Scénarios, tactiques et vues architecturales

Sécurité

[**1 Le système doit réagir à quelqu’un tenant d’accéder à un compte avec une carte volée.**](#_gjdgxs) **3**

[1.1 Tactique 1 : Detect Intrusions](#_7sy6e91l7q6w) 3

[1.2 Tactique 2 : Lock Computer](#_1fob9te) 3

[1.3 Tactique 3 : Maintain Audit Trail](#_3znysh7) 3

[1.4 Vue architecturale (à l’extérieur de la classe)](#_tp4fivli0xhy) 3

[1.4.1 Description du diagramme](#_2et92p0) 4

[1.4.2 Description des éléments](#_tyjcwt) 4

[1.5 Relation entre éléments et tactiques](#_3dy6vkm) 4

[1.5.1 Tactique 1 : Detect Intrusions](#_1t3h5sf) 4

[1.5.2 Tactique 2 : Lock Computer](#_4d34og8) 4

[1.5.3 Tactique 3 : Maintain Audit Trail](#_2s8eyo1) 4

[**2 Deux transactions ont été fait à l’intérieur d’un intervalle de temps dont l’emplacement des deux transaction sont trop éloigné pour être effectué.**](#_saaccc1lhq0x) **5**

[2.1 Tactique 1 :Revoke Access](#_aipzj1bb2hu3) 5

[2.2 Tactique 2 : Identify Actors](#_xwwyz3dohzng) 5

[2.3 Tactique 3 : Maintain Audit Trail](#_17dp8vu) 6

[2.4 Diagramme](#_353kzwds8552) 6

[2.4.1 Texte de description du diagramme](#_gfz93fmrhzj5) 7

[2.4.2 Table de description des éléments des diagrammes](#_qq8qi18jnjhn) 8

[2.4.3 Texte décrivant la relation entre les éléments et les tactiques](#_t9i4a2knkscr) 8

[**3 La banque veut qu'un ATM soit bloqué suite à plusieurs tentatives infructueuses d´entrée d´un NIP**](#_eej8xo665lbd) **9**

[3.1 Tactique 1 : React to attacks](#_atw7a7gopal6) 9

[3.2 Vue architecturale (à l’extérieur de la classe)](#_ughag18zyown) 10

[Diagramme](#_gwnyzhslur1) 10

[Légende](#_42jnv9ldfxs) 10

[Texte de description du diagramme  
Le(s) moniteur(s) souscrivent à l'événement AttackEvent de l’ATM. Si une attaque est détecté, l’ATM envoie l'évènement à tous les subscribers et les subscribers ont l’option de bloquer l’ATM.](#_vlfvj7vuv0a2) 11

[3.2.4 Table de description des éléments du diagramme](#_ajwo0dxu6w04) 12

[3.2.5 Texte décrivant la relation entre les éléments et les tactiques](#_knxdw210qh6e) 12

[**4 Restreindre l’accès aux fonctionnalités portées sur un compte bancaire (dépôts, retraits, informations, etc.) seulement à la personne détenant le compte**](#_25jv822mj9xd) **13**

[4.1 Tactique 1 : Authentifier les acteurs (résister aux attaques)](#_r9wrc11fdqls) 13

[4.2 Vue architecturale (à l’extérieur de la classe)](#_5ct41cuj2kvt) 14

[4.2.1 Système d’authentification du GAB](#_3rdcrjn) 14

[4.2.2 Texte de description du diagramme](#_rf5cz6ne2etd) 14

[4.2.3 Table de description des éléments du diagramme](#_3rr775k991b) 14

[4.2.4 Texte décrivant la relation entre les éléments et les tactiques](#_mezjrbizeny8) 15

[**5 Récupérer des arnaques physiques sur les utilisateurs. Un utilisateur forcé à effectuer une transaction devrait pouvoir en aviser la banque discrètement.**](#_k2nluf6co3on) **16**

[5.1 Tactique 1 : Detect Intrusion](#_7vaj308p544u) 16

[5.2 Tactique 2 : Limit Exposure](#_gf1c3zz33z70) 16

[5.3 Tactique 3 : React to Attacks - Inform Actors](#_wlokdb65sg60) 16

[5.4 Vue architecturale (à l’extérieur de la classe)](#_w3i3jxbbox44) 17

[5.4.1 Diagramme](#_26in1rg) 17

[5.4.2 Table de description des éléments du diagramme](#_8fmjjux8x0q9) 17

[5.4.3 Table de description des relations des tactiques entre ces éléments](#_9dso34x8w46r) 18

[5.4.4 Description des relations entre les éléments](#_jpkeblz0k1) 18

[**6 Empêcher l’utilisateur d’accéder à un compte qui n’est pas le sien.**](#_ei60k6vqs81j) **19**

[6.1 Tactique 1 : Lock computer](#_g1cz7pptnq9w) 19

[6.2 Tactique 2 : Maintain audit trail](#_e339chpe6zrp) 19

[6.3 Vue architecturale (à l’extérieur de la classe)](#_jmoq3nm1u1do) 20

[6.3.1 Description](#_zfdd8xrzuxx6) 20

[6.3.2 Relation avec la tactique](#_seehggr87sft) 21

[6.3.3 Composantes](#_2ey3mog1s2dx) 21

[**7 Protéger la connexion entre le guichet et le serveur contre les attaques de type “Man-in-the-middle”.**](#_npztrltyrzse) **22**

[7.1 Détection et 1 récupération](#_5ldj5qii7btk) 22

[7.1.1 Tactique 1 : Verify message integrity](#_ovknoq3kcucc) 22

[7.1.2 Tactique 2 : Encrypt data](#_94yb8t2ul5xt) 23

[7.1.3 Tactique 3 : Revoke access](#_4fypkkyvg8ic) 23

# 

# 

# 1 Le système doit réagir à quelqu’un tenant d’accéder à un compte avec une carte volée.

|  |  |
| --- | --- |
| **objectifs d'affaires** | Les données bancaires doivent être privées. |
| **Source** | utilisateur du système |
| **Stimulus** | tentative non autorisée d'afficher les données d'un autre compte. |
| **Artéfact** | Données des comptes |
| **Environnement** | Système en ligne dans un réseau interne avec la banque. |
| **Réponse** | Les données sont protégées |
| **Mesure de la réponse** | Nombre de connexions illégales bloquées. |
| **Questions** |  |

## **1.1 Tactique 1 : Detect Intrusions**

**Description**: Une tentative de connexion ayant échoué (mauvais NIP) est considérée comme une tentative d'intrusion.

**Justification**: Puisque les données bancaires doivent être protégées contre les intrus, une tentative de connexion consistant d'une carte bancaire et un mauvais mot de passe est considéré comme le pire scénario, c'est-à-dire une tentative d'intrusion sur le compte bancaire d'un autre client.

## **1.2 Tactique 2 : Lock Computer**

**Description**: Un verrouillage du système après un événement déterminé par le système.

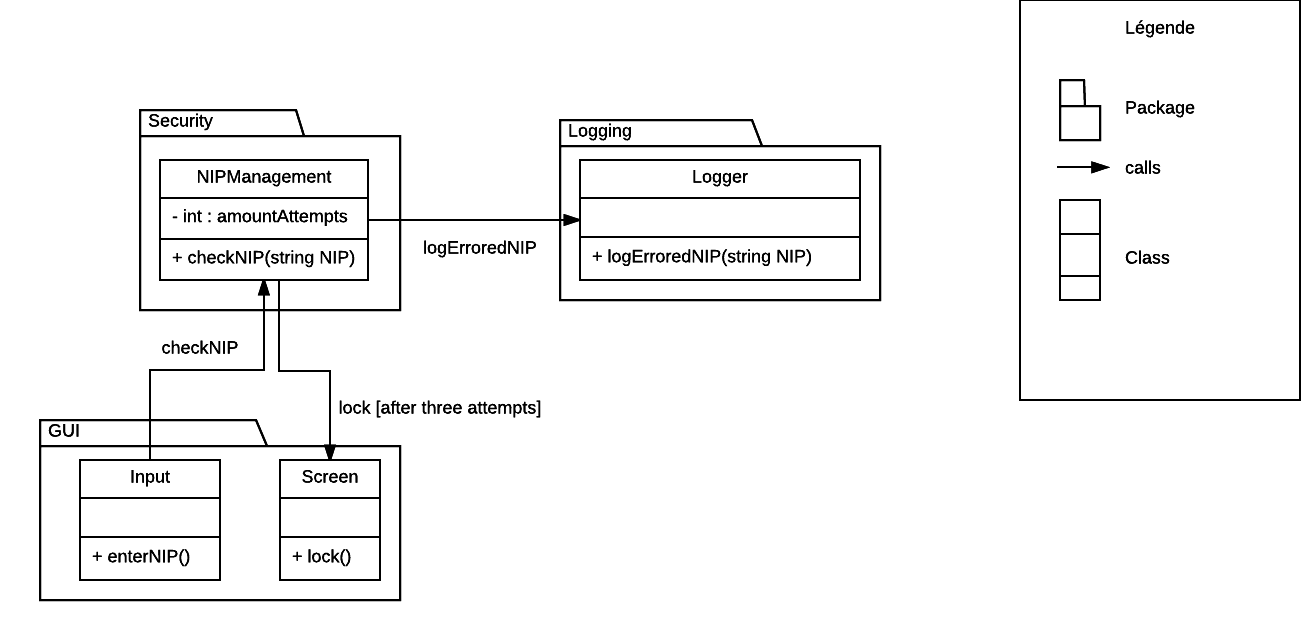
**Justification**: Lorsque le système considère s’être fait attaqué trois fois (soit 3 faux NIPs), il verrouille l’ATM et affiche un message forçant l’utilisateur à aller au comptoir.

## **1.3 Tactique 3 : Maintain Audit Trail**

**Description**: Garder une trace des actions effectuées par les utilisateurs lors de la connexion.

**Justification**: Garder des données de tentatives de connexions permettra de déterminer les tactiques employées par les attaquants.

## **1.4 Vue architecturale (à l’extérieur de la classe)**



### **1.4.1 Description du diagramme**

Le package du GUI reçoit le NIP de l’utilisateur par l’Input. Celui-ci est vérifié par le NIPManagement. Pour chaque tentative erronée, le NIPManagement envoi une requête d’écriture au journal de bord. Après 3 erreurs, le NIPManagement envoi une requête de verrouillage du compte à l’écran.

### **1.4.2 Description des éléments**

**GUI** : Package contenant les composants de l'interface.

**Input** : Classe logiciel comprenant les entrées de l'utilisateur sur le GAB.

**Screen** : Classe logiciel représentant l'écran du GAB.

**Security** : Package contenant les composants de la sécurité.

**NIPManagement** : Classe logiciel représentant la gestion du numéro d’identification personnel.

**Logging** : Package contenant les composants des logs.

**Logger** : Classe logiciel représentant le journal de bord (log).

## 1.5 Relation entre éléments et tactiques

### **1.5.1 Tactique 1 : Detect Intrusions**

Cette tactique est représentée par les packages GUI et Security. L'input du GUI envoie le NIP au NIPManagement qui le vérifie et détecte s’il est bon ou non.

### **1.5.2 Tactique 2 : Lock Computer**

Après que le NIP ait été reconnu comme non valide 3 fois, le NIPManagement envoit une commande pour bloquer l'accès au compte.

### **1.5.3 Tactique 3 : Maintain Audit Trail**

Chaque tentative de connexion est inscrite dans le journal de bord (Logger) pour effectuer des audits si nécessaires.

# 2 Deux transactions ont été fait à l’intérieur d’un intervalle de temps dont l’emplacement des deux transaction sont trop éloigné pour être effectué.

|  |  |
| --- | --- |
| **objectifs d'affaires** | Réduire les coûts des remboursement des transactions frauduleuses annuellement. |
| **Source** | Fraudeur |
| **Stimulus** | ~~Le fraudeur~~ essaye d’effectuer des transactions à un compte auquel il n’est pas autorisé |
| **Artéfact** | Les données du compte client |
| **Environnement** | Le guichet et le système bancaire est en ligne et sont connecté entre eux. |
| **Réponse** | - L’accès au compte est révoqué  - On enregistre toutes les transactions qui sont faites au compte |
| **Mesure de la réponse** | Le coût des remboursement des transactions frauduleuse. |
| **Questions** | 1. Quel est le temps entre les tentative de transactions? 2. Comment le fraudeur a-t-il eu accès à l'information du compte auquel il n’est pas autorisé? 3. À partir de quelle distance peut on considérer que la transaction est frauduleuse |

## 2.1 Tactique 1 :Revoke Access

**Description**: Le système détecte un évènement suspect et empêche/réduit l’accès aux fonctionnalités souhaités.

**Justification**: Avec l’utilisation du Revoke Access, un fraudeur effectuant un évènement suspect pourra être bloqué même si il a les informations de connexion au compte. Permettant ainsi d’améliorer considérablement la sécurité du système.

## 2.2 Tactique 2 : Identify Actors

**Description**: Permet l’utilisation des informations récupérées (Adresse IP, ID ) pour confirmer l’identité du client du compte.

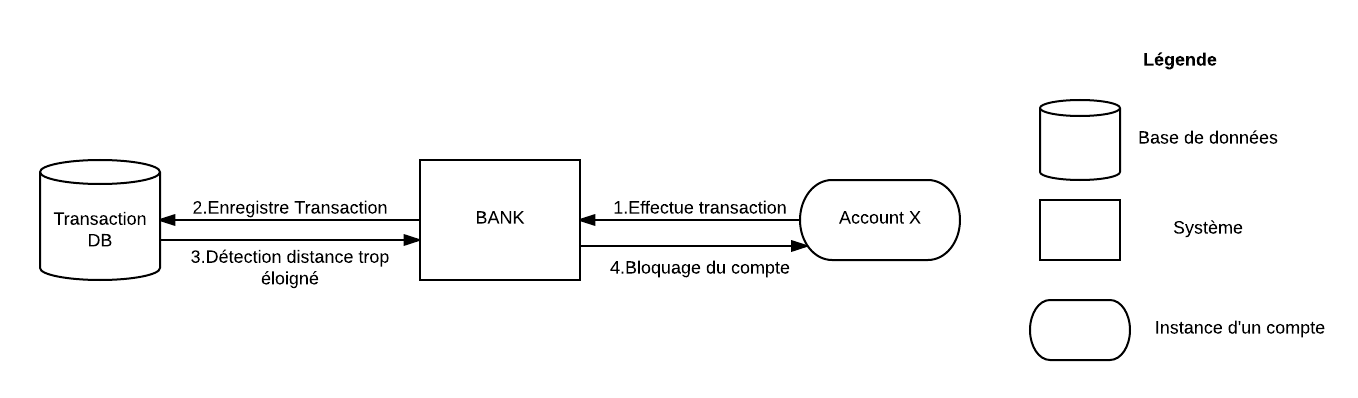
**Justification**: L’ajout de cette tactique permettra au système de vérifier si la demande de transaction a été réalisé par le client du compte. Grâce à la récupération de l’adresse ip, il pourra détecter un adresse ip utilisé pour une première fois étant donc, hautement suspecte.

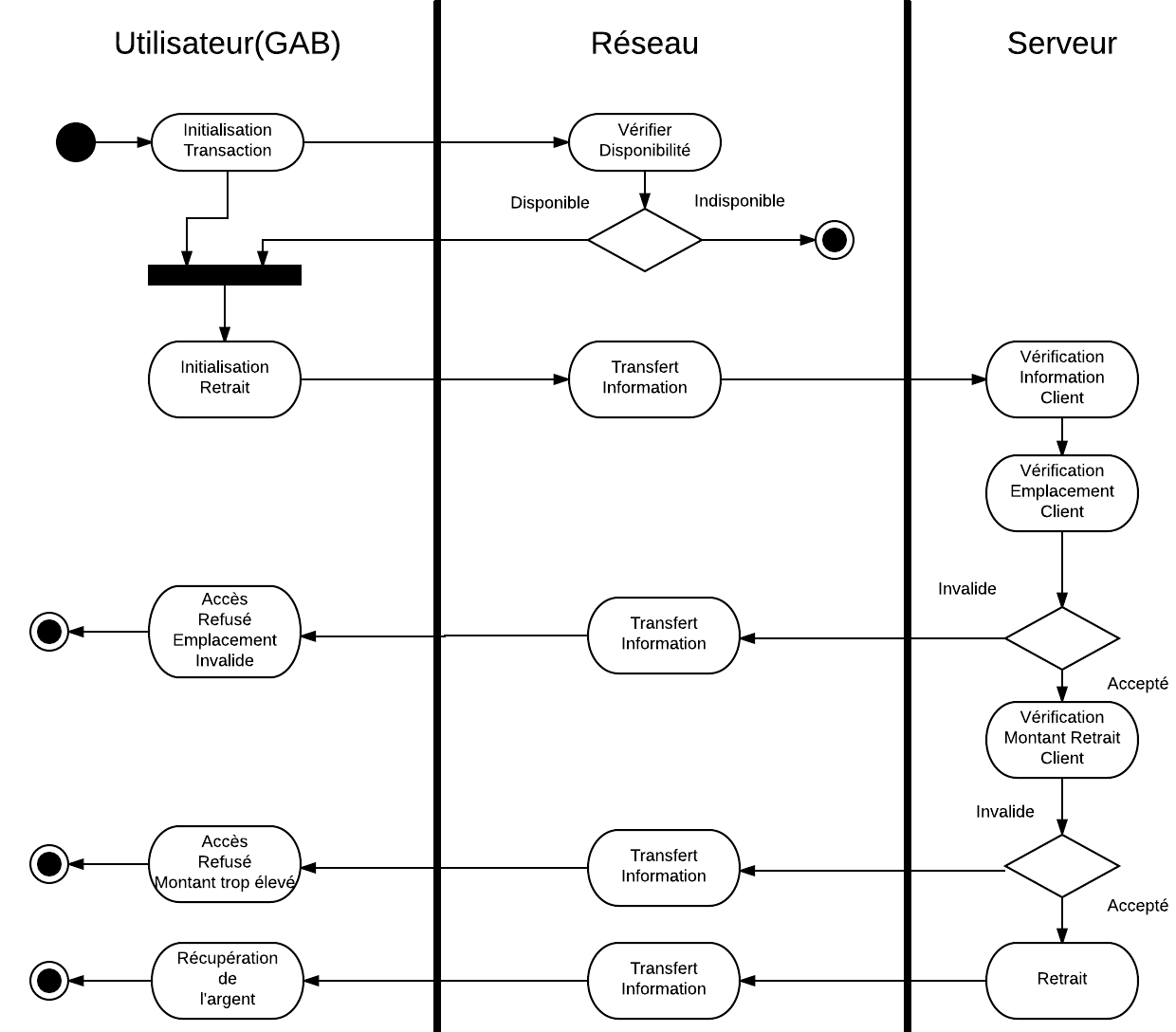
## 2.3 Tactique 3 : Maintain Audit Trail

**Description**: Garde en stock les informations effectuées sur le système permettant ainsi d’identifier une attaque sur le système.

**Justification**: L’utilisation de cette tactique permettra de savoir les actions frauduleuses effectués sur le compte et donc, de permettre d’effectuer les remboursements nécessaires sur le compte client touché.

## 2.4 Diagramme





### 2.4.1 Texte de description du diagramme

Ce diagramme représente comment le système fait pour détecter l’intrusion dans le système. Au début, lorsqu’une personne se connecte à un compte, le guichet va envoyer les informations de la transaction qui a été effectué à la banque qui va ensuite les conserver dans une base de données. Chaque fois qu’il y a une insertion dans la bd, la bd va activer une procédure qui va comparer la transaction avec celles qui ont été fait avant. Elle va regarder l’emplacement, le montant et le temps de la transaction. Si elle détecte une possibilité d’intrusion. Elle va alerter la banque qui va automatiquement bloquer le compte,

Le diagramme d’activité représente une demande typique de retrait d’argent à un compte. Lors de cette transaction, le système vérifiera les informations de connexion du client pour s’assurer que ceux-ci concorde avant l’envoi du retrait. De plus, une vérification de l’emplacement du client via l’adresse IP et son ID sont conforme aux précédentes demandes de retrait. Le système vérifiera que la demande provient d’un emplacement proche des précédentes demandes en plus de prendre en compte le temps. Ainsi, une demande de retrait provenant de plus de 500km (exemple) de la précédente ayant été effectuée il y a deux heures sera automatiquement pris en compte comme étant une action frauduleuse et ne permettra pas le retrait en question. Enfin, une dernière vérification sera fait sur le montant retiré. Une demande de retrait trop élevé en plus d’un emplacement non-habituel sera automatiquement interdite et bloquera le compte.

### 2.4.2 Table de description des éléments des diagrammes

|  |  |
| --- | --- |
| Élément | Description |
| Transaction DB | Base de données qui va conserver en mémoires toutes les transactions qui ont été effectués pour un compte avec l’emplacement de la transaction les informations du compte... |
| Bank/Serveur | Le système externe de la banque. |
| Account | un compte qui va effectuer une transaction à une machine X |
| Utilisateur(GAB) | Représentation de l’utilisateur effectuant une demande. |
| Réseau | Représentation du réseau ainsi que de la communication TCP/IP utilisé pour transférer l’information entre le guichet et le serveur. |

### 2.4.3 Texte décrivant la relation entre les éléments et les tactiques

La tactique revoke access est utilisé par le fait que dès que la base de donnée active la procédure que 2 transactions ont été effectués dans des endroits très éloignés en peu de temps. Cette procédure va envoyer un message au système de la banque que le compte x a probablement été piraté par un fraudeur. Donc, le compte sera bloqué.  
  
La tactique identify actor et maintain audit trail sont représentés par le fait que toutes les informations des transactions qui ont été effectué sont conservé dans la base de données de la banque, De plus l’adresse ip et les informations du compte seront récupéré lorsque la transaction sera effectués

# 3 La banque veut qu'un ATM soit bloqué suite à plusieurs tentatives infructueuses d´entrée d´un NIP

|  |  |
| --- | --- |
| **objectifs d'affaires** | La banque veut qu'un ATM soit bloqué suite à plusieurs tentatives infructueuses d´entrée d´un NIP. |
| **Source** | Une personne externe entre plusieurs NIP erronés. |
| **Stimulus** | Tentative d'accès non-autorisé au service. |
| **Artéfact** | Les services de l´ATM |
| **Environnement** | Système opérationnel |
| **Réponse** | Notification d’une entité (agent) et blocage de l´ATM. |
| **Mesure de la réponse** | Le temps entre le signalement de l'attaque et l'action du blocage de l´ATM. |
| **Questions** | 1. Combien de NIP invalides pour être considéré comme une attaque? 2. Combien de temps entre les entrées des NIP sur la machine pour être considéré comme une attaque? |

## 3.1 Tactique 1 : React to attacks

**Description**: Le système bloque l’accès et informe une entité qu’une attaque pourrait être en cours.

**Justification**: Le système informe un opérateur et bloque l’ATM pour éviter les risques que l’attaque soit un succès. L’opérateur pourra aller voir la personne et débloquer l’ATM après vérification de l’identité de la personne.

## 3.2 Vue architecturale (à l’extérieur de la classe)

### Diagramme

### Légende

|  |  |
| --- | --- |
|  | **ATM** |
|  | **Moniteur des agents** |

### Texte de description du diagramme Le(s) moniteur(s) souscrivent à l'événement AttackEvent de l’ATM. Si une attaque est détecté, l’ATM envoie l'évènement à tous les subscribers et les subscribers ont l’option de bloquer l’ATM.

### 3.2.4 Table de description des éléments du diagramme

|  |  |
| --- | --- |
| **Élément** | **Description** |
| ATM | L’ATM est la représentation physique de notre système bancaire. le client utilise ce terminal afin de faire des opérations bancaires comme un dépôt, un retrait ou un transfert d’argent entre 2 compte. |
| Agent Monitor | L’Agent Monitor est la représentation physique de notre système qui informe les agents des évènements de l’ATM. Les agents utilisent le monitor pour voir les différents évènements survenues sur les ATM et permet d’envoyer des évènement en retour pour effectuer des actions. |

### 3.2.5 Texte décrivant la relation entre les éléments et les tactiques

La détection de l’attaque est détectée lorsque le NIP d’une carte n’a pas été entré correctement plus de 3 fois. L’ATM réagit à l’attaque en informant un agent avec l’architecture publish/subscribe et en bloquant l’accès à l’ATM. Un agent peut débloquer l’ATM en envoyant un event à l’ATM pour que le dispositif soit de nouveau accessible (recover from attacks).

# 4 Restreindre l’accès aux fonctionnalités portées sur un compte bancaire (dépôts, retraits, informations, etc.) seulement à la personne détenant le compte

|  |  |
| --- | --- |
| **objectifs d'affaires** | Restreindre l’accès aux fonctionnalités portées sur un compte bancaire (dépôts, retraits, informations, etc.) seulement à la personne détenant le compte |
| **Source** | Personne se présentant au guichet avec une carte bancaire |
| **Stimulus** | La personne essaie d’accéder au compte bancaire de la carte qu’il a dans ses mains |
| **Artéfact** | Service d’authentification du GAB après avoir entré la carte bancaire |
| **Environnement** | Le système est fonctionnel et en cours d’exécution |
| **Réponse** | Le système protège l’accès en demandant un NIP de la carte bancaire à l’utilisateur ( en plus de la carte elle-même). Toutes les activités d’entrée sont enregistrés dans un journal. |
| **Mesure de la réponse** | Si l’authentification est brisée, toutes les fonctionnalités du GAB s’offrent à la personne. Par contre, après 3 essais de NIP infructueux, la carte bancaire reste à l’intérieur du guichet et il est impossible d’accéder au compte de la banque par la suite |
| **Questions** | 1. Est-ce que toutes les activités d’entrée sont cataloguées? 2. Est-ce que le compte est bloqué après plusieurs accès infructueux? 3. Combien de temps le compte est-il bloqué? 4. Est-ce que la banque nous contacte lors d’activités suspicieuses avec le compte? 5. Si il y a entrée frauduleuse, quelles sont les fonctionnalités critiques? |

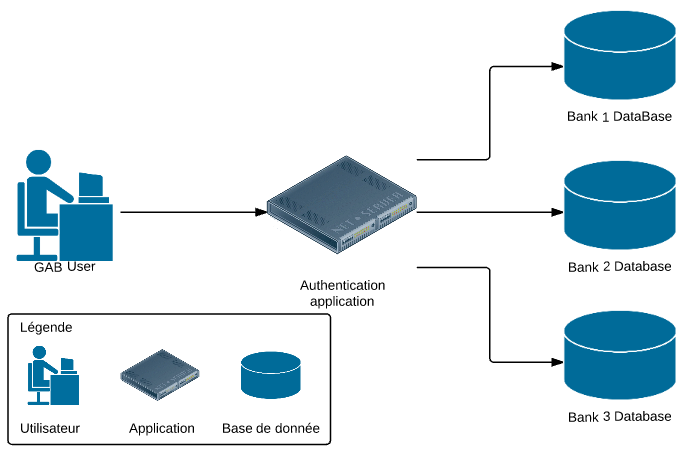
## 4.1 Tactique 1 : Authentifier les acteurs (résister aux attaques)

**Description**: S’assurer d’avoir une authentification efficace et difficile à déjouer. S’assurer que les techniques de bases ne fonctionnent pas pour entré dans le système illégalement.

**Justification**: Avoir une authentification rigoureuse nous permet d’éviter que quelqu’un non-autorisé accède au système illégalement. Ainsi, après trois essais de NIP, il n’est plus possible d’accéder au compte de la carte.

## 4.2 Vue architecturale (à l’extérieur de la classe)

### 4.2.1 Système d’authentification du GAB



### 4.2.2 Texte de description du diagramme

La vue ci-haut représente comment l’authentification du guichet automatisé bancaire s’applique. On y aperçoit l’utilisateur qui tente d’utiliser les fonctionnalités du GAB à l’aide d’une carte bancaire. L’application, qui se présente comme une frontière entre l’utilisateur du GAB et les différentes bases de données, lui demande un NIP. Si le NIP est le bon, l’utilisateur a donc accès au compte de la carte bancaire de la banque concernée. Sinon, il ne peut accéder aux différentes fonctions et/ou informations du compte.

### 4.2.3 Table de description des éléments du diagramme

Les éléments représentent les différents composants en jeu, donc l’utilisateur, l’application d’authentification et les serveurs des banques qui contiennent l’information des comptes bancaires. Ceux-ci sont soient des clients (demandant un service) ou un serveur (fournissant le service). Il y a également des connecteurs entre eux (début et fin des flèches) représentant les types d’activités (requête ou réponse)

### 4.2.4 Texte décrivant la relation entre les éléments et les tactiques

La relation pouvant décrire les éléments avec les tactiques est une relation entre l’utilisateur du GAB et l’application qui l'identifie. La relation peut être catégorisée comme une requête.

# 5 Récupérer des arnaques physiques sur les utilisateurs. Un utilisateur forcé à effectuer une transaction devrait pouvoir en aviser la banque discrètement.

|  |  |
| --- | --- |
| **Objectifs d'affaires** | Récupérer des arnaques physiques sur les utilisateurs. Un utilisateur forcé à effectuer une transaction devrait pouvoir en aviser la banque discrètement. |
| **Source** | Un utilisateur ~~pas encore authentifié sur le GAB.~~ |
| **Stimulus** | Changer le comportement du GAB. |
| **Artéfact** | Un log avec un timestamp de la transaction et l’endroit du GAB. |
| **Environnement** | Le système en en ligne; complètement opérationnel. |
| **Réponse** | La banque est mise au courant de la transaction de secours.  Les autorités sont mises au courant de l’alerte. |
| **Mesure de la réponse** | Temps de réaction des notifications aux autorités.  Taux de réduction des arnaques faites aux guichets. |
| **Questions** | 1. Quel montant est allouée dans la transaction de secours ? 2. Quel serait le coût de l’implémentation du système de sécurité ? 3. Quelle tactique est la plus subtile et efficace pour lancer l’alerte ? |

## **5.1 Tactique 1 : Detect Intrusion**

**Description**: Lorsque l’utilisateur est devant le guichet, il peut ajouter un “9” à la fin de son NIP pour lancer le module d’alerte du compte et du guichet.

**Justification**: L’ajout d’un chiffre à la fin de l’entrée du NIP est une méthode subtile d’aviser la banque de la situation. Il est pris pour acquis ici que c’est l’utilisateur arnaqué qui effectue la combinaison du code, car c’est habituellement le cas.

## **5.2 Tactique 2 : Limit Exposure**

**Description:** Suite à l’entrée du code d’alerte, une “fausse” interface d’utilisateur est affichée sur l’écran. Un montant prédéterminé est affiché comme étant disponible à l’utilisateur pour un retrait. Les actions de base sont encore disponibles, mais seulement sur ce compte factice.

**Justification:** Ce montant n’est pas le vrai montant que l’utilisateur possède, c’est seulement un montant qui peut être retiré et pour restreindre le montant que l’arnaqueur peut possiblement retirer à la victime. Ainsi, l’arnaqueur a moins de chance de s’attaquer à la victime. Il sera plus facile aussi pour la banque de connaître le montant qui est volé et ainsi donner des éléments à l’enquête du vole, une fois la police avisée.

## **5.3 Tactique 3 : React to Attacks - Inform Actors**

**Description:** Lors du lancement de l’alerte, un message incluant un log complet de la transaction est envoyé à la banque, qui a son tour notifie les autorités.

**Justification:** Informer la banque et la police le plus rapidement possible permet un temps de réaction à l’événement beaucoup plus efficace, ce qui augmente les chances d’intervenir à temps pour arrêter l’arnaqueur.

## 5.4 Vue architecturale (à l’extérieur de la classe)

### **5.4.1 Diagramme**



**Figure 1.0 :** Diagramme du scénario de sécurité

### 5.4.2 Table de description des éléments du diagramme

|  |  |
| --- | --- |
| **Élément** | **Responsabilité** |
| Arnaqueur | Ceci représente l’entité (normalement humaine) qui force l’utilisateur à faire des transactions. |
| Utilisateur | Ceci représente l’utilisateur qui se fait manipuler et qui fait des transactions sur son compte, contre sa volonté. |
| GAB | Le guichet qui est relié à la banque sur lequel l’utilisateur fait le code d’urgence. Il doit afficher une fausse page de transaction. |
| Banque | Représente la banque qui reçoit le code d’alerte et qui sait qu’un utilisateur se fait arnaquer. La banque, à ce moment, communique avec le système de gestion d’alertes pour l’avertir de la situation. |
| Système de gestion d’alertes | Représente le système des services d’urgence qui reçoit les informations nécessaires à l'intervention. |

### 5.4.3 Table de description des relations des tactiques entre ces éléments

|  |  |
| --- | --- |
| **Élément** | **Responsabilité** |
| Detect intrusion | Lors de l’entrée du code d’alerte, le système détecte qu’il est question d’une arnaque et passe à un mode conçu à cet effet. |
| Limit Exposure | Une fois que le guichet sait qu’il s’agit d’une urgence, il communique avec la banque et affiche une interface limitée pour la sécurité de l’utilisateur. |
| Inform Actors | Le GAB informe la banque du problème. La banque alerte les autorités concernées qu’il y a une arnaque en cours. |

### 5.4.4 Description des relations entre les éléments

Lors d’une situation où un arnaquer force un utilisateur à retirer de l’argent d’un guichet, l’utilisateur se rend au guichet et entre le code d’alerte pour avertir le guichet. À ce moment, avec la tactique ‘detect intrusion’ le guichet comprend qu’il y a une situation d’urgence en cours. Le guichet utilise la tactique ‘limit exposure’ en affichant une fausse interface de transaction pour que l’arnaqueur pense que l’utilisateur fait une vrai transaction. Cette interface va offrir les même opérations, mais avec un montant prédéterminé et avec une limite de transactions plus basse. Dès que la banque va avoir reçu l’alerte du guichet, celle-ci va utiliser la tactique ‘inform actors’ en communiquant l’alerte au système de gestion d’alertes qui va communiquer avec les autorités concernées avec les informations nécessaires.

# 6 Empêcher l’utilisateur d’accéder à un compte qui n’est pas le sien.

|  |  |
| --- | --- |
| **Objectifs d’affaires** | L’objectif est qu’aucun utilisateur n’accède à un compte qui n’est pas le sien en tout temps |
| **Source** | Utilisateur |
| **Stimulus** | * Authentification |
| **Artéfact** | * Accéder au service du système bancaire |
| **Environnement** | * Opération normale |
| **Réponse** | * Notifier l’utilisateur * Notifier les administrateurs * Conserver la carte de l’utilisateur |
| **Mesure de la réponse** | * Le temps de délais avant qu’un administrateur soit notifié * Le système a pu résister combien de fois d’accès interdit aux personnes sans autorisation * Bloquer l’accès de l’utilisateur après un certain nombre d’accès |
| **Questions** | * Combien de temps ça prend avant de notifier l’utilisateur ? * Combien de temps ça prend pour notifier les administrateurs du système ? |

## **6.1 Tactique 1 : Lock computer**

**Description**: Si une certaine condition est atteinte, le système entre en mode barré qui interdit l’utilisation normale.

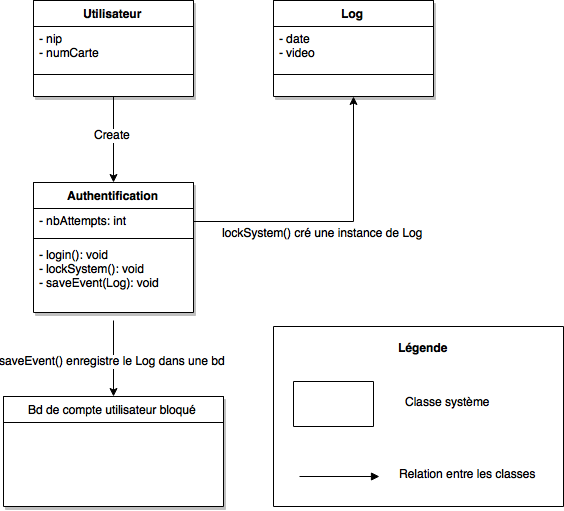
**Justification**: Lorsque l’utilisateur entre le mauvais NIP trois fois consécutive, le système devient inaccessible pour l’utilisateur qui l’utilise et conserve la carte de celui-ci. Il doit alors communiquer avec la banque afin de regagner l’accès au guichet.

## **6.2 Tactique 2 : Maintain audit trail**

**Description**: Recueillir et sauvegarder des informations pertinentes lors d’une attaque.

**Justification :** Lors d’une attaque, il est important d’enregistrer les informations de la session et la capture de la caméra de l’atmpour ensuite envoyer ces données vers les administrateurs du système et le service de sécurité de la banque.

## 6.3 Vue architecturale (à l’extérieur de la classe)



### 6.3.1 Description

Chaque utilisateur qui tente d’utiliser le guichet créer une nouvelle authentification. À partir de ce moment, l’utilisateur a droit à trois tentatives pour réussir à entrer le bon NIP. S’il n’y arrive pas, la classe d’authentification, avec sa fonction *lockSystem()*, barre le système et conserve la carte de l’utilisateur.

Également, le classe conserve la date et le vidéo du guichet à l’aide de la classe Log.

Finalement, le compte bloqué de l’utilisateur est enregistré dans une base de données sur le serveur.

### **6.3.2 Relation avec la tactique**

*Lock computer*Après une troisième tentative infructueuse, le système tombe en mode barré.

*Maintain Audit trail*La classe *Authentification* utilise la classe *Log* afin d’enregistrer les données de la session de l’utilisateur en faute afin de garder une trace des événements.

### 6.3.3 Composantes

*Utilisateur*Contient l’information de la carte et le NIP.

*Authentification*

Contient le nombre de tentatives autorisées ainsi que les méthodes permettant de mettre le système en mode barré, d’enregistrer les informations de la session ainsi que d’enregistrer le compte dans une base de données.

*BD de compte utilisateur bloqué*Contient tous les utilisateurs dont le compte a été bloqué.

*Log*Contient la date ainsi que le vidéo de tous les sessions ayant résultées en un compte barré

# 7 Protéger la connexion entre le guichet et le serveur contre les attaques de type “Man-in-the-middle”.

|  |  |
| --- | --- |
| **objectifs d'affaires** | En tant que fournisseur de service banquiers je veux protéger les informations personnels et bancaires des mes clients pour augmenter la confiance des clients envers l’entreprise. |
| **Source** | Attaque d’une tierce partie |
| **Stimulus** | Une attaque non autorisée est faite afin d’avoir accès aux services du système |
| **Artéfact** | Connexion réseau et les données |
| **Environnement** | Mode d’opération normal |
| **Réponse** | Les messages entre le guichet et le serveur devrait être authentifiés ou refusés |
| **Mesure de la réponse** | * L’importance de l’impact sur la performance du système. * Le délai de récupération suite à une attaque * Nombre d’attaques qui ont été résisté |
| **Questions** | 1. Quelle est le temps de réponse de l’intrusion à atteindre. 2. Si le système a révoqué l’accès combien de temps est ce que ça prend avant qu’un technicien remette l’ATM en marche. |

## 7.1 Détection et 1 récupération

### 7.1.1 Tactique 1 : Verify message integrity

**Description**: Un bloc de données supplémentaire est échangé entre le client et le serveur. Ces données sont une validation encryptée du contenu du message. Si le message est modifié en cours de route sur le réseau, le destinataire pourra le détecter.

**Justification**: Permet de détecter si une tierce partie a modifié un message transmis entre le guichet et le serveur. Si une anomalie est détectée, le message doit être retransmis.

### 7.1.2 Tactique 2 : Encrypt data

**Description**: Un échange de clefs privées et de clefs publiques entre le client et le serveur permet d’encrypter puis de décrypter les données transmises.

**Justification**: Il ne sera pas possible de forger des messages aux clients ou aux serveurs, ni de lire les message transigeant sur le réseau.

### 7.1.3 Tactique 3 : Revoke access

**Description**: Ne plus permettre à ce client d’interagir avec le système.

**Justification**: Si un guichet (ou un attaquant) tente de signer un message avec une clef périmée, ce guichet devrait voir tous ses accès révoqués. Comme il s’agit d’une attaque très ciblée, une approbation manuelle doit être faite afin de réactiver ce guichet ou client.

# **Scénario : Retrait d’argent avec une carte volée**

|  |  |
| --- | --- |
| **objectifs d'affaires** | Empêcher à 99,99% l’utilisation d’une carte volée |
| **Source** | Humain, attaquant externe. |
| **Stimulus** | Tentative de connexion au compte avec un NIP |
| **Artéfact** | Les données (argent) du propriétaire de la carte. |
| **Environnement** | Mode d'opération normal |
| **Réponse** | 1. Journalisation de l’incident,  2. Retenir la carte dans l’ATM  3. Désactiver le compte du client  Informer le propriétaire de la carte volée |
| **Mesure de la réponse** | Nombre de transactions effectuées avec des cartes volées |
| **Questions** | 1. Combien de tentatives d’authentification est-ce que l’utilisateur peut avoir avant que le système ne le bloque?  2. Est-ce que l’ATM conserve la carte lorsqu’il y a eu trop de tentatives et que le compte est bloqué ?  3. Combien de temps une session peut-elle être active ?  4. |

## **Tactique 1 : Revoke Access**

**Description**: Lorsqu’un NIP non valide est entré 3 fois de suite dans une même session, l’ATM notifie la banque que le compte relié à cette carte est compromis. La banque gèle le compte empêchant ainsi toutes transactions futures reliées à celui-ci jusqu’à ce que le détenteur du compte déclare sa carte comme volée ou perdue.

**Justification**: Cette tactique permet de protéger les comptes d’une tentative de fraude si quelqu’un détient une carte qui n’est pas la sienne. En bloquant un compte, on empêche aussi l’usage de cartes qui pourraient avoir été clonées.

## **Tactique 2 : Detect Intrusion**

**Description**: Lorsqu’un NIP non valide est entré 3 fois de suite dans une même session, l’ATM garde la carte dans son lecteur de carte empêchant ainsi l’utilisateur de la reprendre.

**Justification**: Une personne non autorisée qui essaye d’utiliser une carte qui n’est pas la sienne n’a le droit qu'à trois essais réduisant ainsi grandement le risque d’intrusion.

## **Tactique 3 : Maintain Audit Trail**

**Description**: Lorsqu’une transaction est effectuée par un client, celle-ci est enregistrée dans un fichier de journalisation des transactions. Dépôt, virement, retrait, paiement, etc. Tout type de transactions est gardé en mémoire.

**Justification**: Un client qui observe des transactions portées à son compte qu’il n’a pas effectuées pourra en conclure qu’une attaque a été effectuée sur son compte.

## Diagramme 1.0 Modélisation de la sécurité du système d'ATM.

### **Description du diagramme:**

### Deux composants du système, l’ATM et le serveur de la Banque ont des relations de sécurité en cas d’attaques. Les deux systèmes respecteront la tactique de détection d’intrusion pour empêcher le vol d’argent avec de cartes volées. De plus, le système respectera la tactique de Revoke Access pour geler le compte attaqué après l’identification de l’attaque. Également, avec la tactique de Maintain Audit Trail le système permet de journaliser les transactions.

### 

### Table de description des éléments du diagramme :

|  |  |
| --- | --- |
| **Tactiques** | **Descriptions** |
| Detect Intrusion | Détecter l'intrusion au compte avec la carte volée |
| Revoke Access | Geler le compte attaqué |
| Maintain Audit Trail | Journalisation des transactions |

### Relations :

Les lignes de l'ATM vers le serveur représentent la tactique de détection d’intrusion, obstruction du compte et la journalisation des transactions.