

**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 la sécurité d’un système d’authentification par la frappe au clavier**

**Olivier Brizai / Maxime Thoraval**

Table des matières

[1) Introduction 3](#_Toc285122370)

[2) Présentation du contexte de mise en place du système d'authentification 3](#_Toc285122371)

[3) Présentation générale du système 3](#_Toc285122372)

[a) Structure informatique 3](#_Toc285122373)

[i. Les domaines 3](#_Toc285122374)

[ii. Les modules 4](#_Toc285122375)

[iii. Les architectures génériques 4](#_Toc285122376)

[b) Utilisateurs 10](#_Toc285122377)

[4) Expression des besoins de sécurité 10](#_Toc285122378)

[a) Choix des critères de sécurité 10](#_Toc285122379)

[b) Détermination de l'échelle des besoins 12](#_Toc285122380)

[5) Vulnérabilités du système 14](#_Toc285122381)

[6) Les évènements redoutés 15](#_Toc285122382)

[7) Les scénarios de menaces 15](#_Toc285122383)

[a) Scénarios de menaces possibles 15](#_Toc285122384)

[b) Menaces du système à analyser 15](#_Toc285122385)

[i. Le(s) capteur(s) 15](#_Toc285122386)

[ii. Lien(s) entre capteur(s) et extracteur(s) d’informations 16](#_Toc285122387)

[iii. L’extracteur(s) d’informations 16](#_Toc285122388)

[iv. Lien(s) entre l’extracteur(s) et le module(s) de calcul 17](#_Toc285122389)

[v. Le(s) module(s) de calcul 17](#_Toc285122390)

[vi. La(es) base(s) de données 17](#_Toc285122391)

[vii. Lien(s) entre la(es) base(s) de données et le(s) module(s) de calcul 18](#_Toc285122392)

[viii. Le(s) module(s) de décision 18](#_Toc285122393)

[8) Croisement des évènements redoutés et des scénarios de menaces 19](#_Toc285122394)

[9) Contres-mesures 19](#_Toc285122395)

[10) Identification des objectifs de sécurité 19](#_Toc285122396)

[11) Conclusion 19](#_Toc285122397)

# Introduction

Ce document propose une étude d’un système utilisant des données comportementales pour l’autehntification, plus précisément la frappe au clavier.

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

Une école d’Ingénieur de Normandie, fière de son nouveau système d’authentification au clavier, souhaite le déployer auprès de ses étudiants. L’objectif est de ne plus faire retenir de mot de passe aux étudiants pour leur compte informatique, mais de les authentifier grâce à leur login et leur frappe au clavier.

# Présentation générale du système

Voici la structure proposée pour mettre en place ce système

## Structure informatique

L'étude doit mettre en évidence les différents composants permettant l'authentification des utilisateurs. Nous proposons ici une liste générique de ces composants et des architectures permettant de lier ces composants entre eux. Reste à l'utilisateur de la méthodologie de décrire précisément l'architecture de son système et les modules qui la compose.

### Les domaines

On définit tout d'abord 3 grands domaines :

* Le système centrale d'identification : Le système informatique centrale de l’école, qui gère habituellement les comptes des étudiants.
* Les points d'acquisition : Un point d’acquisition est ici n’importe quel ordinateur, où système informatique muni d’un clavier.
* Le domaine de l'utilisateur : Il s’agit de la donnée comportementale de l’utilisateur à savoir sa façon de frapper au clavier et son login.

Bien entendu ces différents domaines doivent communiquer entre eux : L'utilisateur doit avoir accès à un point d'accès pour transférer ces informations au système d'acquisition. Le système d'acquisition doit quand à lui être en lien avec le système centrale.

### Les modules

1– Les capteurs

Le capteur sera ici le clavier de l’ordinateur.

2 – La base de données

La base de données est située sur le système centrale de gestion des comptes de l’école.

4 – L'extracteur des données

L’extracteur des données est situé dans le système centrae.

5 – Un module de calcul

Le module de calcul est situé dans le système centrale.

6 - Module de prise de décision

La prise de décision est également faite par le système centrale.

### Les architectures génériques

**Modèle avec base de données et calculs dans le système centrale. Capteur coté acquéreur.**

Il s’agit du modèle utilisé par l’école. Les éléments qui composent cette architecture ont été définis dans la partie précédente.



## Utilisateurs

Un utilisateur du système est un étudiant de l’école qui souhaite développer cette solution.

# Expression des besoins de sécurité

## Choix des critères de sécurité

Le choix des critères de sécurité est essentiel pour évaluer les risques auxquels est soumis le système d'authentification.

Dans le cadre particulier qui est le notre, nous proposons la liste ce critères génériques suivante :

|  |  |
| --- | --- |
| **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

Les biens essentiels : les procédures de la cinématique d’authentification

On définit dans le tableau ci-dessous les procédures essentielles pour l’authentification comportementale par frappe au clavier :

|  |  |  |
| --- | --- | --- |
| **Processus généraux** | **Processus essentiels** | **Informations essentielles concernées** |
| **Capture des données d’authentification** | | |
| Authentification | Frappe au clavier  Entrée du login | Login  Données comportementales sur la frappe |
| **Extraction de l’information comportementale** | | |
| Traitement de l’acquision | Traitement de la frappe au clavier | Les données transmises par le clavier |
| Transmission du poste d’aquisition vers le système centrale | Transférer les données du poste d’acquisition vers le système centrale sur le réseau | Login, frappe au clavier |
| **Module de cacul et décision** | | |
| Vérification authentification | Verification frappe au clavier associée au login | Login, frappe au clavier |
| Prise de décision | Prise de décision | Résultats du matching par le module de calcul |
| **Retour de la demande d’authentification** | | |
| Réponse à la demane d’authentification | Transfert de la réponse sur le réseau  Gestion de la réponse sur la machine cliente |  |

**Liens entre biens essentiels et biens supports**

On présente ici le lien entre les biens essentiels et les biens supports.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Biens supports | Biens essentiels | Entrée du login (frappe au clavier) | Transférer les données | Traitement de la frappe au clavier | Verification frappe au clavier associée au login | Prise de décision | Transfert de la réponse sur le réseau | Gestion de la réponse sur la machine cliente |
| Domaine utilisateur | | | | | | | | |
| Données comportementales | | X |  |  |  |  |  |  |
| Point d’acquisition | | | | | | | | |
| Clavier (capteur) | | X |  |  |  |  |  |  |
| Ordinateur | | X |  |  |  |  |  | X |
| Extracteur des données | |  |  | X |  |  |  |  |
| Système centrale | | | | | | | | |
| Module de calcul | |  |  |  | X |  |  |  |
| Base de données | |  |  |  | X |  |  |  |
| Module de prise de décision | |  |  |  |  | X |  |  |
| Les réseaux | | | | | | | | |
| Le réseau entre l’utilisateur et le système centrale | |  | X |  |  |  | X |  |

# Vulnérabilités du système

Ce schéma présente l’architecture d’un système biométrique, chaque point correspond à un site plausiblement vulnérable à différentes menaces.

# Les évènements redoutés

On identifie les évènements redoutés par le système de frappe au clavier. Voici une liste d’évènements redoutés scuceptibles d’apparaître sur le système ;

|  |  |  |  |
| --- | --- | --- | --- |
| **Evènements redoutés** | **Besoin de sécurité** | **Impact** | **Gravité** |
| Entrée du login (frappe au clavier) | | | |
| Clavier indisponible | Disponibilité | Deni de service | Limité |
| Ordinateur indisponible | Disponibilité | Deni de service | Limité |
| Données utililisteur récupérées | Confidentialité | Vol de compte | Importante |
| Transférer les données vers le serveur centrale | | | |
| Ecoute des données transmises | Confidentialité | Vol de compte | Importante |
| Altération des données transmises | Intégrité | Deni de service | Limité |
| Surcharge réseau | Disponibilité | Deni de service | Importante |
| Traitement de la frappe au clavier | | | |
| Module extraction indisponible | Disponibilité | Deni de service | Limité |
| Verification frappe au clavier associée au login | | | |
| Base de données altérée | Intégrité, Disponibilité |  | Critique |
| Intrusion base de données | Confidentialite |  | Critique |
| Prise de décision | | | |
| Usurpation d’identité | Authenticité | Vol de compte | Importante |
| Code du module du module de prise de décision modifié | Autehnticité | Vol de compte | Importante |
| Rejet d’un utilisateur | Auhenticité | Deni de service | Importante |
| Transfert de la réponse vers le client | | | |
| Ecoute des données transmises | Confidentialité | -- | Négligeable |
| Altération des données transmises | Intégrité | Deni de service | Limité |
| Surcharge réseau | Disponibilité | Deni de service | Importante |

# Les scénarios de menaces

L’architecture d’un système à base d’authentification biométrique possède différentes cibles d’attaques. Voici les scénarios de meance pour chaque partie du système étudié.

### Le(s) capteur(s)

On étudie ici les scénario sur l’ensemble clavier + ordinateur associé.

|  |  |
| --- | --- |
| **Capteurs** | |
| **Scénarios de Menaces** | **Vraisemblance** |
| Ensemble clavier ordinateur | |
| Récupération login et frappe au clavier (ex : vidéo) | Forte |
| Virus pour récupérer les données (ex : keylogger) | Forte |
| Destruction physique du matériel (ex : attentat) | Minimale |
| Destruction logicielle du matériel (ex virus) | Minimale |

### Lien(s) entre Le domaine d’acquisition et le système central

Attaque sur le réseau entre l’ordinateur et l’extracteur de données :

|  |  |
| --- | --- |
| **Extracteurs d’informations** | |
| **Capteurs** | |
| **Scénarios de Menaces** | **Vraisemblance** |
| Exctrateur des informations comportementales | |
| Clavier et ordinateur | |
| Man In the Middle | Limité |

### L’extracteur(s) d’informations

Les extracteurs d’informations peuvent être soumis à des menaces, elles doivent être définis aussi.

|  |  |
| --- | --- |
| **Extracteurs d’informations** | |
| **Scénarios de Menaces** | **Vraisemblance** |
| Extracteur d’informations 1 | |
| Destruction (ex : ev. Climatique) | Negligeable |

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

Chaque module de calcul peut être soumis à des attaques.

|  |  |
| --- | --- |
| **Modules de calcul** | |
| **Scénarios de Menaces** | **Vraisemblance** |
| Module de calcul 1 | |
| Destruction (ex : ev. Climatique) | Négligeable |
| Altération du code | Négligeable |

### La(es) base(s) de données

Les bases de données aussi sont cibles de nombreuses attaques, nous les définissons dans un tableau.

|  |  |
| --- | --- |
| **Bases de données** | |
| **Scénarios de Menaces** | **Vraisemblance** |
| Base de données 1 | |
| Intrusion BDD | Négligeable |
| Altération BDD | Négligeable |

### Le(s) module(s) de décision

Un module de décision peut subir différentes attaques à définir dans un tableau.

|  |  |
| --- | --- |
| **Modules de décision** | |
| **Scénarios de Menaces** | **Vraisemblance** |
| Module de décision 1 | |
| Destruction | Négligeable |
| Modification code | Négligeable |

# Croisement des évènements redoutés et des scénarios de menaces

On constate le domaine du système qui est le plus soumis à des attaques à la fois de gravité élevées et de vraissemblance élevé est le domaine acquisition des données comportementales.

En effet on considère que le système central de traitement et de conservation des données est suffisamment sécurisé par les administrateurs du système. Il reste notamment important de conserver des serveurs de secours du système en des sites différents. En cas de déstruction physique, même si la Normandie n’est pas connue pour ses tremblements de terres.

Le domaine d’acquisition est sensible à la récupération des données des utilisateurs. Des virus installés sur les ordinateur, ou du matériel vidéo pour filmer l’enrôlement porteur sont possibles.

# Contres-mesures

Voici des contres-mesures applicables pour les risques identifiés

|  |  |
| --- | --- |
| **Risques** | |
| **Menaces** | **Contre-mesures** |
| Vol des données coté acquisition | |
| Keylogger | Prévention sur les risques des virus aux utilisateurs |
| Destruction du système central | |
| Risque natuel | Mener une étude précise sur les risques natuels dans la région |
| Menace terroriste | Le site est-il potentiellement une menace terroriste (étude à mener) |

# Identification des objectifs de sécurité

Le principal objetcif de sécurité est donc coté utilisateur. Les utilisateurs doivent être prudents dans leur utilisation des ordinateurs au risque de se faire voler leurs données comportementales lors de la frappe au clavier par des malwares.s

# Conclusion

Si modèle comportementale de la frappe au clavier assure suffisamment l’authenticité d’un utilisateur, il pourrait-être intéressant de développer ce système. Reste à réflechir au login à utiliser qui doit-être suffisamment grand pour permettre une authentification comportementale au clavier.