**LOG430 – Architecture logicielle**

Scénarios de qualité, tactiques et justifications des attributs produits par les équipes en classe

[Proposition](#_1fob9te)

[Sécurité – Justification (en classe)](#_3znysh7)

[Un individu ayant subtilisé la carte bancaire d’un client et connaissant le NIP effectue un retrait de plus de 200$.](#_tyjcwt)

[Un bidouilleur accède à la connexion du guichet pour s’immiscer dans le réseau bancaire et mettre la main sur les renseignements des clients de la banque.](#_1t3h5sf)

[Sécurité – Tactiques pour le scénario 1](#_17dp8vu)

[Sécurité – Tactiques pour le scénario 2](#_3rdcrjn)

[Sécurité – Vue architecturale](#_lnxbz9)

[Diagramme](#_35nkun2)

[Éléments du diagramme](#_2jxsxqh)

[Relation entre éléments et tactiques](#_3j2qqm3)

[Maintain audit trail](#_1y810tw)

[Inform actors](#_4i7ojhp)

[Relation entre tactique et scénarios](#_1ci93xb)

[Scénario 1](#_3whwml4)

[Authenticate actors](#_2bn6wsx)

[Maintain audit trail](#_qsh70q)

[Scénario 2](#_3as4poj)

[Proposition](#_1pxezwc)

[Des opérations ont été effectuées avec une carte volée et le propriétaire désire être remboursé.](#_49x2ik5)

[Tentative de connexion à partir de deux endroits éloignés dans un laps de temps trop court](#_ihv636)

[Tactique - Scénario 1](#_32hioqz)

[Tactique - Scénario 2](#_1hmsyys)

[Vue architecturale](#_vx1227)

[Proposition](#_3fwokq0)

[Sécurité - Justification](#_1v1yuxt)

[Un individu cherche à se connecter à un compte d’un autre client en faisant plusieurs tentatives.](#_4f1mdlm)

[Un utilisateur malveillant veut lire les données envoyées au serveur.](#_2u6wntf)

[Sécurité – Tactique 1](#_3h992ba31vdm)

[Sécurité – Tactique 2](#_mx0ssza3evom)

[Sécurité – Vue Architecturale](#_5uish1rgznxg)

[Description du diagramme](#_3tbugp1)

[Table de description des éléments des diagramme](#_28h4qwu)

[Proposition](#_nmf14n)

[<Sécurité> – Justification](#_37m2jsg)

[Un utilisateur tente de trouver le NIP d’une carte volée par essai-erreur](#_46r0co2)

[Les informations d’un compte sont chiffrées afin qu’elles ne puissent pas être lus en cas d’attaque](#_3l18frh)

[<Revoke Access> – Tactique 1](#_206ipza)

[<Restrict dependencies> – Vue Architecturale](#_1egqt2p)

[Proposition](#_3ygebqi)

[Un pirate informatique tente de s’infiltrer dans le système informatique bancaire en insérant un périphérique directement dans l’ATM](#_2dlolyb)

[Une carte catégorisée comme étant volée est insérée dans le guichet ATM](#_sqyw64)

[Sécurité – Tactique 1: Détection d’intrusion](#_l74nh2xq9ljw)

[Sécurité – Tactique 2: Informer les acteurs](#_n5st9tua5fpg)

[Sécurité – Vue Architecturale-Scénario 1](#_1rvwp1q)

[Description du diagramme et des relations](#_2r0uhxc)

[Description des éléments du diagramme](#_1664s55)

[Tactiques répond aux scénarios](#_25b2l0r)

[Sécurité – Vue Architecturale-Scénario 2](#_kgcv8k)

[Diagramme et légende](#_34g0dwd)

[Description du diagramme et des relations](#_1jlao46)

[Description des éléments du diagramme](#_43ky6rz)

[Tactiques répond aux scénarios](#_xvir7l)

[Proposition](#_3hv69ve)

[Sécurité – Justification (en classe)](#_cq45dickurqj)

[Un voleur rate 3 fois de suite le nip pour une carte volée.](#_1x0gk37)

[Attaque de type man-in-the-middle](#_4h042r0)

[Sécurité – Tactique 1 (en classe)](#_fjxz6ju41kji)

[Sécurité – Tactique 2 (en classe)](#_dqo1nrmi0y1m)

[Sécurité – Vue Architecturale (à l’extérieur de la classe)](#_k4mcbwro5hgk)

[Tableau des éléments](#_2w5ecyt)

[Description de la relation entre les éléments et les tactiques](#_3vac5uf)

[Proposition](#_2afmg28)

[Vol de carte](#_pkwqa1)

[Acces a un compte bloqué](#_39kk8xu)

[<Attribut-qualité> – Tactique 1 (en classe)](#_s38kl5qbubqb)

[<Attribut-qualité> – Tactique 2 (en classe)](#_qeuzkcvf5z8c)

[Proposition](#_1opuj5n)

[Accès au guichet avec une carte bancaire volée](#_2nusc19)

[Accès non autorisé à un guichet à distance](#_1302m92)

[Tactique - Scénario I](#_8pmyr6t1ycek)

[Tactique - Scénario II](#_1kktt9v0jwh8)

[Vue Architecturale](#_xtcu9np90xjn)

# Proposition

## Sécurité – Justification (en classe)

Un guichet automatique est un outil du domaine bancaire; il constitue donc une cible intéressante pour les pirates informatiques. Les attaques peuvent engendrer des pertes et des conséquences financières pour les intervenants:

Les clients des banques veulent d’abord et avant tout éviter le vol d’argent suite à un accès non autorisé à leur compte; les banques appliquent souvent une politique de non-responsabilité en la matière, mais elle induit certains désagréments (délais et lourdeurs administratives). De plus, il s’agit souvent d’un point d’entrée qui expose le client à d’autres attaques: un compte bancaire contient des informations nominales (nom, adresse) et un relevé de transactions qui peut constituer une atteinte à la vie privée.

L’administration des banques veut réduire les pertes financières reliées au remboursement des clients, selon la politique de non responsabilité, et en frais de récupération (en cas d’attaque à grandes échelles). Il s’agit également de préserver sa réputation pour conserver leurs clients.

| Scénario | Un individu ayant subtilisé la carte bancaire d’un client et connaissant le NIP effectue un retrait de plus de 200$. |
| --- | --- |
| Objectifs d'affaires | Robustesse de l’authentification et de l’autorisation pour empêcher un accès non autorisé;  Autorisation supplémentaire pour toute transaction dépassant un seuil quotidien de 200$;  Détection de transactions illégitimes en moins de 2 jours ouvrables. |
| Attribut de qualité | Sécurité |
| Source | Individu malveillant |
| Stimulus | Accès authentifié et autorisé mais malveillant du compte bancaire d’un client |
| Artéfact | Guichet automatique, données bancaire du compte client |
| Environnement | Opération normale |
| Réponse | Les partis de la transaction sont identifiés avec assurance : la transaction est autorisée à condition que l’individu réponde à une question de sécurité;  Le système enregistre les détails de la transaction |
| Mesure de la réponse | La quantité de données bancaires vulnérables à l’attaque;  Le délai écoulé avant la détection de l’attaque;  Le délai écoulé avant le rétablissement du compte bancaire |
| Questions | 1. Quel seuil est acceptable pour un retrait avant d’ajouter un niveau de sécurité supplémentaire? 2. Comment est-il possible de départager les transactions illégitimes et illégitimes? 3. Serait-ce pertinent d’enregistrer l’endroit où la transaction a été effectuée? |

# 

| Scénario | Un bidouilleur accède à la connexion du guichet pour s’immiscer dans le réseau bancaire et mettre la main sur les renseignements des clients de la banque. |
| --- | --- |
| Objectifs d'affaires | Protéger les données sensibles des clients |
| Attribut de qualité | Sécurité |
| Source | Individu malveillant |
| Stimulus | Tentative non autorisé d’accéder aux données bancaires |
| Artéfact | Services du système bancaire, données confidentielles des clients |
| Environnement | Opération normale du guichet automatique, guichet connecté au réseau |
| Réponse | Les données confidentielles sont protégés d’un accès non autorisé;  La tentative d’accès non autorisé est enregistrée;  Les intervenants concernés sont avertis |
| Mesure de la réponse | La proportion du système qui a été compromise;  Le délai écoulé avant la détection de l’attaque;  Le délai nécessaire avant le rétablissement du système;  La proportion des données bancaires vulnérables à ce type d’attaque |
| Questions |  |

# 

# 

## Sécurité – Tactiques pour le scénario 1

Description: *Authenticate actors*

Justification: Pour les retraits de plus de 200$, un facteur d’authentification supplémentaire est demandé: le client devra répondre à une question de sécurité. Cette méthode n’est pas sans faille: un bidouilleur bien informé sur sa victime pourra répondre correctement à la question. Toutefois, l’application de cette tactique permettra de diminuer les accès illégitimes.

Description: *Maintain audit trail*

Justification: En examinant les journaux d’évènement pour un compte, il sera possible d’identifier les transactions illégitimes et rembourser le client en conséquence. De plus, l’examen automatisée des journaux permettra de détecter certains évènements atypiques, révélateurs d’accès non autorisés : transactions effectuées dans des lieux géographiquement éloignés en très peu de temps, retraits massifs etc. L’application de cette tactique permettra d’empêcher les accès illégitimes consécutifs et donc d’améliorer la sécurité globale.

## Sécurité – Tactiques pour le scénario 2

Description: *Detect intrusion*

Justification: Il serait pertinent de mettre en place un système de surveillance du trafic acheminé vers le serveur bancaire central, de façon à empêcher qu’une intrusion dans un guichet automatique ne compromette pas le serveur central. Pour ce faire, un module d’analyse des paquets de données entrantes pourrait être mis en place sur le serveur central de façon à surveiller le trafic réseau et comparer les signatures de ce dernier à des types de signature malicieuses connues. Ce module agirait donc en tant que mécanisme de détection en cas d’attaque.

Description: *Inform actors*

Justification: Suite à la détection de l’attaque, il serait pertinent d’informer les administrateurs réseau ainsi que l’équipe responsable de la sécurité informatique afin qu’ils puissent prendre des actions nécessaires telles que révoquer l’accès au système central à partir du guichet compromis.

Description: *Revoke access*

Justification: Une fois l’attaque détectée et les intervenants avertis de l’attaque, il serait pertinent de limiter l’accès au réseau bancaire et au serveur central afin de limiter la proportion du système compromise. Pour ce faire, il serait possible de restreindre considérablement l’accès au serveur central lors d’attaques pour tous les utilisateurs du système et ce, tant et aussi longtemps que l’attaque ne soit pas terminée et gérée.

## Sécurité – Vue architecturale

## Diagramme

### 

## 

## Éléments du diagramme

| **Élément** | **Description** |
| --- | --- |
| Guichet automatique | Composant représentant le terminal avec lequel les clients interagissent pour compléter des transaction bancaires avec leur carte bancaire. Chacune des instances de guichet est identique au niveau du fonctionnement. |
| Module d’encryption | Composant internet du guichet responsable de déchiffrer |
| Serveur bancaire | Composant représentant un serveur qui traite des transactions bancaires provenant du répartiteur de charge. Chacune des instances de serveur est identique au point de vue du fonctionnement et leur charge est gérée par le répartiteur. |
| Unité de traitement | Composant interne du serveur responsable de compléter les transactions. Il reçoit ces transactions du gestionnaire de transactions, les complète et renvoie une réponse correspondante au gestionnaire, pour que ce dernier l’achemine vers le guichet en remontant suivant le parcours inverse de la requête. |
| Connecteur réseau HTTP / ISO 8583 | Connecteur établissant un lien entre les clients et les serveurs sur le réseau reliant les guichets automatiques et les serveurs bancaires. Ce connecteur emploie le protocole HTTP pour la connexion réseau et le protocole ISO 8583 pour la forme des messages de transaction bancaire. |
| Système de surveillance | Module indépendant de l’architecture qui surveille les flux de données entre plusieurs guichets et vérifie les flux entre le module de basculement et le serveur principale/redondant. Ne garde aucune données. Sert uniquement pour s’assurer qu’il n’y a pas d’informations qui s'insèrent entre les modules. |
| Module de décryptage | Composant interne aux serveurs responsable de déchiffrer les informations envoyées des guichets. Peut aussi crypter les données dans le sens inverse. |

## 

## Relation entre éléments et tactiques

#### ***Maintain audit trail***

Le système de surveillance permet à l’architecture de rapidement détecter des attaques et prévenir leur propagation aux composantes critiques du système. De manière plus importante, ce module garde un historique des changements importants du système. Si une collection de transactions est illégitime, le système de surveillance saura les étapes à prendre pour remettre le système à son état original.

#### ***Inform actors***

Le système de surveillance garde un oeil sur les transaction et garde un historique, mais si une attaque requiert les administrateurs, ce système saura notifier ces derniers. Le surveillant peut détecter des attaques du guichet jusqu’au serveur. La notification est envoyé et le journal est mis à jour.

## 

## Relation entre tactique et scénarios

## Scénario 1

#### ***Authenticate actors***

Il va de soi qu’il faut s’assurer que l’utilisateur est bien le détenteur du compte avant de pouvoir effectuer un retrait. Cependant une authentification supplémentaire peut être faite lorsque la banque détecte la transaction comme inhabituelle.

#### ***Maintain audit trail***

Le fait d’enregistrer l’historique des transactions permet de retracer le moment et l’endroit des activités inhabituelles afin d’identifier le voleur de façon rétroactive. De plus, en enregistrant les lieux fréquentés il sera possible d’identifier des transactions inhabituelles de façon proactives.

## Scénario 2

***Detect intrusion***

Le but ultime du scénario 2 étant de limiter ou même prévenir les dégats d’éventuelles attaques, il faut d’abord être en mesure de détecter ces attaques.

***Inform actors***

Dans le cas éventuel qu’il s’agisse d’une fausse alerte, il est nécessaire de pouvoir avertir les administrateurs du système afin qu’ils puissent rétablir le système à un fonctionnement normal. Dans le cas d’une situation délicate il peut aussi être utile de s’assurer qu’il est possible d’avertir les personnes responsables.

***Revoke access***

Il est bien beau de pouvoir détecter une attaque, il faut encore être en mesure de la bloquer lorsqu’elle est en cours. C’est justement la finalité de cette tactique.

# Proposition

| Scénario | Des opérations ont été effectuées avec une carte volée et le propriétaire désire être remboursé. |
| --- | --- |
| Objectifs d’affaires | Pouvoir vérifier l’identité de ceux qui ont effectué des opérations avec une carte déclarée volée. Cela permet de savoir si la carte a vraiment été volée avant de rembourser le client. |
| Attribut de qualité | Sécurité |
| Source | Client de la banque. |
| Stimulus | Demande de remboursement suite à un vol de carte. |
| Artéfact | Argent du propriétaire de la carte. |
| Environnement | Opération normale |
| Réponse | L’utilisation de la carte est bloquée. L’identité de la personne qui a effectué des opérations avec la carte déclarée volée est vérifiée et le client est remboursé. |
| Mesure de la réponse | Le temps requis pour vérifier les retraits et rembourser le client. |
| Questions |  |

## 

## 

| Scénario | Tentative de connexion à partir de deux endroits éloignés dans un laps de temps trop court |
| --- | --- |
| Objectifs d’affaires | Sécurité des avoirs de clients et pas de perte d’argent pour la banque. |
| Attribut de qualité | Sécurité |
| Source | Humain |
| Stimulus | Tentative de connexion non autorisée |
| Artéfact | Service d’opérations de la banque |
| Environnement | En ligne, mode d’opération normal |
| Réponse | L’accès au service est refusé |
| Mesure de la réponse | Le nombre d’attaques qui ont été bloquées. |
| Questions | * Quel serait un délai raisonnable entre deux tentatives de connexion distantes pour le même compte? |

## Tactique - Scénario 1

**Description**: Maintain Audit Trail

**Justification**: Le fait de conserver un historique des opérations permet de fournir une preuve qu’une attaque a eu lieu et permet aussi d’améliorer la sécurité pour prévenir des attaques futures.

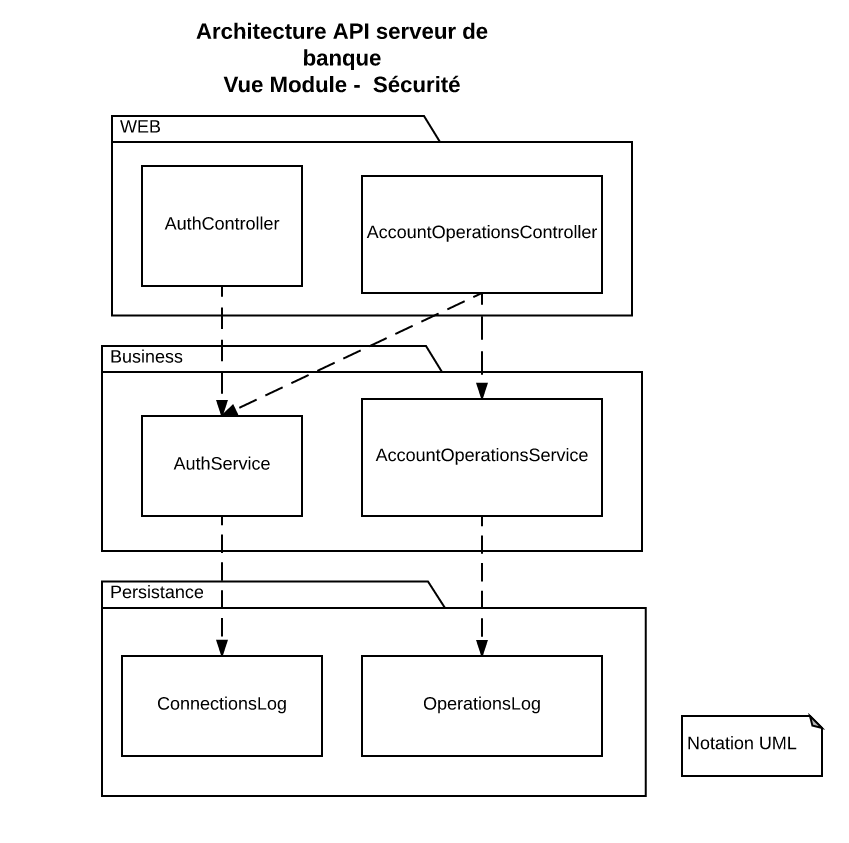
## Tactique - Scénario 2

**Description**: Revoke Access

**Justification**: Si deux connexions sont effectuées pour un même compte dans un laps de temps trop court, la connexion est bloquée. Cela permet de protéger les avoirs du propriétaire du compte.

## 

## Vue architecturale



Description du diagramme et description des relations au scénario

La vue architecturale de type module présente certains composants d’un API web d’une banque utilisé par les guichets afin d’effectuer des opérations sur des comptes. La première tactique *Maintain Audit Trail* est implémentée à l’aide d’un historique des opérations persisté dans une base de données. La deuxième tactique *Revoke Access* est implémentée l’aide d’un service d’authentification qui vérifie l’historique des connexions avant d’autoriser la connexion d’un client.

Description des éléments du diagramme

| AuthController, AccountOperationsController | Points d’entrée de l’API. Un reçoit les requêtes d’authentification et l’autre reçoit les requêtes de transactions. |
| --- | --- |
| AuthService, AccountOperationsService | Services contenant la logique d’affaires concernant l’authentification et les transactions effectuées sur des comptes. |
| ConnectionsLog, OperationsLog | Historiques de connexions et d’opérations utilisés pour détecter les connexions potentiellement frauduleuses et pour garder une trace d’attaques réussies dans le passé. |

# Proposition

## Sécurité - Justification

La sécurité du système est essentiel pour:

* Assurer la consistance des données
* Assurer l’intégralité des données
* Contrôler l'accès aux données
* Protéger les utilisateurs contre des attaques malveillantes

| **Scénario** | Un individu cherche à se connecter à un compte d’un autre client en faisant plusieurs tentatives. |
| --- | --- |
| **Objectifs d'affaires** | Dénier l’accès à l’utilisateur malveillant. |
| **Attribut de qualité** | Sécurité |
| **Source** | Un attaquant humain externe |
| **Stimulus** | Tentative de connexion sur un autre compte. |
| **Artéfact** | Compte d’un autre client |
| **Environnement** | Opérations normales |
| **Réponse** | Le système dénie l’accès au compte utilisateur après 3 tentatives de connexion. |
| **Mesure de la réponse** | L’intégrité des données du compte client. |
| **Questions** | 1. Après combien de tentative est-il nécessaire de bloquer l’utilisateur? |

| **Scénario** | Un utilisateur malveillant veut lire les données envoyées au serveur. |
| --- | --- |
| **Objectifs d'affaires** | Prévenir la lecture des données sensibles à l’utilisateur. |
| **Attribut de qualité** | Sécurité |
| **Source** | Un attaquant humain externe |
| **Stimulus** | Tentative de lecture de données sensibles |
| **Artéfact** | Données sensibles |
| **Environnement** | Environnement spécialisé pour le piratage informatique. |
| **Réponse** | Le système crypte les données envoyées au serveur. |
| **Mesure de la réponse** | L’intégrité des données sensibles. |
| **Questions** | 1. Quel est la technique d’encryption? |

## Sécurité – Tactique 1

Description: Lock computer

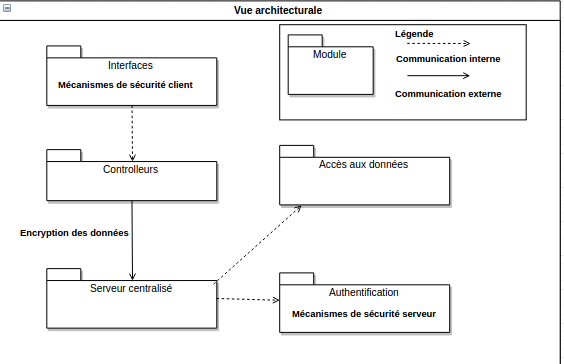
Justification: Lorsqu’un utilisateur essaie trop souvent de se connecter et échoue, alors le système bloquera l’accès à cet utilisateur pour une période définie. Cette méthode permet à des utilisateurs malveillant de faire trop de tentatives

## Sécurité – Tactique 2

Description: Encrypt data

Justification: L’encryption des données permet de passer des données sans que des utilisateurs malveillants puissent les lire. Évidemment, il est possible de décrypter des données, mais cela peut s’avérer extrêmement long, voir impossible, si la méthode de cryptographie est adéquate.

## Sécurité – Vue Architecturale



## Description du diagramme

Les interfaces communiquent avec les contrôleurs, dont eux s’occupent évidemment de faire les interactions avec les serveurs. Les contrôleurs et les interfaces représentent le guichet physique, qui comporte certains mécanismes de sécurité comme la tactique 1, qui est la restriction à un nombre de tentative d’authentification. Puis, selon la tactique 2, les communications entre le guichet et le serveur sont encryptées tel qu’on peut voir entre le module «Controlleurs» et «Serveur centralisé». Cela rend difficile, voir impossible, la lecture des données par un individu malveillant.

## Table de description des éléments des diagramme

Voici un tableau qui décrit les caractéristiques des éléments des vues architecturales présentées à la page précédente.

| **Élément** | **Description** |
| --- | --- |
| Interfaces | Représente l’interface du guichet automatique, qu’il peut verouiller en tout temps sur instruction. |
| Controllers | Cet élément fait partie de chacun des guichets et il interagit avec le serveur. |
| Serveur centralisé | Tous les guichets communiquent avec le serveur pour centralisation des données. |
| Accès aux données | Cet élément concerne la base de données du serveur. |
| Authentification | Cet élément concerne le module d’authentification, qui est évidemment géré par le serveur étant que c’est lui qui a accès aux données. |
| Communication interne | Échange de messages entre les applications locales |
| Communication externe | Échange de messages XML par connexion TCP/IP à des applications distantes |

# Proposition

## <Sécurité> – Justification

Il est important d’avoir une bonne sécurité dans un système afin d’éviter les failles et ainsi éviter d’autres problèmes tel que le vol. Surtout dans un système de guichet bancaire, il est important d’avoir une bonne sécurité parce que c’est un système monétaire. Une faille pourrait signifié un vol d’argent pour les clients et c’est une une priorité pour ce type de système que cela ne se produise pas. Dans cette optique, nous implémentons deux tactiques de sécurité, soit Revoke Access lorsqu’un usager essai de voler un compte en entrant un mot de passe par essai-erreur et Encrypt Data afin de ne pas avoir aucune information en clair dans les serveurs.

# 

| Scénario | Un utilisateur tente de trouver le NIP d’une carte volée par essai-erreur |
| --- | --- |
| Objectifs d'affaires | Éviter les vols aux comptes bancaires des clients |
| Attribut de qualité | Sécurité |
| Source | Utilisateur |
| Stimulus | Saisie de plusieurs NIP erronés |
| Artéfact | Le système d'authentification |
| Environnement | Usage normale |
| Réponse | Bloque le compte |
| Mesure de la réponse | -Bloque le compte après 3 tentatives erronées |
| Questions | 1. Quelle est la procédure de recouvrement du compte ? 2. La carte bancaire est-elle retournée ? |

# 

# 

| Scénario | Les informations d’un compte sont chiffrées afin qu’elles ne puissent pas être lus en cas d’attaque |
| --- | --- |
| Objectifs d'affaires | Éviter les vols aux comptes bancaires des clients |
| Attribut de qualité | Sécurité |
| Source | Utilisateur |
| Stimulus | Essai de voler les informations des clients |
| Artéfact | Les serveurs contenant les informations des clients |
| Environnement | Usage normal |
| Réponse | -Les informations chiffrées |
| Mesure de la réponse | -Aucune information des clients en clair n’est affichée |
| Questions | 1. Est-ce qu’il est possible de déchiffrer les informations ? 2. Quel type de chiffrement est utilisé dans l’industrie? 3. Que ce passe-t-il avec la personne qui tente d’accéder aux informations ? |

## <Revoke Access> – Tactique 1

Description: Un Revoke Access est une tactique permettant de limité les accès à un utilisateur lorsque le système subit une attaque.

Justification: En limitant les accès, on s’assure que si un utilisateur était en train de commettre une tentative de vol, il ne pourra pas la compléter. En effet, si le système détecte qu’il se passe quelque chose d'inhabituel et qu’il est en danger, il empêchera l’utilisateur essayant de se connecter de faire quoi que ce soit. L’utilisateur, étant bloqué par le système, ne peu plus exécuter aucune action et ne peut donc plus effectuer de vols.

# 

## <Restrict dependencies> – Vue Architecturale

Vue-architecturale.png

Description du diagramme:

Les informations des clients sont chiffrées sur les serveurs. Il y a un système de détection des fraudes reliés au lecteur de carte et au clavier qui permet de bloquer l’accès au compte si l’utilisateur entre 3 NIP erronés.

# Proposition

| **Scénario** | Un pirate informatique tente de s’infiltrer dans le système informatique bancaire en insérant un périphérique directement dans l’ATM |
| --- | --- |
| **objectifs d'affaires** | Empêcher le pirate informatique de s’infiltrer dans le système bancaire |
| **Attribut de qualité** | Sécurité |
| **Source** |  |
| **Stimulus** | La crainte qu’un pirate informatique ne modifie ou supprime de l’information |
| **Artéfact** | ATM, serveur de banque, vecteur de communication |
| **Environnement** | Le système est connecté et opérationnel |
| **Réponse** | Dès la détection d’une anomalie, la connexion avec la banque est coupée et une alerte est envoyée au centre de sécurité |
| **Mesure de la réponse** | -Le périphérique est bel et bien détecté  -Une anomalie dans la communication a été détectée  -La communication a été coupée |
| **Questions** | 1. Est-ce qu’un périphérique a été inséré? 2. Y-a-t-il une anomalie au niveau de la communication? 3. Le périphérique est-il d’origine malicieuse? |

| **Scénario** | Une carte catégorisée comme étant volée est insérée dans le guichet ATM |
| --- | --- |
| **objectifs d'affaires** | Appréhender les voleurs de cartes de guichet |
| **Attribut de qualité** | Sécurité |
| **Source** | Une personne avec une carte volée |
| **Stimulus** | Une personne rentre une carte volée dans un guichet ATM |
| **Artéfact** | Le lecteur de carte |
| **Environnement** | Fonctionnement normal du système |
| **Réponse** | Le lecteur de carte détecte que la carte est volée, prend une photo de la personne aillant inséré la carte et avise les opérateurs du système de la situation. La carte reste dans l’ATM et est sécurisé dans un compartiment comme preuve. |
| **Mesure de la réponse** | -La photo permet d’identifier le voleur  -La carte reste bel et bien dans le guichet |
| **Questions** | 1. Est-ce que les opérateurs doivent appeler la police? 2. Quel est la procédure à suivre |

## Sécurité – Tactique 1: Détection d’intrusion

Description: Un système est mis en place pour détecter automatiquement tout ajout de périphérique au guichet ATM, ainsi que toute anomalie dans la communication entre celui-ci et la banque lors de transactions. Le centre de sécurité est alors averti et procède selon la situation.

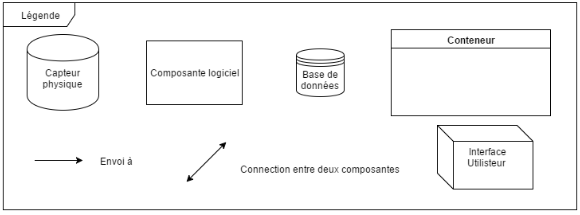
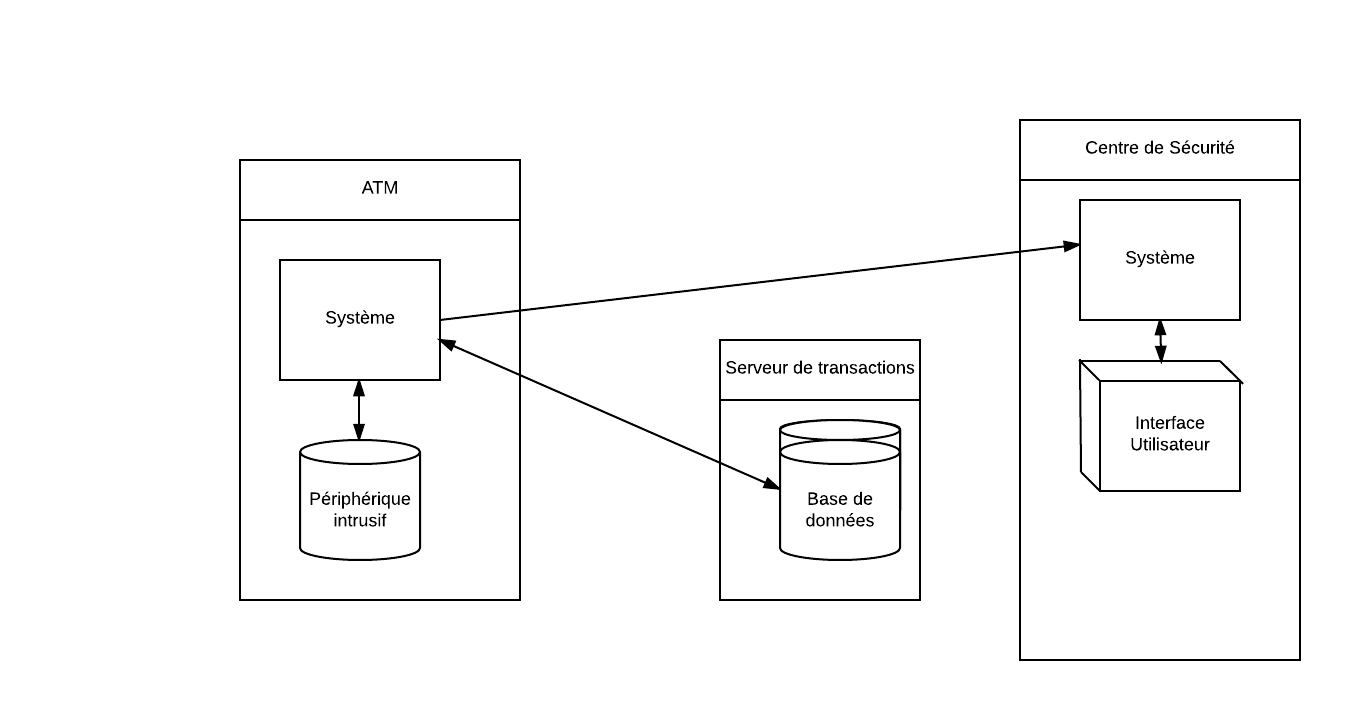
Justification: La tactique ici présentée est pertinente dans cette situation puisqu’elle permet de trouver la source du problème dès son apparition, permettant au centre de sécurité de régler le problème le plus vite possible

## Sécurité – Tactique 2: Informer les acteurs

Description: Lorsque la carte insérée dans le guichet est identifié comme étant volée, le système informe automatiquement les opérateurs du système et prend une photo du suspect pour la police. Les opérateurs informé peuvent ensuite contacter la police avec ces informations pour entamer des procédures judiciaire si nécessaire.

Justification: La meilleure tactique pour répondre à ce scénario serait d’informer les opérateurs du système afin qu’ils prennent les mesures nécessaire pour arrêter le suspect aillant inséré une carte volée. Cette tactique permet donc de remplir cette tâche adéquatement

## Sécurité – Vue Architecturale-Scénario 1



#### Description du diagramme et des relations

Lorsqu’une anomalie est détectée, soit au niveau du périphérique, soit au niveau communication, une alerte est envoyée au centre de sécurité qui, si nécessaire, fait couper la connexion au serveur de transactions.

## Description des éléments du diagramme

| ATM | Représente un appareil physique et son système  embarqué sur le site d’opération (banque) |
| --- | --- |
|  |
| Serveur d’identification | Serveur contenant toutes les informations permettant d’identifier et relier une carte à un compte utilisateur. |
|  |  |
| Nom de l’élément | Description |
|  |  |
| Périphérique Intrusif | Périphérique ajouté à l’ATM par un pirate informatique |
|  |  |
| Système | Système de l’ATM |
|  |  |
| Système (sécurité) | Système utilisé par le centre de sécurité |
|  |  |
| Base de données | Base de données où est contenu toutes les informations reliées aux transactions bancaires |
|  |  |
|  |  |
| Interface utilisateur | Interface utilisateur utilisé par les opérateurs du Centre de sécurité |
|  |
|  |  |
| Tactiques répond aux scénarios | |

La tactique <<Detect Intrusions>> répond au scénario en permettant de détecter une intrusion dès son apparition. Dans ce cas particulier, on parle d’ujn utilisateur insérant un périphérique directement dans l’ATM afin d’atteindre de l’information confidentielle. La détection d’une telle intrusion démontre bien l’utilisation de la tactique concernée.

## Sécurité – Vue Architecturale-Scénario 2

#### Diagramme et légende

Sécurité scénario 2.png

## Description du diagramme et des relations

Lorsque le capteur de carte détecte une carte, celui-ci envoi les paramètres de la carte au système et celui-ci vérifie les paramètres de la carte dans la base de données. Si la carte est indiquée comme une carte volée, la caméra prend une photo qui est ensuite acheminée au système des opérateurs qui est ensuite affiché sur leur poste.

## Description des éléments du diagramme

| ATM | Représente un appareil physique et son système  embarqué sur le site d’opération (banque) |
| --- | --- |
|  |
| Serveur d’identification | Serveur contenant toutes les informations permettant d’identifier et relier une carte à un compte utilisateur. |
|  |  |
| Système centrale d’opération | Représente le système de gestion des ATM. Ce système est géré par les opérateurs du système. |
|  |  |
| Caméra | Capteur permettant de prendre la photo de l’utilisateur si sa carte est jugée volée. |
|  |  |
| Système | Système de l’ATM |
|  |  |
| Capteur de carte | Capteur permettant de recueillir des informations de l’utilisateur à l’aide de sa carte soit son compte utilisateur. |
|  |  |
| Base de données | Base de données où est contenu toutes les informations permettant d’identifier et relier une carte à un compte utilisateur. |
|  |  |
|  |  |
| Interface utilisateur | Interface utilisateur utilisé par les opérateurs du système centrale d’opération |
|  |
| Système des opérateurs | Système des opérateurs du système centrale d’opération |
|  |  |
| Tactiques répond aux scénarios | |

La tactique <<Inform actors>> répond au scénario en permettant d’informer les acteurs faisant la gestion de l’ATM soit les opérateurs du système centrale. En effet, les opérateurs sont informés lorsqu’une attaque survient. Dans le scénario, l’attaque survient sous la forme de la tentative d’utilisation d’une carte volée.

# Proposition

## Sécurité – Justification (en classe)

Permets d’avoir une bonne satisfaction pour les clients. Ils pourront avoir une bonne tranquillité d’esprit. Permets aussi d'éviter les pertes monétaires pour les différentes parties prenantes.

| **Scénario** | Un voleur rate 3 fois de suite le nip pour une carte volée. |
| --- | --- |
| **Objectifs d'affaires** | Satisfaction du client. |
| **Attribut de qualité** | Sécurité |
| **Source** | Voleur |
| **Stimulus** | Plusieurs tentatives d'accès au compte. |
| **Artéfact** | Détails du compte. |
| **Environnement** | Opération normal |
| **Réponse** | Désactivation de la carte pendant 24h.  Notification de l’usager pour changer son nip.  Log de l’infraction. |
| **Mesure de la réponse** | Le temps entre les attaques. |
| **Questions** | 1. Quel est le temps moyen pour entrer son nip ? |

| **Scénario** | Attaque de type man-in-the-middle |
| --- | --- |
| **Objectifs d'affaires** | S’assurer de la satisfaction des clients |
| **Attribut de qualité** | Sécurité |
| **Source** | Personne a l'extérieur de l’organisation |
| **Stimulus** | Tentative de modification des données |
| **Artéfact** | Message entre l’ATM et le serveur |
| **Environnement** | Opération normal |
| **Réponse** | Log des messages |
| **Mesure de la réponse** | Le temps entre les attaques |
| **Questions** | 1. Quel est le temps normal pour la réception/envoi d’un message ? |

## Sécurité – Tactique 1 (en classe)

Description: **Revoke access**

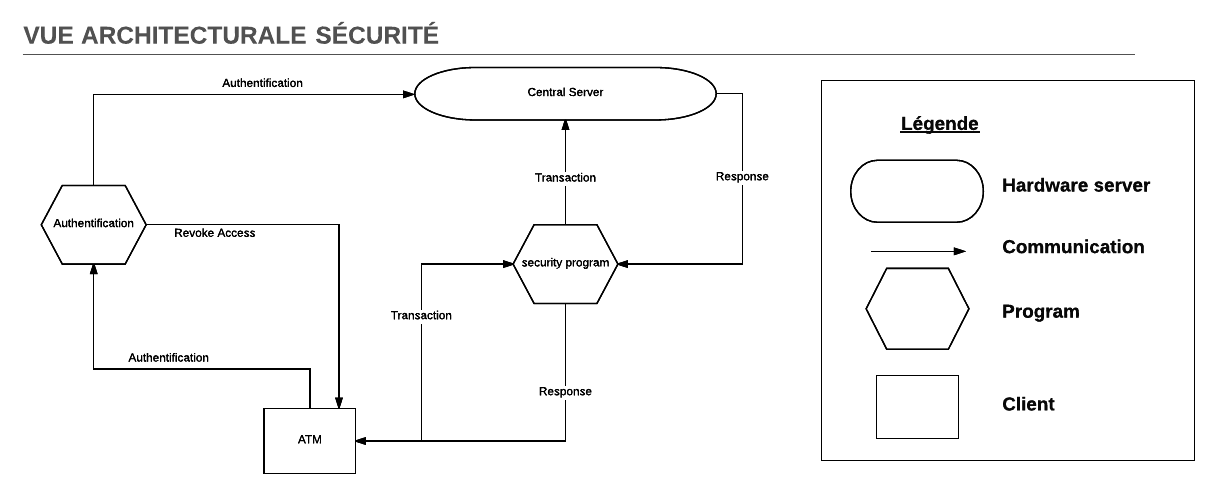
Justification: Pour éviter d’autre accès au système non autoriser, nous révoquons l'accès aux personnes mal intentionné. De cette façon, nous évitons le brute-force des mots de passe pour accéder aux données des comptes.

## Sécurité – Tactique 2 (en classe)

Description: **Detect message delay**

Justification: Pour détecter les attaques de type man-in-the-middle, nous pouvons détecter le temps entre les messages de cette façon nous pouvons voir si les messages ont été intercepter et donc modifier.

## Sécurité – Vue Architecturale (à l’extérieur de la classe)



## Tableau des éléments

| Éléments | Description |
| --- | --- |
| ATM | Le guichet automatique. |
| Central Server | Serveur physique |
| Authentification | Programme d’authentification ayant la responsabilité de détecté si le client s’authentifie correctement. |
| Security program | Programme de sécurité ayant la responsabilité de vérifier si les messages rentrants et sortants du serveur et de l’atm s’ils ne sont pas anormaux. |
| Authentification (ATM vers Auth.) | Flux d’authentification dirigé vers le programme d’authentification |
| Authentification (Auth vers Central Server.) | Flux d’authentification approuvé par le programme d’authentification et envoyé vers le serveur central |
| Repsonse(Security p. vers ATM) | Réponse du serveur qui vient de passer de façon transparente par le programme de sécurité. |
| Repsonse(Central Server vers Security p.) | Réponse du serveur dirigée vers le programme de sécurité. |
| Transactions (Security program vers Central Server) | Transaction dirigée vers le serveur central. |
| Transactions (ATM vers Security program) | Transaction dirigée vers le programme de sécurité. |
| Revoke access | Retire l’accès à l’utilisateur courant de l’ATM. |

## 

## Description de la relation entre les éléments et les tactiques

L’élément “Authentification” a pour responsabilité d’analyser et d’approuver l’authentification ou de retirer les droits de l’utilisateur s’il détecte un comportement douteux lors de multiple essaies d’authenfication de la part de l’utilisateur. De cette façon nous répondons au besoin de la tactique 1.

L’élément “Security Program” a pour responsabilité d’analyser le flux de communication entre le serveur et l’atm en mesurant le temps d’envoi et de réception des messages pour ainsi pouvoir détecter s’il y a des anomalies pour éviter un “man in the middle” ainsi nous appliquons de cette façon la tactique 2.

# Proposition

| **Scénario** | Vol de carte |
| --- | --- |
| **objectifs d'affaires** | Protection du compte du client. |
| **Attribut de qualité** | Sécurité |
| **Source** | Humain |
| **Stimulus** | Le voleur accède le compte avec les informations volées |
| **Artéfact** | Les données du client |
| **Environnement** | Fully operational |
| **Réponse** | Les conditions dans lesquels la transaction à été effectuée |
| **Mesure de la réponse** | Audit des lieux de la transaction.  Nombre de tentatives de nip échoué.  Le montant de la transaction  Le nombre de transactions |
| **Questions** | 1. Combien de tentatives de nip ont été échoué? 2. Le lieux de la transaction est-t-il plausible? 3. Le montant retiré est-il anormal? 4. Le nombre de transactions par minutes est-t-il plausible? |

| **Scénario** | Acces a un compte bloqué |
| --- | --- |
| **Objectifs d'affaires** | Protection du compte du client. |
| **Attribut de qualité** | Sécurité |
| **Source** | Humain |
| **Stimulus** | Tentative d’accès au compte |
| **Artéfact** | Les données du client |
| **Environnement** | Fully operational |
| **Réponse** | Les conditions dans lesquels la transaction à été effectuée |
| **Mesure de la réponse** | Audit des lieux de la transaction. |
| **Questions** |  |

## <Attribut-qualité> – Tactique 1 (en classe)

Description: Lock system

Justification: Barre le système (le compte du client) temporairement pour éviter un vol.

## <Attribut-qualité> – Tactique 2 (en classe)

Description: Lock system

Justification: Le système garde la carte pour éviter un vol étant donné que le compte est bloqué.

# Proposition

| **Scénario** | Accès au guichet avec une carte bancaire volée |
| --- | --- |
| **objectifs d'affaires** | Empêcher des malfrats de pouvoir effectuer des transactions de façon illégale avec les comptes d’autres utilisateurs. |
| **Attribut de qualité** | Sécurité |
| **Source** | Un humain ayant volé la carte bancaire d’une personne. |
| **Stimulus** | Authentification de la carte avec entrée de NIP |
| **Artéfact** | Système de gestion des comptes bancaires |
| **Environnement** | Opération normale |
| **Réponse** | Verrouillage du compte utilisateur compromis et notification des entités concernées (le malfrat, le détenteur de la carte et la banque) de l’événement |
| **Mesure de la réponse** | Temps de récupération d’un compte verrouillé  Nombre de tentatives d’accès avec un NIP invalide avant le verrouillage du compte |
| **Questions** |  |

| **Scénario** | Accès non autorisé à un guichet à distance |
| --- | --- |
| **objectifs d'affaires** | Empêcher un accès réseau non autorisé au guichet automatique |
| **Attribut de qualité** | Sécurité |
| **Source** | Un logiciel ou usager malveillant |
| **Stimulus** | Accès à la caisse |
| **Artéfact** | Système de gestion de la caisse |
| **Environnement** | Opération normale |
| **Réponse** | Le guichet détecte et bloque l’accès non autorisé et notifie le service de sécurité distant |
| **Mesure de la réponse** | Le nombre de tentatives d’accès, la durée de reprise du suite à a une attaque, le nombre de données piratées |
| **Questions** | - Comment exploiter les traces des accès non autorisé pour identifier le fraudeur?  - Quel sera l’impact de des stratégie de sécurité sur la disponibilité? |

## Tactique - Scénario I

**Description**: Lock computer

**Justification**: Cette tactique permet d’empêcher à la personne qui tente d’acquérir le bien d’un autre d’avoir accès au guichet automatique bancaire. Si cette personne continue avec des autres machines, il serait bien aussi d’utiliser la tactique Inform Actors afin de contacter le propriétaire de la carte pour confirmer que c’est lui qui l’utilise ou quelqu’un d’autre.

## Tactique - Scénario II

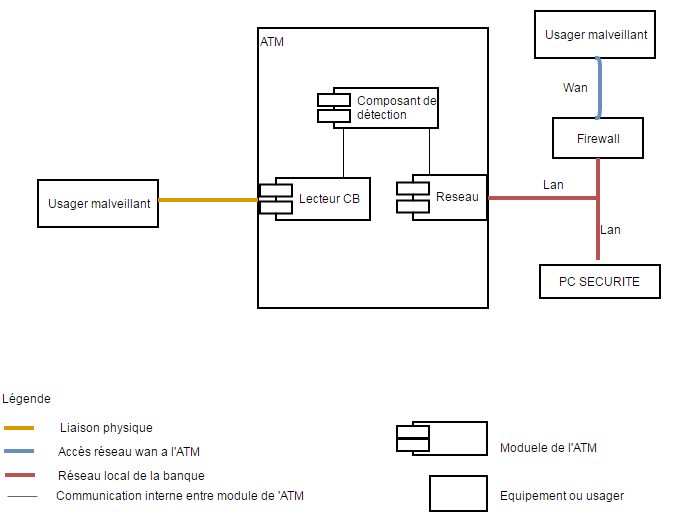
**Description**: Limitation de l’exposition et protection de la communication

* Utilisation de firewall, utilisation de profil mainteneur avec mot de passe crypté
* Utilisation de protocole dédié.
* Mettre en place un composant de log pour stocker les information de communication, l’état courant du guichet.

**Justification**: Un guichet automatique est un équipement du domaine bancaire très exposé aux attaques malveillantes. Il constitue un enjeu économique. Garder le système en sécurité une source de motivation importante pour fidéliser les clients. Cependant, cela demande une application des règle très strict de sécurité. Il importe donc ce mettre un accent sur la prévention et de protection car un guichet attaqué peut provoquer des transactions frauduleuses importante.

## Vue Architecturale

**Diagramme - Scénario I & II**



Ce diagramme représente le système de sécurité de l’ATM permettant la détection des intrus. Il contient les composants qui sont des cible pour les malveillant et qui permet d’empêcher les attaques.

| **Éléments** | **Descriptions** |
| --- | --- |
| **Guichet** | Le guichet automatique |
| **Composant de détection** | Module de détection des attaques malveillantes |
| **Reseau** | Module de communication réseau du guichet automatique |
| **Firewall** | Serveur permettant de faire respecter la politique de sécurité du réseau |
| **Lan** | Réseau local dédié |
| **Wan** | Réseau informatique couvrant une grande zone géographique |
| **Pc sécurité** | Le service de maintenance a distance des guichets |
| **Lecteur CB** | Le lecteur de la carte bancaire |

Pour faire le lien avec les scénarios et le choix des tactiques, le Firewall est utilisé pour empêcher d’avoir accès à distance les guichets. Sinon, il y a le composant de détection qui est présent dans le système en cas que le Firewall n’a pas réussi à protéger. Il représente aussi celui qui va déterminer s’il doit faire un Lock Computer et l’inform Actors quand un malveillant essaye de forcer le NIP d’une carte qu’il a volée.