* Divulgation
* Evènements climatiques
* Sinistres phisiques

## Menaces du système à analyser

Nous allons maitenant lier les menaces aux différents composants du système.

### Le(s) capteur(s)

Dans notre système, il n’y a qu’un seul capteur, celui de la veine de la main lié à la salle.

|  |  |
| --- | --- |
| **Capteurs** | |
| **Menaces** | **Vraisemblance** |
| Capteur des veines de la main | |
| Utilisation de module contrefait | Minimale |
| Pannes matérielles | Minimale |
| Altération du module | Significative |
| Dysfonctionnement du matériel | Minimale |
| Ecoute passive | Minimale |
| Evènements climatiques | Minimale |
| Sinistres physiques | Significative |

### Lien(s) entre capteur(s) et extracteur(s) d’informations

|  |  |
| --- | --- |
| **Extracteurs d’informations** | |
| **Capteurs** | |
| **Menaces** | **Vraisemblance** |
| Extracteur d’informations des veines de la main | |
| Capteur des veines de la main | |
| Ecoute passive | Minimale |
| Espionnage à distance | Minimale |
| Altération des données | Minimale |
| Pannes matérielles | Significative |
| Dysfonctionnement du matériel | Significative |
| Evènement climatique | Minimale |
| Sinistres physiques | Significative |

### L’extracteur(s) d’informations

Un seul extracteur d’information.

|  |  |  |
| --- | --- | --- |
| **Extracteurs d’informations** | | |
| **Menaces** | **Vraisemblance** | |
| Extracteur d’informations des veines de la main | | |
| Utilisation de module contrefait | Minimale |
| Pannes matérielles | Minimale |
| Altération du module | Minimale |
| Dysfonctionnement du matériel | Minimale |
| Ecoute passive | Minimale |
| Evènements climatiques | Minimale |
| Sinistres physiques | Significative |
| Utilisation de module contrefait | Minimale | |

### Lien(s) entre l’extracteur(s) et le module(s) de calcul

|  |  |
| --- | --- |
| **Modules de calcul** | |
| **Extracteurs d’informations** | |
| **Menaces** | **Vraisemblance** |
| Modules de calcul | |
| Extracteur d’informations des veines de la main | |
| Espionnage à distance | Minimale |
| Altération des données | Minimale |
| Pannes matérielles | Significative |
| Dysfonctionnement du matériel | Significative |
| Evènement climatique | Minimale |
| Sinistres physiques | Significative |
| Ecoute passive | Minimale |

### Le(s) module(s) de calcul

Un seul module de calcul.

|  |  |  |
| --- | --- | --- |
| **Modules de calcul** | | |
| **Menaces** | **Vraisemblance** | |
| Module de calcul | | |
| Utilisation de module contrefait | Minimale |
| Pannes matérielles | Minimale |
| Altération du module | Minimale |
| Dysfonctionnement du matériel | Minimale |
| Ecoute passive | Minimale |
| Evènements climatiques | Minimale |
| Sinistres physiques | Significative |
| Utilisation de module contrefait | Minimale | |

### La(es) base(s) de données

Une seule base de données.

|  |  |
| --- | --- |
| **Bases de données** | |
| **Menaces** | **Vraisemblance** |
| Base de données | |
| Pannes matérielles | Minimale | |
| Altération des données | Significative | |
| Dysfonctionnement du matériel | Minimale | |
| Evènements climatiques | Minimale | |
| Sinistres physiques | Significative | |
| Divulgation | Significative | | |

### Lien(s) entre la(es) base(s) de données et le(s) module(s) de calcul

Les liens entre les bases de données et les modules de décisions peuvent être soumis à différentes menaces. Il est possible de lier le même module de calcul à plusieurs bases de données (comme pour le « Module de calcul 1 »).

|  |  |
| --- | --- |
| **Bases de données** | |
| **Modules de calcul** | |
| **Menaces** | **Vraisemblance** |
| Base de donnée | |
| Module de calcul | |
| Espionnage à distance | Minimale |
| Altération des données | Minimale |
| Pannes matérielles | Significative |
| Dysfonctionnement du matériel | Significative |
| Evènement climatique | Minimale |
| Sinistres physiques | Significative |
| Ecoute passive | Minimale |

### Le(s) module(s) de décision

Un seul module de décision.

|  |  |  |  |
| --- | --- | --- | --- |
| **Modules de décision** | | | |
| **Menaces** | **Vraisemblance** | | **Gravité** |
| Module de décision | | | |
| Pannes matérielles | | Minimale | |
| Altération des données | | Significative | |
| Dysfonctionnement du matériel | | Minimale | |
| Evènements climatiques | | Minimale | |
| Sinistres physiques | | Significative | |

# Croisement des évènements redoutés et des scénarios de menaces

* Module indisponible
  + Destruction du module (capteur, module de décision, de calcul, base de données, extracteur)
  + Denis de service
  + Pannes matérielles
  + Sinistres physiques
  + Evènements climatiques
* Vol des données
  + Modification d’un module
  + Ecoute passive
  + Espionnage
  + Utilisation d’un faux module
* Modification des données
  + Modification d’un module
  + Altération des données dans la base de données
  + Disfonctionnement du matériel
  + Utilisation d’un faux module
* Authentification d’un imposteur
  + Disfonctionnement du matériel
  + Modification d’un module
  + Altération des données
  + Ecoute passive
  + Espionnage
  + Utilisation d’un faux module
* Non authentification d’un utilisateur
  + Utilisation d’un faux module
  + Disfonctionnement du matériel
  + Altération des données
* Système HS
  + Destruction d’un module
  + Pannes matérielles
  + Sinistres physiques
  + Evènements climatiques

# Contre-mesures

Un nombre important de contre-mesures génériques sont disponibles au sein de la Section 5 de EBIOS : « *Outillage pour le traitement des risques SSI* ».

Il va maintenant falloir lier ces contre-mesures aux risques et menaces précédemment sélectionnés.

|  |  |
| --- | --- |
| **Risques** | **Contre-mesures** |
| Module indisponible | Vérifier l’accès à la salle contenant les différents modules, de plus, il pourrait être interessant de séparer ces modules afin qu’il ne soit pas touts accessible en même temps  Prévoir des lieux de backup (pour la base de donnée) situés dans des zones géographiques différentes et éloignées  Système anti-incendie  Vérifier le matériel fréquemment |
| Vol des données | Les liens entre les modules sont considérés comme sûr (dans murs…). Il faut donc sécuriser l’accès aux modules ainsi qu’à la base de données. Définir des catégories de personnes pouvant y avoir accès. Définir des protocoles de transfert criptés. |
| Modification des données | Vérifier l’intégrité des messages  Vérifier la véracité et le fonctionnement des modules |
| Authentification d’un imposteur | Vérifier l’intégrité des messages  Vérifier la véracité et le fonctionnement des modules |
| Non authentification d’un utilisateur | Vérifier l’intégrité des messages  Vérifier la véracité et le fonctionnement des modules  Vérifier l’état de fonctionnement des modules |
| Système HS | Vérifier l’état de fonctionnement des modules  Prévoir sécurité anti-incendie et autre évènements naturels. |

# Identification des objectifs de sécurité

On doit s’assurer que seules les personnes autorisées peuvent accéder à la salle et donc aux informations confidentielles. Il faut aussi vérifier que les données d’authentification ne sont pas modifiées et/ou divulguées.

# Conclusion

Le système pourrait être plus sécurisé. En effet, pour le moment tout se base sur la “puissance” des différents modules et réseaux (modèle du capteur, HSMs, cables au sein des murs). Cependant, tous sont situés dans un même batîment, qui plus est, dans la même salle. Une personne ayant accès à cette salle peut modifier le fonctionnement du système. De plus, il n’y a aucun système de secours, si une dégradation naturelle ou criminelle est effectuée sur la base de données, celle-ci ne pourra être récupérée.