Université du Québec en Outaouais

Département d'informatique et d'ingénierie

Thèse de doctorat

Contrôle de flux d'informations basé sur la granularité

Présentée comme exigence partielle du programme de

Doctorat en sciences et technologies de l'information

sous la direction de:

Professeur Luigi Logrippo

PAR

OMAR ABAHMANE

Octobre 2015

Jury d'évaluation

Président du Jury :	Dr. Larbi Talbi
Membre du Jury :	Dr. Amy Felty
Membre du Jury :	Dr. Chamseddine Talhi
Membre du Jury :	Dr. Karim El Guemhioui
Directeur de recherche :	Dr. Luigi Logrippo

Thèse acceptée le : 20 octobre 2015

Dédicace

Louange à **DIEU**, Le Clément et Miséricordieux.

A ceux à qui je dois tous mes moments de succès passés et futurs; **mes chers parents**.

A celle qui m'a soutenu au meilleur de ses capacités et qui m'a accompagné et encouragé tout au long de ce parcours **ma chère épouse**.

A **mes chers enfants,** qui ont toujours été là pour revitaliser ma vie en temps de pression et de détresse.

A mon **cher professeur Luigi Logrippo** qui a été derrière l'aboutissement de ce projet de recherche.

Remerciements

Je tiens à exprimer ma profonde gratitude au Professeur Luigi Logrippo pour son soutien, sa disponibilité et son engagement tout au long de ce projet de recherche. Je remercie également les membres du jury : Professeur Larbi Talbi, Professeur Amy Felty, Professeur Chamseddine Talhi et Professeur Karim El Guemhioui de leurs remarques, suggestions et apports enrichissants. Je tiens aussi à remercier toute personne ayant contribué de près ou de loin à la réalisation de ce projet. Enfin, Je remercie, tout autant, les membres de ma famille pour leur encouragement et leur patience.

Ce travail a été subventionné en partie par le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG).

Table des matières

Liste des figures

Figure Page

Liste des tableaux

Tableau Page

Liste des abréviations, sigles et acronymes

Abréviation	Langue	Signification
ABAC	*(Ang)*	Attribute-Based Access Control
Admin.	*(Fr-Ang)*	Administrateur (Administrateur de sécurité)
AF	*(Fr)*	Allocation de Fichiers *(Ang. FA)*
AFV	*(Fr)*	Allocation de Fichiers Volatile *(Ang. VFA)*
BLP	*(Ang)*	Bell–LaPadula Model
DAC	*(Ang)*	Discretionary Access Control
DoD	*(Ang)*	Department of Defense
EGA	*(Fr)*	Engin de Gestion d'Accès *(Ang. AME)*
GBFC	*(Ang)*	Granularity Based Flow Control
IA2	*(Fr-Ang)*	Identification – Authentification - Autorisation
IBAC	*(Ang)*	Identity-based Access Control
ID	*(Fr-Ang)*	Identifiant
ISO	*(Ang)*	International Organization for Standardization
LCC	*(Fr)*	Libérer - Charger - Construire
LgCC	*(Fr)*	Libérer – Granuler - Charger – Construire
MAC	*(Ang)*	Mandatory Access Control
MLS	*(Ang)*	Multi-Level Security
NLP	*(Ang)*	Natural Language Processing
RBAC	*(Ang)*	Role-Based Access Control
RuBAC	*(Ang)*	Rule-Based Access Control
UCON	*(Ang)*	Usage Control
UML	*(Ang)*	Unified Modeling Language
VB	*(Ang)*	Visual Basic
VSTO	*(Ang)*	Visual Studio Tools for Office
XACML	*(Ang)*	eXtensible Access Control Markup Language

Note : autres acronymes relatifs aux modèles de sécurité sont listés dans l'annexe 1.

Résumé

Dans ce projet de recherche, nous présentons de nouvelles techniques qui adressent deux principaux problèmes: la protection de l'information à différents niveaux de granularité et le contrôle de flux de données. Nous procédons tout d'abord par une étude des défis et des limites des modèles de contrôle d'accès conventionnels en matière de contrôle de flux. Par la suite, nous introduisons un nouveau modèle de contrôle de flux basé sur la granularité, le GBFC, dans ses aspects logique et prototype. GBFC est capable de garantir le contrôle de flux sous des hypothèses raisonnables. En outre, il offre des avantages dont l'adaptabilité, le contrôle total, la fiabilité et la compatibilité. Essentiellement, dans GBFC l'information classifiée confidentielle est manipulée à divers niveaux de granularité puis accédée à travers des références volatiles qui leur sont attribuées. Le contrôle de flux d'informations est appliqué sur ces références. Nous introduisons également le concept de vues pour l'accès à l'information et celui d'injection de bruit qui représentent des mécanismes de base du modèle de contrôle de flux basé sur la granularité. Avec l'injection de bruit, un document peut être transformé selon différents points de vue pour supprimer ou remplacer des informations confidentielles de façon quasiment indétectable par le lecteur non autorisé. Par conséquent, l'inférence peut être rendue beaucoup plus difficile avec ce procédé. Le modèle GBFC est destiné à compléter, plutôt que remplacer les méthodes de contrôle d'accès existantes.

Abstract

In this research project we present new techniques that address two main issues: information protection at various levels of granularity and data flow control. We first investigate challenges and limits of established access control models regarding flow control. We then introduce a new flow control model based on granularity, the GBFC, in both aspects logic and prototype. GBFC is capable of guaranteeing flow control under reasonable assumptions. In addition, it offers advantages such as adaptability, full control, reliability and compatibility amongst others. Essentially, in GBFC, classified information at

suitable levels of granularity is accessible through volatile references and information flow control is applied on the references. We also introduce the concepts of views for information access and Noise Injection that represent building blocks for the Granularity Based Flow Control. With noise injection, a document can be transformed into different views to erase or replace protected information and this transformation can be made almost undetectable to the unauthorized reader. Therefore, inference can be made much more difficult with this method. The GBFC model is intended to complement, rather than replace, existing access control methods.

Publications

Les Chapitres 4 et 5 ont fait l'objet d'une publication dans les actes de la conférence : Privacy, Security and Trust 2014 (PST 2014), Toronto, Juillet 2014 selon la citation :

Omar Abahmane, Luigi Logrippo, "Granularity Based Flow Control", in the Proceedings of the Twelfth Annual International Conference on Privacy, Security and Trust (PST), Toronto, Canada, July 2014, pp. 239-248

L'article a fait partie des 46 articles acceptés parmi 161 soumis à cette conférence (*taux d'acceptation : 28.5 %*)

Le texte intégral de l'article est disponible sur le lien :
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6890945

L'intégralité de ce projet de recherche est en cours d'être synthétisée pour faire l'objet d'un article de journal.

Chapitre 1 : Présentation générale

1.1 Introduction générale

Avec la large prolifération des réseaux de données et des technologies de l'Internet, la venue des réseaux sociaux et de l'infonuagique [1] ainsi que l'extraordinaire propagation des technologies d'accès mobile aux données, l'information devient de plus en plus disponible et par la même occasion davantage à risque de fuites, d'accès ou de flux illégitimes. Dans ce contexte extrêmement complexe, la sécurité des données et de l'information est devenue une préoccupation continue.

En effet, l'enjeu est majeur et ne fait qu'être continuellement confirmé par les statistiques et la presse spécialisée. *"Il est difficile de juger si la sécurité se détériore, les acteurs malveillants s'améliorent ou une combinaison des deux... Durant les six derniers mois, huit incidents de sécurité ont été derrière la fuite de pas moins de 80 millions d'enregistrements confidentiels et les prévisions sont à la hausse..."* commente Inga Goddijn Directeur Général des services d'assurance des risques chez RBS [2].

Parmi les préoccupations majeures de la gestion des systèmes de sécurité et de contrôle d'accès aux informations, figure le contrôle de flux d'informations qui met l'accent sur la prévention de propagation et de fuites d'informations confidentielles d'utilisateurs authentifiés et légitimes vers d'autres sujets non autorisés qui ne devraient pas y avoir accès [3].

Ce problème de fuite d'informations est notre principale motivation pour cette thèse et on tentera de proposer une solution appropriée pour y remédier. Notre solution sera sous forme d'un modèle de sécurité dédié au contrôle de flux visant à compléter et consolider les approches et techniques de contrôle d'accès connues dans le domaine de sécurité de l'information. Notre modèle repose sur l'utilisation de l'aspect granulaire de l'information

pour y appliquer des critères de sécurité dans le but de la protéger de toute diffusion qui viole les exigences de sécurité au sein d'une organisation. Pour cela, on procédera par une étude bibliographique et analytique des modèles de sécurité et de contrôle de flux actuellement en application afin d'en faire ressortir les principales limites qui pourraient justifier l'ampleur du problème de fuites d'informations (*Information leaks*) constaté en pratique. Puis, on fournira une étude détaillée de notre modèle, de son mode d'action et de ses fondements logiques lui permettant de réaliser les objectifs souhaités et garantir un contrôle de flux qui satisfait les besoins de sécurité prescrits.

On estime que notre modèle de contrôle de flux basé sur la granularité (GBFC) sera capable d'apporter une amélioration considérable par rapport aux solutions existantes du fait de son architecture centralisée et dynamique basée sur l'information comme élément de base pour l'implémentation des critères de sécurité. Par ce modèle, on tentera de fournir une solution globale qui adresse les principales causes du problème de fuites d'informations en proposant une combinaison novatrice des concepts de disponibilité et de granularité de l'information.

On amènera à l'appui des atouts de notre modèle un ensemble d'exemples et de scénarios d'application qui en illustrent la faisabilité et mettent en valeur les contributions du modèle. Le modèle logique et le prototype software du GBFC viendront appuyer les capacités de ce modèle et confirmeront davantage son apport quant à la garantie de la sécurité des flux et à la protection contre les fuites d'informations.

Le concept de granularité sur lequel repose notre modèle est un concept généraliste appliqué dans plusieurs disciplines et qui considère le niveau de détails avec lequel les données sont manipulées. Ainsi, un haut niveau de granularité induit une manipulation à un niveau atomique de haut niveau de distinction entre les éléments composant l'information. D'autre part, un bas niveau de granularité suppose un niveau d'agrégation plus élevé renfermant moins de détails (plus de détails sur ce concept sont présentés dans la section 4.5 du chapitre 4).

1.2 Proposition du sujet

1.2.1 Motivation pour le sujet

Depuis les années 70, un grand nombre de modèles et de techniques ont été développés pour préserver les données et garantir un niveau acceptable de sécurité au sein des systèmes d'informations et sur les réseaux. Ces modèles et techniques visent à empêcher les accès illégitimes aux données et prévenir les flux non autorisés des informations.

Cependant, et malgré tous les efforts entrepris dans ce sens, la sécurité des flux d'informations reste un grand défi. En effet, un bon nombre de problèmes de fuites d'informations, d'accès illégitimes aux données confidentielles et de protection d'informations personnelles et de vie privée persistent. Il est courant de nos jours de trouver disponibles au grand publique des informations privées et même classifiées confidentielles sur l'Internet.

Les statistiques de fuites d'informations publiées par Digital Forensics Association, pour la période de 6 ans (2005-2010) reportent un nombre d'incidents de fuites d'informations qui dépasse 3765, affectant un total de 806.2 millions d'enregistrements avec un coût estimé de 156.7 milliards de dollars [4]. Le nombre d'incidents reportés atteint 4363 durant les 3 dernières années (2012-2014) avec plus de 1.2 milliards d'enregistrements affectés, selon Open Security Foundation [5]. Le coût estimé durant ces 3 dernières années est de l'ordre de 233 milliards de dollars (Figure 1)

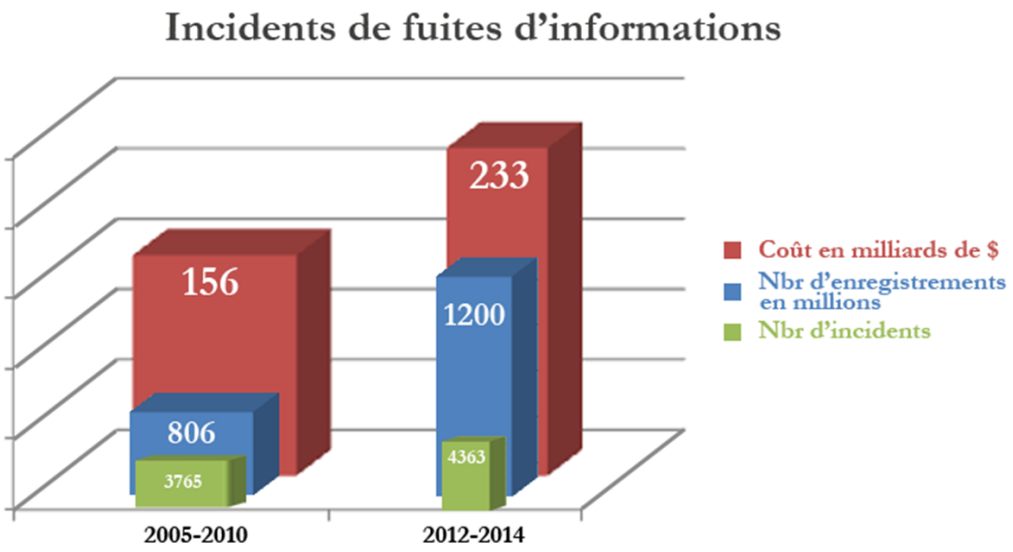


Figure 1. Statistiques des incidents de fuites d'informations

Malgré l'existence d'une multitude de modèles et de techniques de renommée renforçant la sécurité des informations, de nombreux problèmes de sécurité et d'atteinte à la vie privée continuent d'émerger. Ceci favorise le développement de toute une économie basée sur le commerce en ligne de données personnelles ou d'informations classifiées qui deviennent des produits disponibles au grand public. Cette économie propose des prestations allant de simples services en ligne procurant des informations privées et personnelles sur les individus (identité, professionnelles, financières, voire juridiques), aux grandes institutions offrant des informations classifiées et sensibles à la demande, *Wikileaks* [6] étant un des récents et des plus controversés exemples parmi beaucoup d'autres. Dans la majorité des cas, la publication et la mise à disposition de ces informations constitue un flux illégitime considéré comme une violation de la vie privée ou des règles de confidentialité pour le propriétaire de l'information. Un exemple beaucoup plus simple serait un Curriculum Vitae qui se transforme, sans consentement préalable, en informations bibliographiques offertes par des tiers sur Internet après qu'un candidat l'ait remis à un recruteur.

Dans notre recherche, nous faisons une distinction entre contrôle d'accès aux données et contrôle de flux. Le contrôle d'accès se préoccupe du contrôle des droits d'accès à

l'information, soit : qui accède quoi? L'objectif majeur étant d'empêcher l'accès aux informations par des sujets non autorisés. Le contrôle de flux, d'autre part, se préoccupe du contrôle de propagation de l'information, soit : à qui est communiquée l'information? Le contrôle de flux a pour objectif principal de prévenir les fuites d'informations à des sujets non autorisés.

Lorsque nous examinons un processus qui a déclenché des fuites d'informations, nous remarquons que durant le transfert de données, un sujet -sous forme d'utilisateur ou de processus- a volontairement ou involontairement diffusé les informations confidentielles auxquelles il a accès à un sujet non autorisé d'accès. La situation devient encore plus sérieuse avec l'adoption de l'informatique portative où certaines applications mobiles peuvent mettre à risque de flux illégitime les informations confidentielles de l'utilisateur sans que celui-ci s'en rende compte. Il est évident que la situation aurait été bien plus catastrophique si des mécanismes de contrôle d'accès n'avaient pas été mis en place, au moins pour empêcher l'accès illégitime aux données confidentielles par des sujets non autorisés.

Cependant, des techniques plus robustes et plus efficaces de contrôle de flux devraient être proposées pour traiter ces possibles fuites d'informations. La mise en œuvre de modèles et techniques spécifiques au contrôle de flux serait d'un grand apport quant à la protection de l'intimité (flux illégitime de données personnelles et de vie privée) et à la préservation des droits d'auteurs (flux illégitime de contenus sous droit d'auteurs).

1.3 Problématique

Considérant deux sujets (utilisateurs ou processus du système) S_1 et S_2, on peut dire qu'il y a un flux d'information de S_1 vers S_2 quand S_1 propage (diffuse) ou transmet des données de façon volontaire ou involontaire à S_2. En d'autres termes: S_1 écrit les données dans un objet O_1 (mémoire, fichier, etc.) auquel S_2 accède en lecture. [7, 8].

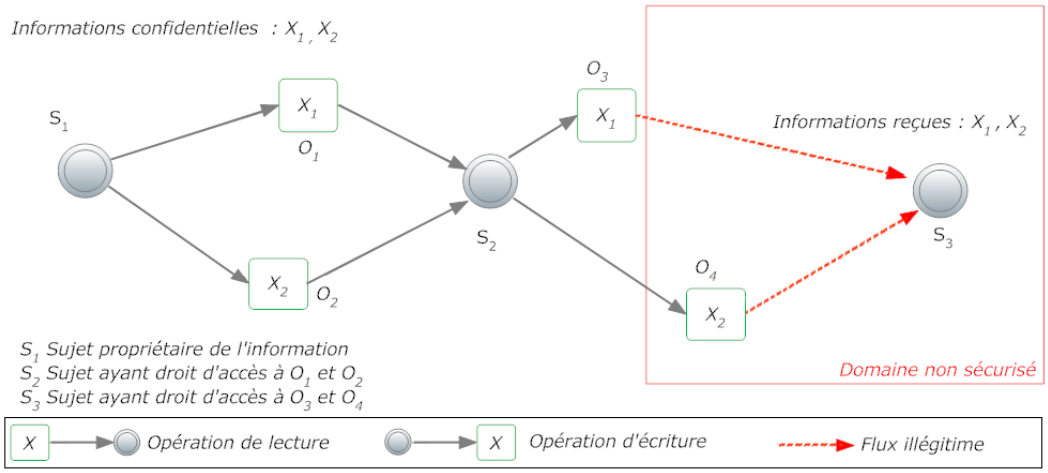


Figure 2. Flux d'informations illégitime

Se basant sur cette définition, un flux illégitime d'information survient lorsque S_2 écrit des données confidentielles classifiées [9, 10] dans un objet O_3 accessible par un quelconque sujet S_3 qui ne devrait pas avoir accès à ces données. Le résultat étant une fuite d'information en violation avec la politique de sécurité appliquée dans le système. Voir Figure 2.

En fait, il s'agit d'une pratique aussi ancestrale et aussi répandue qu'est l'être humain. Cette pratique se manifeste dans la vie de tous les jours et de tout le monde par la simple divulgation d'un secret par son possesseur. Dans le monde des affaires, on la retrouve dans tout ce qui est espionnage industriel, atteinte aux droits d'auteurs, etc.

Une telle pratique est considérée dans la majorité des cas illégitime, illégale voire même une trahison, comme l'est le cas dans le domaine politique et militaire. Un flux illicite d'information pourrait être un fichier confidentiel ou privé remis à un collaborateur, qu'on retrouve chez d'autres parties qui ne devraient pas l'avoir. Ou encore un email qui a été transféré volontairement ou involontairement à un tiers non autorisé à le recevoir.

Le contrôle de flux d'informations a été implémenté dans certains modèles de contrôle d'accès aux informations, tels que le contrôle d'accès obligatoire (MAC), etc., mais avec une faiblesse persistante qui est la possibilité pour les utilisateurs ou les programmes

d’accéder illégalement et de manière indirecte à des éléments d'information en collaborant avec des utilisateurs qu’y ont un accès légal [11].

Pour illustrer ce problème, nous pourrions envisager l'exemple d'une transaction commerciale engendrant un paiement électronique réalisé par téléphone. Durant cette transaction, le client fournit tous les renseignements susceptibles de déclencher l’opération de paiement par sa carte de crédit ou par son organisme financier. Ces informations collectées par l’agent commercial sont considérées confidentielles du fait que leur possession par n’importe quel autre sujet pourrait engendrer leur utilisation frauduleuse et poser un sérieux problème de fuite dont les répercussions et les responsabilités pourraient être difficiles à cerner. Ces données confidentielles collectées deviennent encore plus vulnérables si on prend en considération un ensemble de facteurs organisationnels et managériaux, tel les démissions du personnel, leurs transferts ou changements de responsabilités ou même les cas de mise en liquidation ou vente de la compagnie.

La protection de telles informations a toujours été un des soucis majeurs des entreprises. Certaines ont adopté des solutions simplistes comme l’interdiction d’appareils photographiques dans le lieu du travail. D’autres forcent, en plus, des environnements de travail sans papier afin d’empêcher toute reproduction ou transfert d’informations confidentielles. Pour les plus évoluées, on essaye de collecter les informations confidentielles de façons diversifiées (manuelle, automatisée, ...) de façon à empêcher un même sujet de disposer d’éléments d’informations susceptibles de porter atteinte à la confidentialité, une fois réunies.

Trois principales remarques peuvent être faites sur un processus de flux d’informations tel que décrit dans l’exemple précédent :

1- l’existence d’un transfert (flux) d’informations confidentielles
2- le fait que le transfert est opéré sous forme d’un flux total des éléments d’information confidentielle

3- la formulation de l'information confidentielle de manière facilitant son exploitation illicite.

Pour cette recherche, on se penchera principalement sur le contrôle de flux indirect d'informations élaborées sous forme de texte avec la possibilité de généralisation des divers concepts à d'autres formes de flux d'informations.

1.4 Hypothèse de travail

Les faiblesses des modèles de contrôle d'accès quant au contrôle de flux d'informations -modèles discutés dans la littérature et présentés dans le Chapitre 4- nous amène à avancer l'hypothèse que : **Un contrôle de flux robuste peut être implémenté à travers la conception d'un modèle dédié capable de prévenir la fuite d'informations dans les divers scénarios de manipulation (transfert volontaire, perte de données, attaques malveillantes, etc.). On estime qu'un modèle qui permet de transférer les informations dans un état granulaire, sous forme de références avec certaines restrictions de flux serait une solution acceptable au problème de fuites d'informations.** Pour arriver à ce but, nous envisagerons des mécanismes capables de satisfaire la condition suivante :

Toute tentative d'un sujet S_1 de transférer -de façon volontaire ou non- une information confidentielle à un sujet non autorisé S_2, rend cette information inaccessible pour S_2.

La conception d'un mécanisme qui réalise cette exigence est le sujet de notre thèse. Une preuve formelle (par analyse de scénarios) que le mécanisme que nous proposons rencontre cette exigence est donnée dans les Sections 6.4.2.4 et 6.4.2.5 du Chapitre 6.

1.5 Conventions de recherche

Il est à souligner que tout au long de ce document on adoptera des conventions de recherche et de présentation dans lesquelles:

1- Un *système* est un ensemble de ressources matérielles et logicielles en interaction ou interdépendance agissant pour réaliser un ensemble de fonctions spécifiques [12].

2- Un *domaine de sécurité* D est un ensemble d'entités qui adoptent la même politique de sécurité renforcée par la même autorité. En d'autres termes un environnement de sécurité homogène [12, 13].

3- Pour cette recherche on définit une *information confidentielle* comme étant toute information sous forme écrite refermant une valeur potentielle qui est privée (non disponible au publique), protégée et dont l'accès est régi par des droits et des autorisations spécifiés par son propriétaire ou par une instance d'administration de sécurité [12, 14].

4- Un *sujet* est une entité active du système sous forme d'un utilisateur (usager) ou d'un processus qui peut exécuter les différentes opérations d'accès à l'information ou de flux d'informations possibles dans le système. Un sujet peut être sous forme humaine ou logicielle et peut, générer, accéder, lire, écrire et manipuler des informations au sein du système. Un sujet S sera représenté graphiquement par un cercle portant le nom du sujet ou par un bonhomme en fil de fer (*Ang. stick man*) similaire à la notation UML d'un acteur [12, 15].

5- Un *objet* est un composant passif sous forme de matériel ou logiciel dans lequel une information peut être stockée. Un objet peut être physique tel un espace mémoire ou un secteur sur un disque, comme il peut être logique tel qu'un fichier, un paquet sur le réseau, etc. Un sujet a un nom et est représenté par un carré à coins arrondis. Le carré peut ou non

porter à l'intérieur un nom représentant l'information qu'il contient s'il y a lieu. Généralement, l'accès à un objet implique l'accès à l'information qu'il contient [12].

6- Une *opération d'accès (Op)* est une action exécutée par un sujet sur un objet. Généralement ces opérations peuvent être de type lecture, écriture, ajout ou exécution. Une *opération de lecture* (R) de données ou d'informations s'exécute par un sujet à partir d'un objet qui contient ces données ou informations. Une opération de lecture est schématisée par une flèche pointant de l'objet contenant l'information vers le sujet qui exécute la lecture. Une *opération d'écriture* (W) de données ou d'informations s'exécute par l'écriture d'une information par un sujet dans un objet donné. Une opération d'écriture est schématisée par une flèche pointant du sujet exécutant l'opération d'écriture vers l'objet sélectionné pour recevoir les données ou informations. Dans le cadre de cette recherche on est principalement concernés par les flux d'informations et qui se manifestent sous forme de lectures et d'écritures (R et W). Pour cela, on se limitera dans cette étude à ces deux types d'opérations comme opérations d'accès.

8- Pour un modèle de contrôle d'accès, on considère un *droit d'accès* comme étant l'autorisation de réaliser une opération *Op* par un sujet donné *S* sur un objet *O*. Ceci est représenté sous forme de *règle d'accès* : *Ar*< *S*, *O*, *Op* > qui renferme les composants principaux nécessaires pour exprimer un droit d'accès [16, 17].

1.6 Plan de la recherche et contributions visées

A la suite de cette brève introduction au sujet, on se fixe comme objectif général de cette recherche de proposer un nouveau modèle de contrôle de flux basé sur la granularité (GBFC). Ce modèle permettra de renforcer le contrôle de flux d'informations confidentielles de sujets autorisés ayant droit d'accès à des sujets non autorisés d'accès. GBFC appliquera de nouveaux concepts tel l'accès aux informations à travers des références, le contrôle de disponibilité des données par un système de fichier volatile, le processus de rafraîchissement des références et la dissolution des informations dans du

bruit afin d'en préserver la confidentialité. Pour arriver à ce but, nous effectuerons avant tout une étude bibliographique et analytique des principaux modèles de contrôle d'accès et de contrôle de flux existants afin d'identifier les causes possibles des fuites et des flux illégitimes d'informations. Cette analyse permettra d'exposer les points forts et dégager les faiblesses des différents modèles de sécurité existants du point de vue du contrôle de flux. En deuxième étape, on proposera notre approche pour pallier les limites relatives au contrôle du flux d'informations en expliquant notre modèle de contrôle de flux basé sur la granularité de l'information. Ainsi, dans cette thèse, on se donne comme objectifs spécifiques de développer le modèle GBFC dans son volet logique et applicatif (prototype). Le modèle logique nous permettra de :

1- proposer le formalisme logique du GBFC
2- valider la capacité de notre modèle de remédier aux faiblesses liées au contrôle de flux dégagées de l'évaluation précédente,
3- valider notre hypothèse de recherche de la Section 1.4.

D'un autre côté, l'application logicielle du GBFC sera sous forme d'un prototype qui nous servira de plateforme pour :

1- réaliser des simulations des fonctionnalités du modèle,
2- tester les divers scénarios d'accès aux informations et évaluer la capacité du modèle d'adresser les situations de fuites d'informations possibles

Dans le Chapitre 2, on se servira d'exemples concrets pour illustrer les différents niveaux d'action de notre modèle pour permettre le contrôle de flux et la protection contre les fuites d'informations. Par la suite, le Chapitre 3 traitera de la sécurité des informations en général et présentera les diverses classifications de l'information ainsi que les principaux critères à respecter durant leur implémentation. Le chapitre comportera aussi des définitions des concepts reliés au contrôle de flux d'informations. Le Chapitre 4 passera brièvement en revue la recherche dans le domaine de la sécurité de l'information et du contrôle de flux. Il commencera par une brève introduction et puis explorera les divers modèles de sécurité des

deux perspectives : contrôle d'accès et contrôle de flux. Le chapitre traitera aussi certaines techniques et méthodes moins connues dont la finalité est le renforcement de la sécurité d'accès et du flux d'information. Dans ce même chapitre on se penchera en détail sur le contrôle de flux et sur les problèmes reliés à son application. Une analyse détaillée sera aussi réalisée afin de déceler les principales limites des divers modèles relativement au renforcement du contrôle de flux. A la fin de ce chapitre nous traiterons les principaux concepts de granularité de l'information en passant en revue certaines publications dans ce domaine tout en mentionnant certains exemples d'application de concepts de granularité. Dans le Chapitre 5 de ce projet on présentera en détail notre modèle de contrôle de flux basé sur la granularité en dégageant les avantages et les apports de ce nouveau modèle.

Le Chapitre 6 dressera ensuite le modèle logique du GBFC capable d'offrir une plateforme de base pour l'implémentation du modèle. On tentera ainsi d'asseoir les fondements logiques capables de valider les capacités du modèle par rapports aux modèles existants quant au contrôle de flux et à la prévention de flux illégitimes. A la lumière de ces développements, on vérifiera notre hypothèse de recherche et on montrera que notre modèle apporte des solutions à certaines des limites des modèles de contrôle d'accès conventionnels : le contrôle de flux dans les divers scénarios d'accès à l'information. Par la suite, on proposera dans le Chapitre 7 une mise en application de certains mécanismes du modèle à travers un prototype logiciel du GBFC. Ce prototype couvrira les principales fonctionnalités du système qu'on essayera de simuler dans notre environnement de développement. Le Chapitre 8 liste certains domaines d'application de notre modèle et offre une approche critique vis-à-vis de certaines limites apparentes liées à l'implémentation du modèle avec discussions et justificatifs.

Une conclusion générale clôturera et résumera les principales contributions de ce projet de recherche et renfermera une synthèse des apports et des réalisations dans le cadre de cette thèse avec une projection sur les applications possibles ainsi que les divers horizons de recherche ouverts par cette étude.

Chapitre 2 : Positionnement du sujet

Pour mieux appréhender les concepts qui seront développés dans notre modèle de contrôle de flux basé sur la granularité, nous examinerons dans ce chapitre un exemple de référence afin d'en découler certaines notions de base sur lesquelles reposeront nos travaux de développement des mécanismes de contrôle du GBFC. Ces notions seront détaillées et analysées afin d'en cerner les différentes facettes pour une meilleure adaptation aux exigences de sécurité de flux d'informations.

2.1 Un exemple de contrôle de flux

Un pilote de chasse est appelé pour une mission confidentielle. On lui affecte un avion de chasse et une heure précise de décollage. Après décollage, la tour de contrôle lui transmet les coordonnées immédiates nécessaires pour un vol de très courte durée. Ces données sont alors fournies au pilote au fur et mesure de l'évolution du vol tout en ayant accès à d'autres données locales accessibles sur le tableau de bord de l'appareil. Les données transmises sont présentées sous forme numérique (démunies de sens compréhensible ou interprétable) du genre : longitude, latitude, amplitude, degré Est, Ouest, etc. Au fur et à mesure de l'évolution de la mission, le pilote reçoit de nouvelles coordonnées de façon graduelle. Telles coordonnées peuvent être pertinentes ou pas, par rapport à la mission elle-même. En d'autres termes, plus le niveau de confidentialité de la mission est élevé, plus on introduit dans le plan de vol des données, des instructions ou des coordonnées susceptibles de dissimuler et de noyer les données sensibles sans pour autant nuire à l'objet de la mission dont le pilote est totalement ignorant. Après une durée spécifique, souvent supérieure à la durée réaliste de la mission, on ordonne au pilote de prendre en chasse un objet spécifique en vue. Une fois la mission exécutée, on inverse le scénario pour ramener le pilote à la base. Après exécution de la mission, l'objectif a bien été atteint. Cependant, le pilote exécutant est quasiment incapable de reconstituer le plan de

vol ou de reconstituer les détails relatifs à sa mission, encore moins pouvoir les transmettre à d'autres.

Ceci serait un exemple d'un processus *sécurisé* (où les informations confidentielles sont protégées), qui renferme un ensemble de flux de données granulaires dont la totalité constitue un ensemble d'informations confidentielles reçues par un sujet. Un sujet qui se trouve dans l'incapacité de reconstituer ou de transmettre ses informations à un autre sujet. Ceci serait donc un exemple typique d'un processus de contrôle de flux d'informations réussi.

Voici quelques remarques ultérieures pour cet exemple :

1- Le contexte général de la mission est inconnu pour le sujet exécutant.
2- Le plan de vol et de la mission est indisponible dans sa totalité à tout moment pendant la mission.
3- Certaines données de la mission sont accédées par le pilote localement et ne font pas objet d'une communication (flux).
4- Les données sont fournies sur besoin, avec un souci de préserver «le moindre privilège »
5- Étant fournies sous forme fragmentaire applicable au contexte immédiat de chaque étape de la mission, les données ne sont pas exploitables dans un autre contexte et ne renferment ainsi aucune valeur transférable par le sujet. Cette forme favorise encore moins leur combinaison pour reconstituer le plan global de la mission.
6- L'existence de données non pertinentes parmi les informations de la mission rend difficile et met en doute tout effort de déductions, de reconstitution ou d'exploitation totale ou partielle du plan global de la mission.

Partant de cet exemple, on pourrait envisager un modèle dans lequel l'information confidentielle est fournie au sujet récepteur sous une forme granulaire, de façon séquentielle permettant son exploitation tout en contrôlant sa confidentialité et son flux. La Figure 3 nous permettra d'illustrer ce processus.

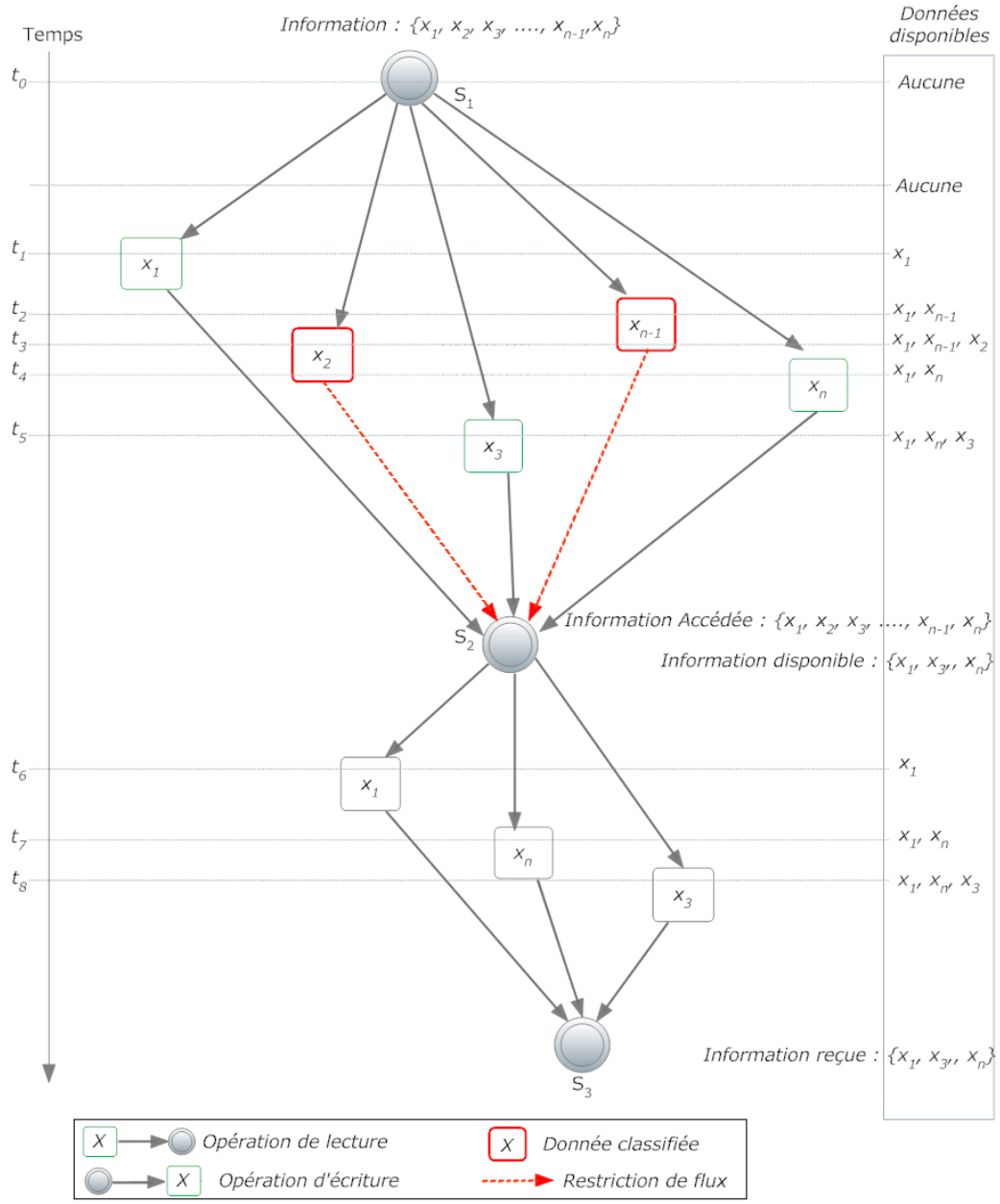


Figure 3. Processus de limitation et de contrôle de flux

Dans cette figure, un sujet S_1 qui dispose d'une information qu'il désire transmettre à un autre sujet S_2 avec un souci majeur : s'assurer du respect de la confidentialité de l'information par S_2 (aucun flux de l'information à partir de S_2).

L'information est alors répartie sous forme d'un ensemble de données granulaires. Parmi ces données granulaires certaines seulement feront objet d'un flux et par conséquent seront reçues par S_2 sous forme de données (exemple x_1, x_3, ... x_n). Les granules restants seront accédées par S_2 sans observation du flux de données (exemple x_2, ...,x_{n-1}). S_1 procède alors à une opération séquentielle d'écriture des données dans des objets accessibles en lecture par S_2. Les mêmes objets peuvent être réutilisés pour l'écriture d'autres données plusieurs fois durant ce processus.

S_2 accède et fait une lecture de façon séquentielle sur les différents objets renfermant les données granulaires et reconstitue graduellement l'information à son niveau. A la réception de la dernière donnée de S_1, S_2 aura reconstitué l'information complète sans pour autant avoir reçu qu'un ensemble limité des données granulaires la constituant. S_2 se retrouvera ainsi dans l'incapacité de réaliser un flux complet de l'information fournie par S_1 vers un sujet non autorisé S_3. Ce processus est un processus récurrent continu constitué de 3 étapes :

1- Libérer

Durant cette phase, le sujet émetteur du flux procède à une libération des objets sur lesquels il a un droit d'écriture afin de procéder à une réécriture de nouvelles données granulaires.

2- Charger

Après la première phase le sujet émetteur exécute des opérations d'écriture de données granulaires composant l'information d'origine dans les objets libérés.

3- Construire

Une fois la phase 2 achevée, le sujet récepteur du flux de données procède à la lecture des données granulaires à partir des objets renseignés et exécute une action de reconstruction de leurs éléments correspondants dans l'information intégrale. Après cette

reconstitution, l'émetteur pourra procéder de nouveau à l'exécution d'une libération des objets (*phase 1*) et ainsi de suite jusqu'à transmission complète de l'information (Figure 4)

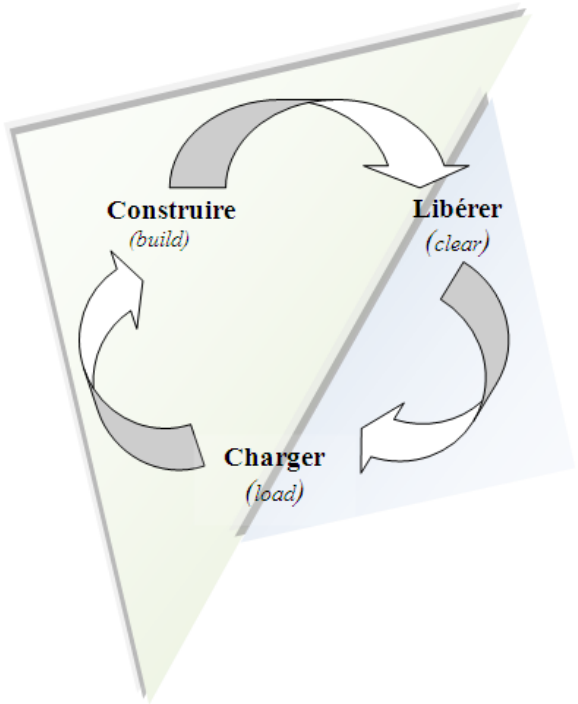


Figure 4. Processus de flux granulaire de données (LCC)

À ces trois étapes pourra s'ajouter une quatrième étape optionnelle réalisée par le sujet transmetteur qui permettra -au besoin- de renforcer davantage le niveau de sécurité:

4- Granuler

Le sujet transmetteur peut durant l'exécution du processus procéder à une re-granulation des données restantes à transmettre. Une re-granulation agit sur le niveau de granularité de données les rendant plus granulaires -plus fines de taille- et ainsi plus difficiles à regrouper et reconstituer en cas de perte ou de flux illégitime. La Figure 5 positionne cette étape dans le diagramme du processus de flux de données:

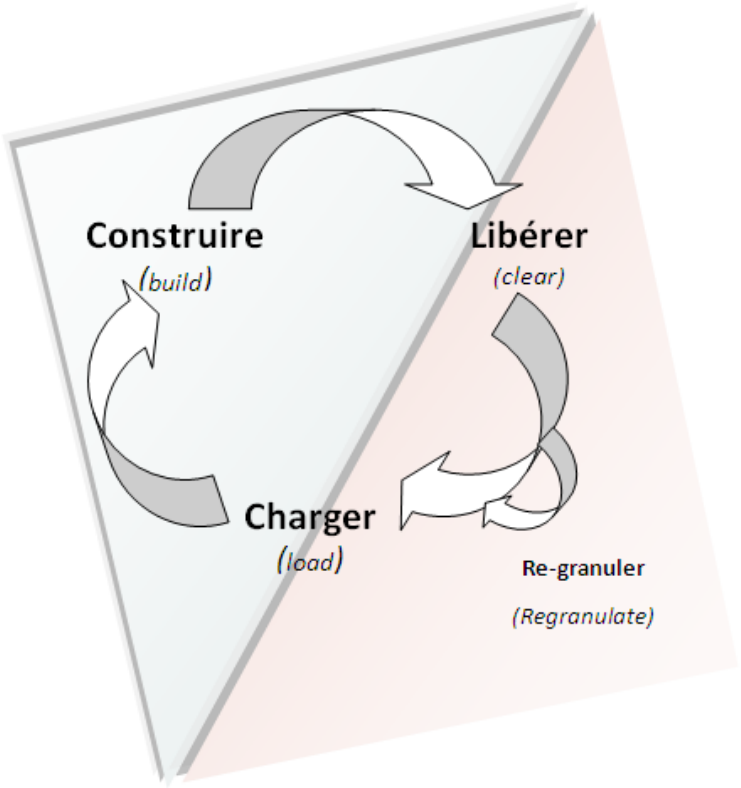


Figure 5. Processus élaboré de flux granulaire de données (LgCC)

2.2 Justification du modèle

En examinant le processus de contrôle de flux proposé, nous constatons que notre approche tente de poser un ensemble d'obstacles devant la réalisation des flux illégitimes par des sujets recevant l'information. Les 4 niveaux de difficultés sont :

1- La granularité (Contrôle du niveau de granularité)
2- L'absence de contexte (Contrôle des règles de construction)
3- Le contrôle de disponibilité et la restriction de flux
4- L'injection de bruit

2.2.1 Niveau 1- Granularité

L'information peut être manipulée à différents niveaux de détail. Le niveau de détail de l'information est généralement défini par son propriétaire ou par une instance de sécurité relativement à la valeur de l'information elle-même et aussi aux besoins des sujets qui l'utilisent. Lorsque l'information est fournie dans son intégralité (souvent sous forme de documents, fichiers ou autres, …), l'utilisateur recevant celle-ci se trouve dans une situation légitime d'accès qui lui favorise son enregistrement, sa duplication ou son transfert à des sujets qui pourraient être non autorisés. Entrainant par conséquent, un flux illégitime et une violation des règles de contrôle d'accès.

En effet, recevoir des parties des états financiers -d'une entreprise par exemple- par un agent externe représente un risque de flux illégitime moindre comparé au cas où l'intégralité de ces états sont transmis. Ainsi, on pourra proposer une manipulation de données qui décompose l'information en données élémentaires sous forme de granules. La taille de ces granules définit le *niveau de granularité* de l'information. On parle alors du niveau de granularité ou du coefficient de granularité. Prenons, par exemple, le document confidentiel présenté en Figure 6. La structure de ce document présente un certains nombre de composants qui, ensemble, constituent la valeur de l'information qu'il renferme. Ces composants permettent d'identifier le document (Code, Référence, Version, …), valider sa source (Organisation, Auteur, Reviseur, …), valider son authenticité (Classification, Instance de classification, Critères de contrôle, …), et cerner son objet et son contexte temporel et géographique (dates, lieu, …). Toutes ces informations s'ajoutent au contenu du document pour constituer la raison de sa classification.

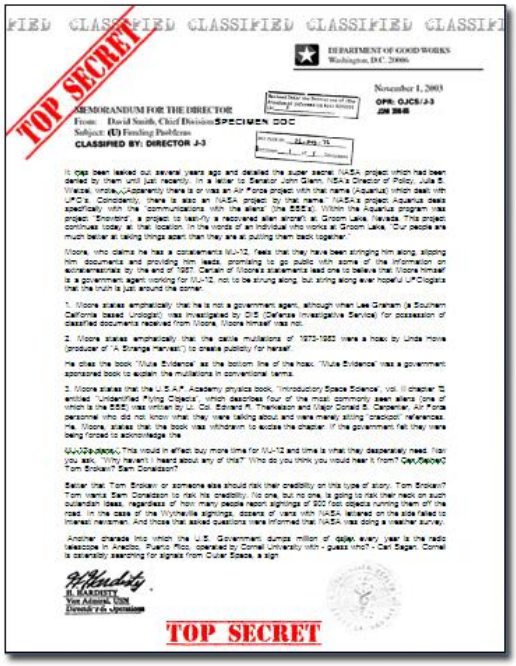


Figure 6. Image d'un document classifié TOP SECRET

Le découpage de ce document en composants plus petits engendre une granulation de son contenu similaire à la création d'un puzzle. Bien évidemment, plus petites seront les pièces (granules) de ce puzzle, plus nombreuses seront-elles et par conséquent, plus difficile deviendra sa reconstruction. La forme granulaire du document permet ainsi de rompre les liens entre ses différents composants, et de rendre chaque granule individuel démuni de sens pour le lecteur en l'absence de relations avec les autres granules du document.

La Figure 7 illustre le document confidentiel à divers niveaux de granularité allant du non granulaire (faible niveau de granularité) à gauche, au hautement granulaire (haut niveau de granularité) à droite. On distingue nettement l'accroissement du niveau de difficulté relative à la reconstitution du document d'origine proportionnellement au niveau de granularité appliqué.

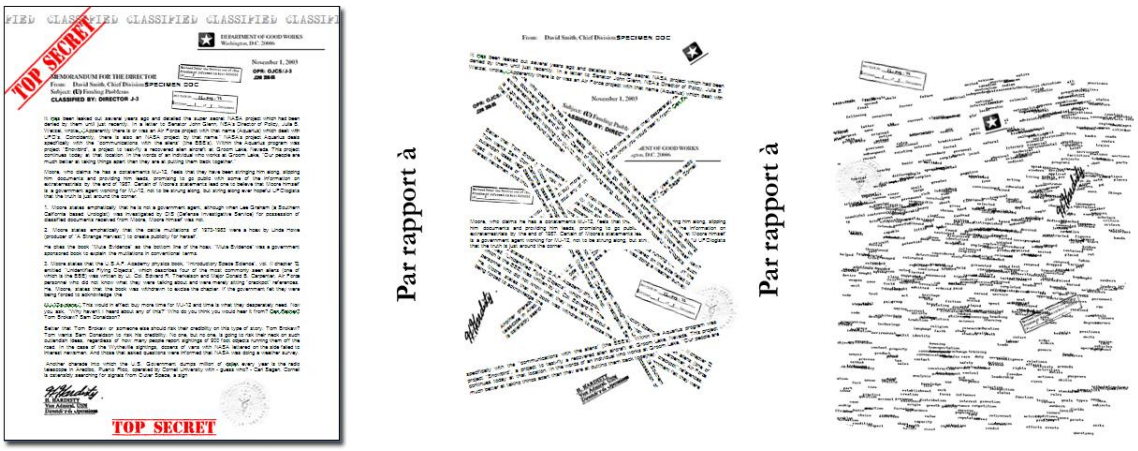


Figure 7. Niveau de granularité allant du non, à hautement granularité

2.2.2 Niveau 2- Absence de contexte

A un niveau de granularité donné, la reconstruction du document est facilitée par la connaissance préalable de son contexte général (objet, auteur, date, classification, …). Ce contexte général est similaire à l'image de référence pour la reconstitution d'un puzzle. Sans ce contexte général ou encore l'ensemble des règles de reconstruction, et avec un niveau de granularité élevé il est quasiment impossible de reconstituer un document assez long (Figure 8).

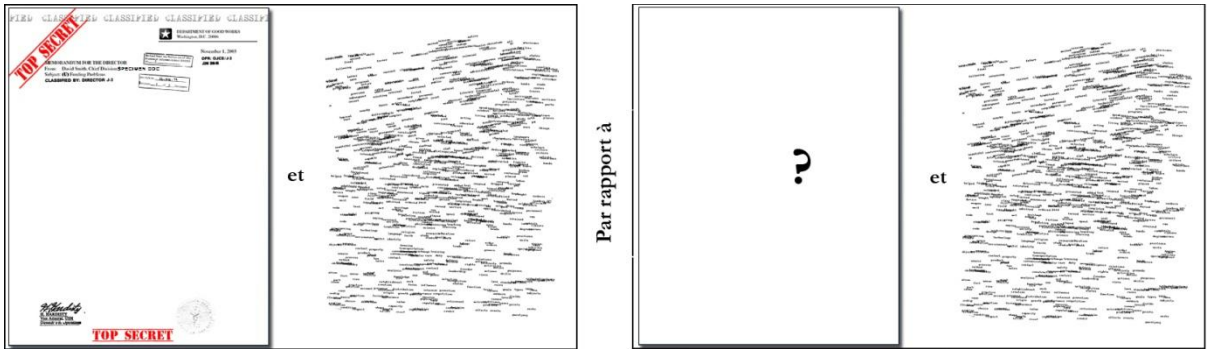


Figure 8. Niveau de difficulté de reconstruction en l'absence de contexte

2.2.3 Niveau 3- Contrôle de disponibilité et restriction de flux

Un troisième niveau de difficulté pourra être additionné au deux premiers. Considérant une information dans un état granulaire à haut niveau de granularité et en l'absence de regèles de reconstitution de l'information à partir de ces granules, on pourra envisager un

cas où les granules disponibles réunis ne sont pas en mesure de reconstituer l'information confidentielle mais seulement les parties dont un sujet a besoin à un moment donné. En d'autres termes, on ne procure pas, à un instant donné, à l'utilisateur tout l'ensemble des granules reconstituant l'information (Figure 9). Celui-ci n'est pas en mesure de savoir quels granules sont manquants à cause de l'absence du contexte vu ultérieurement, rendant ainsi la reconstitution de l'information intégrale, à un moment donné, une tâche laborieuse sinon impossible. Le contrôle de disponibilité dans notre cas est traduit par une absence de flux d'informations.

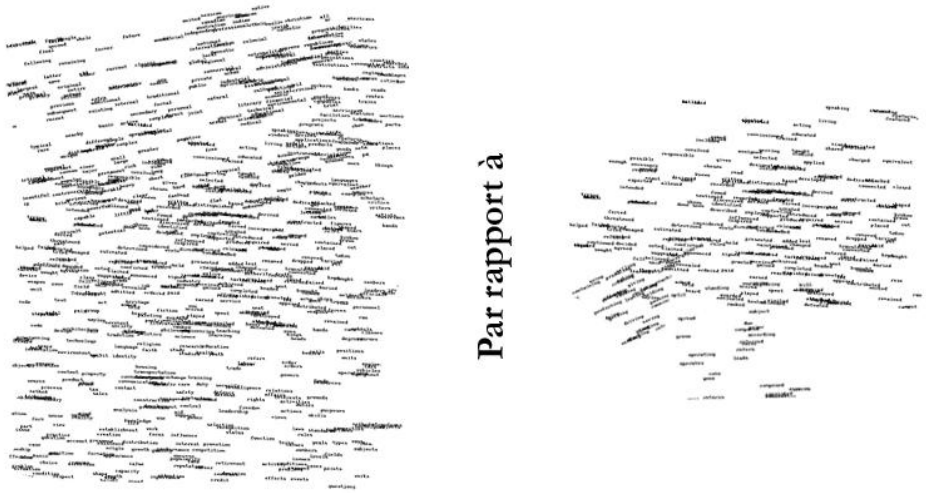


Figure 9. Niveau de difficulté de reconstruction en l'absence de granules

2.2.4 Niveau 4- L'injection de bruit

A ce niveau on continue à renforcer la confidentialité des granules d'information en introduisant des granules d'information non pertinents (bruit) choisis sur la base d'un niveau de similarité élevé par rapport aux granules pertinents. Une fois les deux ensembles de granules fusionnés, l'information confidentielle se trouve noyée dans un ensemble d'informations erronées rendant ainsi la distinction des bonnes informations de celles erronées très difficile. Les informations confidentielles sont ainsi non distinguables et non reconstituables (Figure 10).

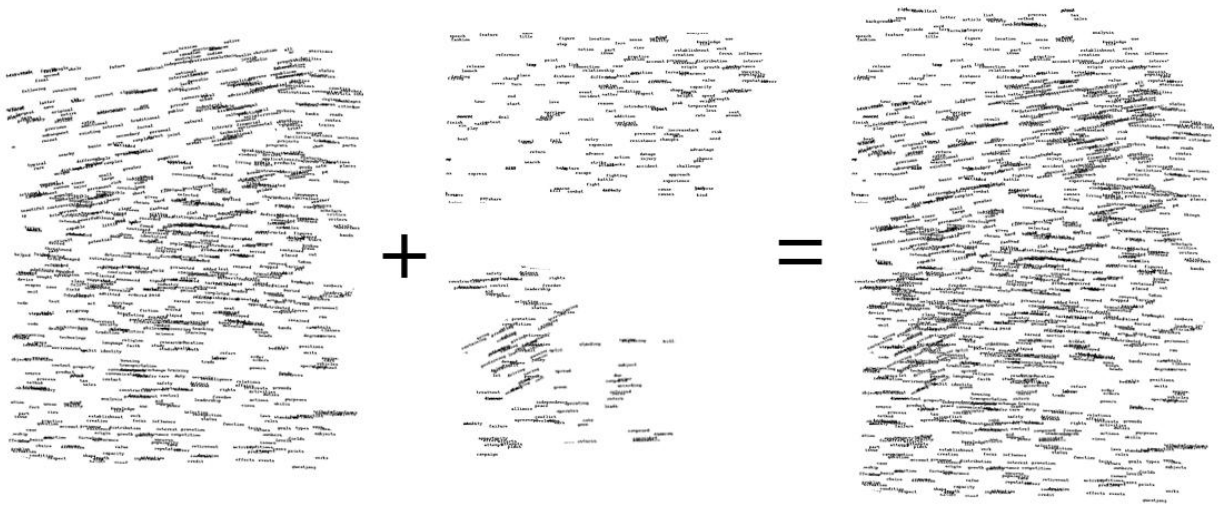


Figure 10. Injection de granules de bruit dans l'information

Ces quatre obstacles que nous venons de dresser devant tout flux illégitime d'information constituent les fondements sur lesquels on se basera pour définir notre modèle. En effet, on adoptera l'aspect granulaire de l'information pour une meilleure maitrise de la maniabilité et de la confidentialité des données. On se basera sur l'absence de contexte, le contrôle de disponibilité et la restriction de flux pour empêcher toute propagation indésirable des granules d'informations. Quant à l'injection de bruit, elle nous permettra de dissuader tout sujet malveillant d'accéder (mesure préventive) ou d'exploiter nos informations confidentielles (mesure curative).

Chapitre 3 : Sécurité et contrôle de flux d'information

Personne ne peut nier que l'information est un actif de valeur qui constitue généralement une ressource vitale pour son détenteur alors qu'elle peut d'un autre côté engendrer des conséquences parfois dramatiques et coûteuses en cas de perte ou d'accès par des sujets non autorisés. Ceci devient encore plus apparent quand on passe du niveau de l'individu au niveau de l'organisation et encore plus sensible quand des vies ou des actifs financiers de groupes sont concernés (tel les cas de gouvernements, armées, entreprises et similaires). Pour ces raisons, la sécurité de l'information a pris une place majeure dans tout type de projet ou de réalisation, et il est rare qu'on trouve un projet démuni d'une politique de sécurité de données lui étant associée.

Dans ce chapitre, on se penchera sur les définitions des concepts de base de sécurité des informations. En particulier, on traitera le processus d'identification, d'authentification et d'autorisation des sujets. On examinera aussi les principes de base de classification de l'information avec une attention particulière portée aux critères de cette classification. Nous présenterons également certains concepts fondamentaux de contrôle de flux d'informations.

3.1 La sécurité de l'information

En effet, ces politiques -parfois même stratégies- de sécurité visent principalement à assurer l'Identification et l'Authentification des utilisateurs et vérifier leurs Autorisations (IA2) tout en veillant à tout moment à la Confidentialité et au respect de l'Intégrité de l'information. Ceci, sans pour autant nuire à la disponibilité de l'information. La *sécurisation de l'information* est ainsi réalisée à travers le *contrôle d'accès* qui se manifeste en trois phases : Identification, Authentification et Autorisation.

- **Identification**

L'*identification* consiste en une sorte de preuve d'identité du sujet (utilisateur) sous forme d'information connue par l'utilisateur et qui l'identifie de façon unique par rapport au système tel qu'un numéro de compte, un nom d'utilisateur, une adresse courriel, etc.

- **Authentification**

Une fois l'utilisateur identifié par le système, celui-ci procède à la vérification de la concordance entre les informations de demande d'accès avec celles enregistrées dans sa base de données. Cette concordance concerne l'information dont le sujet dispose par rapport à celle introduite dans le système lors de la création du compte utilisateur. Cette information peut être un code, un mot de passe, une empreinte numérique ou physique, etc. et constitue la base d'*authentification* du sujet.

- **Autorisation**

Se basant sur un modèle de contrôle d'accès donné, l'*autorisation* spécifie de façon détaillée les divers droits que peut exercer l'utilisateur sur les informations ou sur les ressources du système (lecture, écriture, modification, suppression, etc.) en veillant à l'application du principe du «besoin de connaître».

Le *concept du « besoin de connaître* » désigne la décision par le propriétaire d'une information ou par une instance de sécurité d'une organisation qu'un utilisateur éventuel nécessite d'avoir connaissance ou prendre possession d'informations classifiées confidentielles pour l'exécution de tâches ou services essentiels à la réalisation des fonctions qui lui sont attribuées [18, 19].

Il faudrait noter, néanmoins, que le fait qu'un utilisateur soit identifié et authentifié dans un système n'implique pas forcement que celui-ci ait le droit d'accès aux informations de ce système [20]. La Figure 11 illustre le positionnement des trois étapes d'Identification,

d'Authentification et d'Autorisation d'un sujet par rapport à l'accès au système et aux données qu'il renferme.

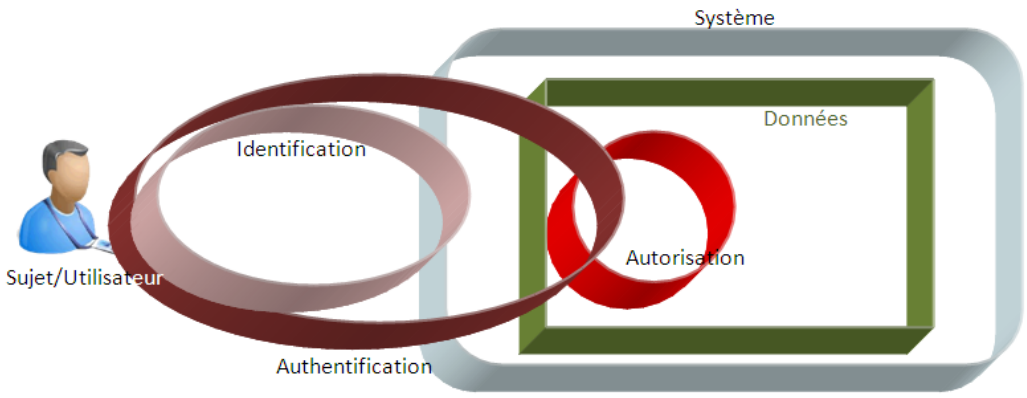


Figure 11. Sécurité et accès à l'information (IA2)

3.2 Classification de l'information

La sécurité et la confidentialité des informations a toujours été un souci majeur tant pour les individus que pour les organisations, commençant du plus petit secret de la vie privée d'une personne au plus complexe des secrets d'un État. Ceci engagea le monde de l'industrie et le monde de la recherche dans une quête continue pour de nouvelles méthodes, procédures et techniques de classification et de sécurisation des informations afin d'éviter tout accès ou flux indésirable. Une information est dite *classifiée* lorsque celle-ci nécessite une protection contre tout accès non autorisé et est marquée en conséquence pour indiquer son statut et son niveau de classification. Cette classification est généralement opérée sur des informations sous forme documentaire. Le processus inverse est connu sous le nom de *déclassification* par lequel on indique que l'information classifiée n'a plus besoin d'être protégée, ce qui se traduit par une réduction de son niveau de classification [12, 21]. Plusieurs techniques de classification des données et des informations ont vu le jour dont la plus commune est la classification en quatre groupes de niveaux de sécurité [22] qui sont déterminés comme suit :

3.2.1 Public (Public)

Une information est considérée *publique* si elle est disponible et accessible à tous. Soit, à tous les acteurs internes ou externes d'une organisation par exemple. Les informations à ce niveau sont aussi dites non-classifiées (unclassified).

3.2.2 Protégé (Protected)

Une information est *classifiée* ou encore *protégée* quand elle est jugée sensible au-delà des sujets qui en sont propriétaires ou qui y ont droit d'accès. D'où le besoin qu'elle soit protégée de tout accès externe. Les documents et communications internes aux organisations sont souvent considérés dans cette catégorie et leur accès est restreint aux instances et sujets qui ont explicitement un «besoin d'en connaitre» pour ces informations protégées.

3.2.3 Confidentiel (Confidential)

Une information *confidentielle* est caractérisée par le fait qu'elle est considérée sensible même au sein de l'instance qui l'a produite ou qui en est propriétaire et par conséquent n'est accessible qu'aux membres d'une fonction ou d'un groupe donné ou aux détenteurs de rôles spécifiques.

3.2.4 Restreint (Restricted)

Le quatrième niveau de classification restreint encore plus l'accès à l'information considérée dans ce cas secrète, voire ultra secrète accessible uniquement par des instances et sujets précis de l'organisation.

Ces niveaux de classification peuvent prendre diverses appellations et se décomposer en plusieurs sous niveaux de détail selon le secteur d'application et selon les informations sujettes à cette classification. Le tableau ci-dessous présente un exemple de cette diversité.

Info.	Niveaux de classification	Domaine des affaires	Gouvernement et militaire	Classification intersectorielle	GBFC
Non Classifiée	**Publique**	Publique	Publique Sensible non classifiée	Couleur : Blanche	Non Classifiée (U)
Classifiée	**Protégée**	Sensible	Restreinte	Couleur : Verte	Classifiée (C)
	Confidentielle	Privée	Confidentielle	Couleur : Jaune/Ambrée	Secret (S)
	Restreinte	Confidentielle	Secret Top Secret	Couleur : Rouge	Top Secret (TS)

Table 1. Correspondance des niveaux de classifications des informations

Dans le domaine informatique on retrouve cette notion, tel la classification : publique, protégée et restreinte présente en modélisation et programmation orientée objet. L'élaboration de ces niveaux de classification se base principalement sur les résultats de l'analyse des risques liés aux diverses informations dans l'organisation. Cette analyse prend en considération les risques financiers (capitaux, matériaux, …) ou humains (accidents, décès, …) liés à l'accès aux informations pour déterminer leurs niveaux de sensibilité et par la suite, le niveau de classification approprié pour leur sauvegarde [10]. De plus, ces niveaux de classification s'appliquent à la durée de vie et aux états de l'information que ce soit durant sa production, sa possession ou son utilisation. Durant toute cette durée de vie, l'information devra être sécurisée en tout temps conformément à sa classification et indépendamment de son état [9].

Pour la suite de ce projet de recherche, on adoptera la classification : Unclassified *(U)*, Classified *(C)*, Secret *(S)* et Top Secret *(TS)*.

3.3 Critères de classification

Il existe cinq critères de base pour classifier les informations, qui sont pris en considération lors de la détermination des exigences de sécurité et d'accès aux actifs d'information. Ces critères sont les suivants [23]:

- *Confidentialité*

L'organisation internationale de normalisation (ISO [24]) définit la confidentialité comme étant une caractéristique inhérente à l'information. Selon l'ISO, protéger la confidentialité de l'information revient à s'assurer que cette information disponible n'est pas divulguée à des sujets non autorisés que ce soit des individus ou des processus.

- *Intégrité*

Préserver l'intégrité de l'information veut dire protéger son exactitude et son intégralité ainsi que celle des méthodes utilisées pour l'accéder et la gérer [24].

- *Disponibilité*

Étant, en fait, l'un des objectifs et fondements d'instauration des systèmes d'information, la disponibilité des informations aux utilisateurs légitimes reste la priorité et ne devrait pas -en principe- être affectée par les autres critères de sécurité implémentés au sein du système [21].

- *Audit d'accès*

Il s'agit du suivi des transactions engendrant des accès et des transactions sur les données sécurisées ainsi que toutes les informations afférentes (date et temps, lieu, type d'accès, etc.) qui relie chaque transaction à son responsable en produisant et maintenant des rapports sur ces transactions : « Qui a fait quoi? Quand? …» [25].

- *Non-répudiation*

Souvent, généralisé ou confondu avec l'audit d'accès, ce principe empêche tout essai de l'utilisateur de se désengager par rapport à ses accès et modifications des informations.

Ceci signifie que le système veille à l'établissement de journaux auditant tous les accès et transactions opérés sur les données sécurisées. Ce principe, une fois implémenté force le maintien de traces irréversibles des transactions de l'utilisateur [21].

Les instances de sécurité au sein des organisations exigent que les informations classifiées soient protégées en tout temps. Dans certains environnements (gouvernement, militaire, ...), même certaines informations non classifiées considérées sensibles doivent être protégées et seuls les sujets autorisés peuvent y accéder et les manipuler sur la base des besoins et des exigences de sécurité spécifiés dans le système. La protection concerne le contrôle d'accès sous toute forme, la sauvegarde de l'intégrité de l'information contre toute falsification, perte ou destruction et enfin la prévention du transfert et de la divulgation aux tiers non autorisés [9].

3.4 Contrôle de flux d'informations

La plupart des organisations implémentent leurs politiques de sécurité en se basant sur trois facteurs : la classification des utilisateurs (sujets), la classification de l'information (objets) et la sécurisation des systèmes où celle-ci est manipulée (processus). Les principaux modèles de contrôle d'accès reflètent cette réalité. Cependant, et bien que ces modèles puissent limiter les droits d'un utilisateur à l'accès aux informations, ceux-ci se retrouvent limités vis-à-vis du contrôle de flux d'informations auxquelles un utilisateur a accès, que ce soit au sein du système ou au delà. Ceci se produit principalement quand le flux d'information ne s'opère pas dans une situation de violation des dispositions de la politique de sécurité.

En effet, un bon nombre de systèmes de sécurité qui sont instaurés pour veiller à l'application de politiques de sécurité se retrouvent incapables de restreindre les flux d'informations qui adhèrent à ces politiques [26].

3.4.1 Flux d'information

Selon Lowe et Manteli, il n'existe pas de définition formelle généralisée de la notion de flux d'information [27, 28, 29]. Les définitions proposées diffèrent selon les auteurs et dépendent des modèles et des concepts de sécurité adoptés telles les définitions basées sur les concepts de non-interférence ou d'indépendance, etc.

De façon générale, on dit qu'il y a *flux d'information* d'un objet O_1 de niveau de classification L_1 (source) vers un autre objet O_2 de niveau de classification L_2 (destination) au sein d'un système chaque fois que l'information stockée dans O_1 est propagée vers O_2 de façon directe ou indirecte. Ceci est normalement le résultat de l'existence d'un processus qui effectue une lecture à partir de O_1 possiblement suivie par une série de lectures-écritures et se terminant par une écriture dans O_2 [7]. Dorénavant, et pour cette recherche, on définira un *flux d'information* contenue dans un objet O_1 comme étant la propagation de cette information par une opération d'écriture dans un objet O_2. Ainsi, par exemple, un flux d'information est possible d'un objet classifié *Secret* vers un objet de classification *Top Secret* sans violation des politiques de sécurité qui autorisent ce genre d'opération. Suite à cette définition, on considère qu'un *flux d'information illégitime* se produit lorsqu'un sujet S_1 ayant accès en lecture à un objet O_2 contenant l'information classifiée arrive à reproduire cette information et l'écrire dans un objet O_3 accessible par un sujet S_2 qui ne devrait pas avoir accès à cette information. Un *flux illégitime* est ainsi un flux d'information qui viole cératines règles de sécurité appliquées à cette information. En d'autre termes : un flux qui provoque une fuite d'information vers des sujets non autorisés d'accès (voir Figure 2).

De ce fait, les techniques d'analyse et de contrôle de flux d'informations permettent la définition, la surveillance et la régulation de toute propagation d'informations entres les objets d'un système (flux internes) ou entre ces objets et ceux externes au système (flux externes) [8] dans le but de prévenir tout flux illégitime.

Il est à noter que les informations confidentielles ou classifiées peuvent se propager au-delà des utilisateurs authentifiés et par conséquent au-delà des frontières sécurisées d'un système si les politiques de sécurité des flux ne sont pas appliquées et maintenues. Pour cette raison, le contrôle de flux est d'une importance cruciale. Le contrôle de flux empêche également la circulation d'informations indésirables ou erronées à des niveaux stratégiques et décisionnels d'une organisation, par la protection de l'intégrité des données [29]. Le contrôle de flux est mis en œuvre grâce à des politiques de confidentialité et à travers différents mécanismes qui appliquent une sécurité de bout en bout [30].

Le premier modèle de flux d'information largement reconnu a été proposé par Denning en 1976 [31]. Un flux d'information $L_1 \mapsto L_2$ entre deux objets de classes de sécurité L_1 et L_2 est possible, si et seulement si l'information dans l'objet de classe L_1 est autorisée à se propager dans l'objet de la classe L_2. Pour qu'un modèle de flux soit considéré sécurisé, toute exécution d'une séquence d'opérations ne peut pas produire un flux qui viole la relation "↦" [31, 32, 27].

3.4.1.1 Types de flux d'information

Il existe deux principaux types de flux d'informations : flux directs et flux indirects [31, 33].

Un flux d'informations est *direct* ou *explicit* quand il s'opère directement entre le sujet propriétaire ou détenteur de l'information et d'autres sujets. Ce type de flux est généralement légitime considérant qu'il se déroule sous contrôle du sujet détenteur de l'information et requiert une autorisation explicite de sa part. Un flux direct se manifeste généralement sous forme d'affectation de variables (a = b) ou d'opération de lecture/écriture (sauvegarde, impression, …).

Un flux indirect ou implicite se produit lorsque l'information circule entre des sujets autres que le propriétaire ou le détenteur de l'information [27, 34] avec ou sans son

consentement préalable. Le flux d'information indirect entre les sujets peut être limité par propagation ou révocation des droits d'accès tels que les droits de lecture ou d'écriture, etc. Une autre forme de flux implicite se manifeste sous forme de structures conditionnelles ou de boucles. Par exemple le code suivant renferme un flux d'information implicite du fait que, dépendamment de la valeur de *b*, on peut déduire si la valeur de *a* est supérieure à zéro ou non [3].

si a>0
alors b :=nul;

Généralement, les fuites d'informations confidentielles sont plus probables dans les cas de flux indirect tel que présenté dans la Figure 2, où des informations confidentielles sont transférées à des sujets non autorisés soit délibérément ou à la suite d'erreurs.

3.4.1.2 Problème de fuites d'informations

Une *fuite d'information* est un *flux d'information illégitime* d'un sujet (émetteur) ayant droit d'accès à l'information à un autre sujet (récepteur) non autorisé. Ce flux est initié par le sujet émetteur qui exécute une lecture de l'information à partir de l'objet qui la contient suivie d'une écriture de cette information dans un deuxième objet que le sujet récepteur accède en lecture. Dans une situation de fuite d'information deux principaux scénarios sont envisageables :

1- Un sujet non autorisé tente d'accéder à des informations confidentielles auxquelles il n'a pas droit d'accès (espionnage, erreur, curiosité, …).
2- Un sujet autorisé transmet, de façon délibérée on non, des informations confidentielles auxquelles il a droit d'accès à un sujet non autorisé (agent espion, erreur, perte de contrôle ou de matériel, ...).

Une information enregistrée sur un ordinateur peut être accédée par des processus qui représentent des instances d'exécutions de programmes exécutés par les usagers. Ces processus héritent ainsi des droits d'accès dont dispose le sujet qui les a déclenchés [35].

Ces processus peuvent provoquer des fuites d'informations vers d'autres processus ou objets et par conséquent à d'autres sujets non autorisés. Le problème soulevé par ce genre de fuites illégitimes d'informations est généralement connu comme le *problème de confinement*. Généralement, les fuites d'informations exploitent des mécanismes de transfert illégitimes d'informations confidentielles dont les canaux cachés (présentés en détail dans la Section 3.4.1.3 de ce chapitre), les chevaux de Troie, les programmes espions et autres.

Les fuites d'informations peuvent aussi surgir de l'observation des signaux électromagnétiques émis ou transférés par ou via les composants physiques (câbles, périphériques, technologies sans fil, …) des ordinateurs ou du réseau [36]. Nous verrons dans le Chapitre 5 que notre modèle arrive à résoudre ce genre de problèmes bien que non couverts directement par cette recherche.

Bien que ces mécanismes malveillants représentent une menace sérieuse pour des postes de travails isolés, leur danger est encore plus amplifié en présence de réseaux de communication et de données ouverts sur l'Internet [37]. Les modèles de sécurité classiques traitent certains de ces problèmes de fuites d'informations (chevaux de Troie par exemple) mais sont vulnérables devant la majorité de ces menaces.

3.4.1.3 Canaux cachés (Covert channels)

Les canaux cachés ont été définis pour la première fois par Lampson en 1973 [38] comme étant des canaux de communication non destinés au transfert ou au flux d'aucun genre d'informations. C'est un mécanisme par lequel un processus classifié de haut niveau de sécurité déclenche une fuite d'informations confidentielles vers un processus de bas niveau de sécurité qui ne devrait pas y avoir accès [37].

Lampson liste un ensemble de canaux qui peuvent être utilisés pour ce genre de flux illégitime. La première catégorie de canaux regroupe les canaux légitimes généralement

utilisés par les programmes pour le transfert de données (impression, ports réseaux,…). Ces canaux sont en principe supervisés par les mécanismes de sécurité du système mais peuvent toutefois servir à des fuites d'informations confidentielles après des procédés de réorganisation ou de reformatage. Le deuxième type de canaux est exploité par un programme pour l'enregistrement et la sauvegarde de données. Il s'agit de fichiers temporaires et de variables partagées qui peuvent servir pour des flux illégitimes entre processus. Il s'agit de canaux de stockage. Les derniers canaux sont des canaux cachés qui ne sont généralement pas désignés pour cheminer des flux d'informations mais qui peuvent être exploités pour passer des informations de façon illégitime entre processus. Un exemple est l'utilisation d'une série ordonnancée de *pings* pour signaler la présence ou le contenu d'informations confidentielles. Le déchiffrement de l'ordonnancement par le processus destinataire permet d'inférer le contenu de l'information. Généralement, ces canaux reposent sur l'observation de comportements agencés dans le temps (canaux temporels) [39].

3.4.2 Contrôle de flux

Comme mentionné précédemment, un flux d'information d'un objet O_1 vers un objet O_2 a lieu lorsque, suite à une série d'instructions de lecture/écriture, un sujet arrive à lire l'information de l'objet O_1 et l'écrire dans O_2. Un exemple courant serait la copie de texte d'un fichier dans un autre fichier.

La recherche sur le contrôle de flux date des années 70. Généralement, le contrôle de flux se base sur le concept de classification qui permet à un flux d'exister d'un sujet de classe L_1 vers un autre sujet de classe L_2 seulement lorsque la classe L_2 est supérieure à L_1 ou du moins est du même niveau (L_2 domine L_1). Par exemple un flux d'un sujet de classe SECRET vers un sujet de classe TOP SECRET. De cette façon, le contrôle de flux permet d'empêcher les fuites d'informations confidentielles vers des sujets non autorisés par le biais du contrôle de la manière dont se propagent les données dans les programmes et les processus à l'exécution [40, 41].

Le contrôle de flux d'informations est généralement une extension au contrôle d'accès. En effet, les informations confidentielles dans un système qui implémente une politique de sécurité sont considérées sécurisées tant que cette politique n'est pas violée. Par conséquent, cette même information est théoriquement considérée protégée lors d'un flux tant qu'on peut confirmer que celle-ci ne peut pas outrepasser les frontières du système où la politique de sécurité est appliquée et maintenue. Soit, l'information est empêchée de se propager à un endroit où cette politique est violée. De ce fait, le contrôle de flux se voit maintenu via les mécanismes de contrôle d'accès avec comme préoccupation majeure la garantie de sécurité point à point. Ainsi, des politiques de flux ont été développées et implémentées afin de définir, réguler et sécuriser les flux d'informations au sein d'un système de sécurité et vis-à-vis de systèmes environnants [42, 8]. Il est aussi à noter que l'un des objectifs majeurs du contrôle de flux est la protection de la vie privée [16].

Dans un système de sécurité, le contrôle de flux d'informations permet de gérer et surveiller les types d'informations qui circulent dans le système ainsi que le processus de propagation de celles-ci d'un sujet à un autre. Généralement, ceci se fait de façon centralisée par le biais de classifications des sujets et objets du système avec un renforcement du contrôle des canaux de propagation utilisés pour le flux entre différentes classes. En d'autre terme, le contrôle de flux se réalise en tant qu'activité subséquente au contrôle d'accès. Chose qui n'est pas suffisante du fait que le contrôle d'accès souffre de faiblesses majeures à assurer le contrôle de flux dont certaines sont listées en Section 4.4 du Chapitre 4.

A la fin de ce chapitre, il reste à souligner qu'il existe généralement une relation de concurrence entre la sauvegarde de confidentialité de l'information et l'assurance de sa disponibilité. Ceci constitue souvent le défi majeur des modèles de sécurité comme on le constatera dans notre analyse dans le Chapitre 4. Notre modèle cherchera à garantir un niveau de confidentialité fiable tout en veillant à l'assurance d'un niveau acceptable de disponibilité des informations.

Chapitre 4 : Modèles de sécurité et contrôle de flux : état de l'art

La confidentialité et l'intégrité de l'information ont bel et bien été, et demeurent des préoccupations majeures pour les organisations. Ces préoccupations ont incité à l'instauration de règles et de lois destinées à veiller sur la protection de tout accès illicite ou de toute altération ou mauvais usage de l'information en cas d'accès légitime.

Ces règles ont pris plusieurs formes, du plus simple cadenas sur une armoire renfermant des documents sensibles, au plus sophistiqué des algorithmes de cryptage de nos jours. Cependant, le défi demeure à relever vu que l'information devient un outil majeur de prise de décision, souvent collective, engageant plusieurs acteurs. D'où le besoin de garantir la disponibilité de l'information sans pour autant détériorer son niveau de sécurité. Pour cela, plusieurs modèles ont été élaborés afin de garantir la disponibilité de l'information tout en préservant sa confidentialité et son intégrité.

Dans ce chapitre, nous présenterons les concepts de base de politiques de sécurité et nous examinerons les principaux modèles de contrôle d'accès en accordant une attention particulière aux apports et aux limites de chacun relativement au contrôle de flux d'informations. Un bref survol de l'informatique granulaire et de son exploitation dans le domaine de sécurité des données clôturera cette partie.

4.1 Politiques et modèles de sécurité

Il faudrait tout d'abord cerner les principaux concepts liés à la sécurité de l'information avant de traiter les différents modèles. Ainsi, il faudrait distinguer entre politique de sécurité et modèle de sécurité.

En effet, une *politique de sécurité* est un ensemble de règles et de directives qui fixent la manière dont les informations confidentielles sont gérées, protégées et distribuées au sein d'une organisation [43, 13]. Elle est représentée sous forme de documents qui décrivent de façon générale les divers objectifs que les dispositifs de protection des informations sont censés atteindre. Ces descriptions devront être claires et précises et couvrir les domaines où la sécurité doit être renforcée pour atteindre les objectifs abstraits de sécurité sans se soucier des procédures à implémenter pour les réaliser. Une politique de sécurité spécifie également les canaux que les informations peuvent emprunter lors d'un flux [40].

Un *modèle de sécurité*, généralement désigné : *modèle de contrôle d'accès*, est un système abstrait qui peut être utilisé pour représenter formellement des politiques de contrôle d'accès. Généralement, un modèle de sécurité est conçu sous forme de concepts mathématiques ou analytiques [22]. Les modèles de contrôle d'accès sont exprimés à des niveaux d'abstraction permettant leur adaptation à une grande variété de choix d'implémentations et d'environnements informatiques, tout en fournissant un cadre conceptuel d'analyse de ces politiques de sécurité [44].

La mise en application du modèle se fait à travers des *architectures* qui permettant de représenter de façon concrète et détaillée les techniques informatiques et les structures de données nécessaires à implémenter le modèle dans un système d'information (modèle concret). Cette concrétisation se fait par la définition et l'octroi des droits d'accès et des autorisations afin de permettre tout accès des sujets aux systèmes, aux ressources et aux applications [22].

Des *mécanismes* de conception et de programmation permettent par la suite de traduire les directives de l'architecture en commandes et processus permettant de résoudre des problèmes particuliers de sécurité de l'information [13]. Généralement, les modèles de contrôle d'accès et leurs mécanismes d'implémentation sont caractérisés en termes des politiques qu'ils supportent [44].

Par exemple, si une politique de sécurité stipule que certains objets ne devraient pas être accessibles par certains sujets, le modèle de sécurité serait celui qui fournit les concepts abstraits mathématiques et logiques pour pouvoir implémenter cette politique de contrôle d'accès. L'architecture de sécurité vient traduire ces concepts en procédures informatiques concrètes et détaillées permettant par la suite d'implémenter des mécanismes physiques et logiques capables d'appliquer ces règles au niveau du système d'information (Figure 12).

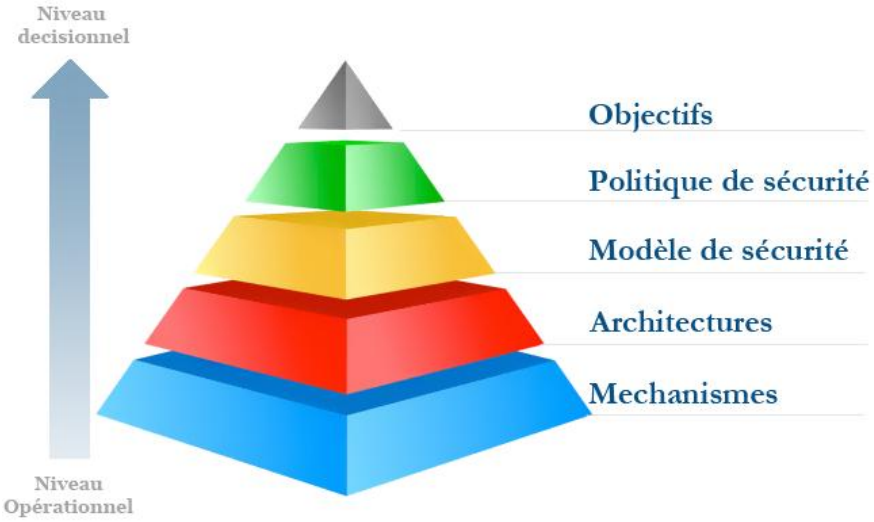


Figure 12. Politiques et modèles de sécurité

4.2 Modèles de flux d'information

Les modèles de flux d'information ont été introduits pour la première fois par Denning en 1976 [45] et veillent à ce qu'une information qui subit un flux d'une classe de sécurité à une autre obéit aux relations de flux prédéfinies dans le système [36].

Dans cette famille de modèles, l'information est manipulée à travers les différents objets qui la renferment et subit un flux sur la base de sa classification et tenant en considération les droits d'accès et les autorisations des sujets utilisateurs. Les principaux modèles de cette famille sont les modèles d'accès obligatoires (Bell-LaPadula, Biba, etc.) [46], les modèles de non-interférence ou d'indépendance [47], certains modèles réseaux basés sur les treillis

[31, 32], ainsi que d'autres applications spécifiques (sécurité de bases de données [48], canaux cachés [49, 50, 51], etc.).

Un modèle de contrôle de flux a 5 principales composantes [31]:

- un ensemble d'objets utilisés pour recevoir les données
- un ensemble de sujets participant au flux
- un ensemble de classes de sécurité pour designer les droit d'accès et les autorisations
- un operateur de combinaison entre classes de sécurité pour valider les opérations d'accès
- une relation de flux qui détermine la possibilité de présence de flux entre deux classes de sécurité de données.

Un exemple sera une tentative de transfert (relation de flux) d'un fichier (objet) confidentiel (classe de sécurité de l'objet) transféré par un utilisateur S_1 (sujet 1) de niveaux d'autorisation L_1 (classe de sécurité du sujet 1) vers un autre utilisateur S_2 (sujet 2) de niveaux d'autorisation L_2 (classe de sécurité du sujet 2) au sein d'un système qui stipule que pour que ce flux soit valide la classe de sécurité du sujet S_2 doit être supérieure ou égale à la classe de sécurité du sujet S_1 : $L_2 \geq L_1$ (operateur de combinaison entre classes de sécurité). On pourra représenter ainsi une *relation de flux* sous forme d'un tuple : $F_r<S, O, L, Op>$.

Ainsi, un contrôle de flux vise à garantir que tout flux d'informations entre deux sujets donnés via des objets donnés ne se trouve pas dans un état de violation de la relation de flux [36]. Dans ce modèle on remarque que la protection des informations confidentielles de flux illégitimes se fait à travers l'application des mesures de sécurité aux sujets et aux objets manipulant cette information sans aucun renforcement de cette sécurité au niveau de l'information elle-même. Ceci se manifeste dans les systèmes d'information sous forme de protection des structures de données renfermant les informations confidentielles tels les fichiers, les variables, etc. Ainsi, par exemple, pour protéger les informations confidentielles contenues dans un fichier, les instances de sécurité dans l'organisation

appliquent des mesures de sécurité sur le fichier du genre classification, règles d'accès, protection par mot de passe et ainsi de suite. Cependant, une fois le fichier accédé par un sujet, les informations confidentielles se retrouvent à risque vu que la barrière de sécurité du fichier a été franchie et qu'il n'existe généralement aucune autre mesure de sécurité appliquée aux informations qu'il contient en tant qu'entités à protéger.

4.2.1 Modèle de non-interférence

Le modèle de non-interférence [52], souvent synonyme du modèle de non-inférence ou encore d'indépendance, est un modèle théorique de sécurité multi-niveaux qui veille à ce qu'au sein d'un système une action d'un utilisateur quelconque n'a aucun effet sur ce que peut voir un autre utilisateur du système sous forme d'extrants. En d'autres termes, prévenir toute possibilité de dériver une information de haut niveau de classification à partir d'une information de moindre niveau de classification. Ainsi, lorsqu'un sujet d'un niveau de sécurité supérieur exécute une action, cette action ne devrait pas avoir d'impact sur l'état d'entités de niveau de sécurité inférieur. Le modèle classique de non-interférence se préoccupe essentiellement de ce que sait l'utilisateur sur l'état du système, soit la visibilité des informations confidentielles que les divers événements introduisent dans le système [56]. La finalité de ce modèle est de distinguer les flux d'informations légitimes autorisés (généralement d'un niveau de sécurité bas vers haut) de ceux illégitimes et interdits (généralement de haut vers bas) se basant sur les relations entre les sujets dans un système de sécurité [53]. De ce fait, c'est un modèle qui a pour but d'empêcher les flux d'informations confidentielles au delà du domaine auquel elles sont confinées à travers l'analyse des états du système [54].

4.3 Modèles de contrôle d'accès

Il existe différents types de modèles de sécurité dont le souci majeur est de veiller au respect des exigences de confidentialité, de disponibilité, d'intégrité et de non répudiation de l'information [46]. Ces modèles peuvent être catégorisés de différentes façons et en différents groupes dépendamment de leurs caractéristiques communes. Ces groupes sont

aussi présents dans l'évolution des modèles de contrôle d'accès depuis les années 70 à nos jours. En effet, ils sont passés de simples modèles couvrant une seule organisation avec une gestion mono-utilisateur sous une autorité de sécurité unique vers des modèles supportant multiples organisations, une multitude d'utilisateurs et un contrôle par plusieurs autorités. Selon cette évolution on est passé d'un accès direct d'un sujet à un objet se basant sur son identité vers un accès indirect à travers des rôles attribués à ce sujet. Cela s'est manifesté par une chronologie d'évolution des principales familles de modèles de contrôle d'accès. On a eu donc des modèles basés sur l'identité, puis basés sur les règles, ensuite basés sur les rôles et finalement basés sur les attributs. La Figure 13 illustre cette évolution.

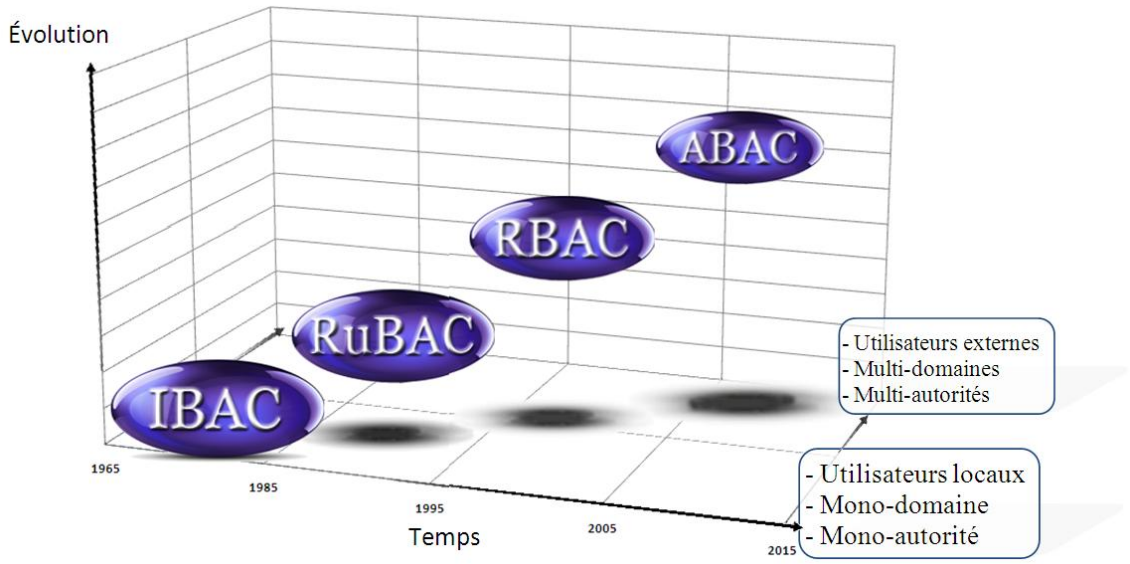


Figure 13. Évolution des modèles de sécurité

4.3.1 Modèles de contrôle d'accès basé sur l'identité (IBAC)

Cette catégorie renferme les modèles qui se basent principalement sur l'identification des sujets pour permettre l'accès aux informations ou aux ressources. Cette famille de modèles se base sur des concepts relativement simples à comprendre et à implémenter [55]. Les premières générations de modèles d'accès font partie du IBAC (Exemples : MAC, DAC, …). Les modèles basés sur l'identité requièrent une connaissance préalable et

explicite de tous les utilisateurs potentiels pouvant avoir accès aux objets et par conséquent à l'information [19] .

Vu l'incapacité de cette famille de modèles à suivre l'évolution des besoins d'accès (accès réseaux, groupes, systèmes distribués, ...) en plus de la difficulté de sa gestion, plusieurs mises à jours ont été introduites en plus de nouveaux modèles tel RBAC [56]. Les modèles DAC et MAC sont présentés en détail dans les Sections 4.3.1.1 et 4.3.1.2 de ce chapitre.

Les modèles de contrôle d'accès basé sur les règles (RuBAC), les modèles de contrôle d'accès basé sur les rôles (RBAC) et les modèles de contrôle d'accès basés sur les attributs (ABAC) sont présentés respectivement dans les Sections 4.3.2, 4.3.3 et 4.3.4.

4.3.1.1 Modèle de contrôle d'accès discrétionnaire (DAC)

Alors que les modèles de contrôle d'accès obligatoire renforcent le contrôle d'accès de façon centralisée qui empêche l'utilisateur de manipuler ses autorisations et ses droits d'accès, on retrouve à l'opposé le *modèle de contrôle d'accès discrétionnaire* (DAC). Le modèle discrétionnaire se différencie par le fait qu'il est moins restrictif en accordant à l'utilisateur propriétaire de l'information le pouvoir et la discrétion de gérer les droits d'accès aux objets selon ses exigences. Il peut par la suite propager et octroyer ces droits à d'autres utilisateurs y compris les droits de modification et de propagation des privilèges et d'autorisations d'accès. Ainsi, un administrateur de compte peut octroyer des droits d'accès à un autre utilisateur tout en lui permettant à son tour de faire de même et gérer les droits d'accès ou les propager à un troisième utilisateur [46]. C'est un modèle où la gestion de sécurité est orientée utilisateur et qui est très répandu à cause des avantages qu'il offre. En effet, le modèle DAC est un modèle simple et flexible avec une grande facilité d'implémentation.

Il y a eu plusieurs généralisations et variations de ce modèle, entre autres le modèle Harrison-Ruzzo-Ullman [57]. Il est à souligner que le principal inconvénient du DAC est que ce modèle ne garantit pas le contrôle de flux d'informations en raison de la propagation des droits d'accès qui est contrôlée par les utilisateurs [35]. De plus, les systèmes implémentant ce modèle sont assez vulnérables aux attaques de programmes malveillants (Chevaux de Troie par exemple) qui peuvent compromettre le compte de l'utilisateur et s'octroyer ses droits d'accès et avoir ainsi le contrôle sur les informations permettant leur diffusion à des tiers non autorisés [46]. On retrouve le modèle de contrôle d'accès discrétionnaire, le plus souvent, dans les systèmes d'exploitation, les systèmes de gestion de bases de données et autres systèmes d'information qui laissent le souci de la sécurité aux usagers.

4.3.1.2 Modèles de contrôle d'accès obligatoire (MAC)

Comme mentionné dans la section précédente, les *modèles de contrôle d'accès obligatoire* (MAC) sont des modèles restrictifs dans lesquels le contrôle d'accès est géré de manière centralisée par l'administrateur ou par les instances de sécurité du système. Ce sont des modèles multi niveaux qui spécifient les différents niveaux de sécurité et réglementent les modes de flux d'informations entre eux. Ils se préoccupent aussi bien de la confidentialité de l'information que de son intégrité [58, 46].

Les utilisateurs dans ces modèles dépendent d'instances administratives pour leur accorder les droits d'accès aux ressources et fichiers du système ou pour modifier ces droits. C'est pour cette raison qu'on retrouve ces modèles plus fréquemment dans des organisations où le contrôle d'accès est critique et les données souvent hautement sécurisées : tel le domaine militaire. Ces restrictions sont implémentées par un mécanisme d'étiquetage qui attribue des étiquettes de sécurité permettant de classer les sujets et les objets du système respectivement selon leurs autorisations (*Ang. clearance*) et leurs classifications (*Ang. classification*). On adoptera la notation L_S et L_O pour designer respectivement la classe d'un sujet S et d'un objet O et la notation L pour désigner une

classe de sécurité en général. Cette opération de classification permet de prévenir tout flux indésirable entre sujets et objets de classes sécuritaires non adéquates [59]. MAC est ainsi l'un des plus anciens modèles de contrôle de flux dans les systèmes d'informations. Le modèle de contrôle d'accès obligatoire est aussi considéré par certains auteurs comme un modèle d'accès basé sur les règles (Rule Based Access Control RuBAC) [26] et est aussi implémenté dans les systèmes d'exploitation qui utilisent des étiquettes de sécurité pour gérer les privilèges des utilisateurs et les droits d'accès aux objets et aux ressources. Les modèles MAC ont été les premiers modèles à instaurer des mécanismes de contrôle de flux en implémentant les règles de circulation de l'information entre les différentes classes [46].

La forme la plus répandue de contrôle d'accès obligatoire est celle des modèles de sécurité multi-niveaux (MLS) qui se basent sur la classification des sujets et des objets d'un système selon plusieurs niveaux de sécurité [17]. Les modèles MLS sont axés sur la gestion des flux d'information et sont implémentés en pratique dépendamment des objectifs de la politique de sécurité sur la base de différents scénarios et contextes. On retrouve les modèles multi-niveaux le plus souvent implémentés au sein des systèmes militaires. Les principales implémentations sont : le modèle de confidentialité de Bell-LaPadula (BLP), les modèles d'intégrité Biba et Clark-Wilson et le modèle de Brewer-Nash aussi connu sous le nom de « Muraille de Chine » [60]. Parmi ces modèles, certains sont des modèles statiques et s'appliquent à des environnements où les critères de sécurité sont stables et statiques dans le temps tel les modèles BLP et Biba décrits ci-dessous. D'autres sont dynamiques et répondent au besoin d'un changement plus fréquent et dynamique des droits d'accès tel que dans le modèle Muraille de Chine.

Le but fondamental des modèles MAC est d'assurer non seulement le contrôle d'accès direct mais aussi le contrôle d'accès indirect, c'est-à-dire le contrôle de flux.

4.3.1.2.1 Modèle de confidentialité de Bell-LaPadula

Le *modèle de Bell-LaPadula* est un modèle de sécurité multi niveau centralisé de la famille MAC qui renforce la confidentialité. Il a été proposé par D. Elliott Bell et Leonard

J. LaPadula [61] dans le but de renforcer la confidentialité des informations dans le secteur militaire. Ce modèle restrictif est conçu pour prévenir toute transmission d'informations confidentielles de sujets de haut niveau de sécurité vers des sujets de moindre niveau tout en empêchant la lecture dans le sens inverse (No write down/No Read up). En effet ce modèle est basé sur deux propriétés de sécurité [62]:

- ***Propriété de sécurité simple*** : qui stipule qu'un sujet *S* est autorisé de lire un objet *O* uniquement si la classe de sécurité de *S* domine ou équivaut la classe de *O* : $L_S \geq L_O$.

- ***Propriété * (étoile)*** : cette deuxième propriété est satisfaite lorsqu'on s'assure que si un sujet *S* a droit d'accès en lecture d'un objet O_1 et a droit d'accès en écriture dans un objet O_2 alors cela implique que la classe de O_2 domine ou équivaut la classe de O_1 ($L_{O2} \geq L_{O1}$). En d'autres termes, aucune écriture n'est permise vers le bas (dans le sens décroissant du niveau de sécurité).

Ainsi, le modèle permet la production d'informations destinées aux niveaux supérieurs de sécurité par des sujets de niveaux inferieurs sans pour autant que ces derniers aient la possibilité de lire des informations de plus haut niveau de sécurité (Figure 14). Ceci est réalisé via l'application de classifications des sujets et des objets selon plusieurs niveaux de sécurité [44, 63]. BLP applique le contrôle de flux d'informations entre les différents niveaux de classification sur la base du concept du « besoin de connaître » présenté plus haut. Ce modèle présente un problème majeur de conservation d'intégrité vu la possibilité pour les sujets de bas niveau de sécurité de modifier les informations destinées aux niveaux de sécurité supérieurs [60]. De plus, le modèle de Bell-LaPadula est vulnérable aux canaux cachés [63].

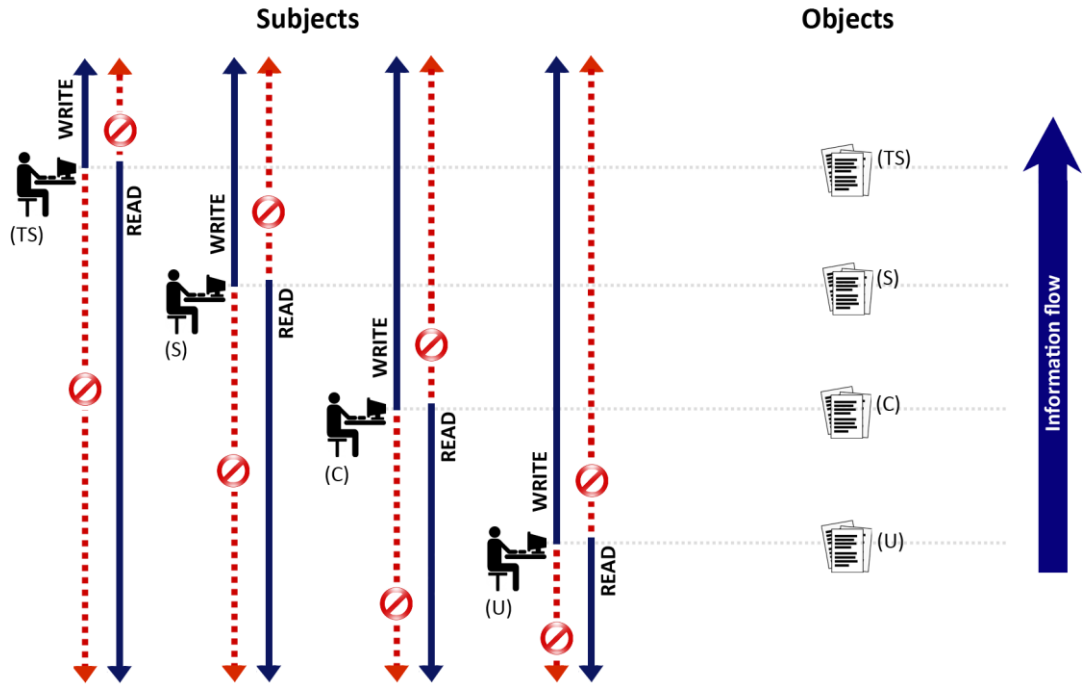


Figure 14. Modèle de confidentialité BLP

4.3.1.2.2 Modèle d'intégrité Biba

Pour remédier au problème de protection d'intégrité des informations du modèle BLP le *modèle Biba* [64] a été développé. Similairement au BLP, ce modèle est un modèle multi-niveaux qui se base sur la classification des sujets et des objets pour renforcer l'intégrité des informations et le contrôle de flux entre les différentes classes d'utilisateurs. Dans ce modèle, chaque sujet et chaque objet du système se voit assigné une classe d'intégrité généralement définie comme Haut (H), Moyen (M) ou Faible (L). Le niveau d'intégrité d'un objet définit le niveau de sécurité nécessaire pour son accès. Le niveau d'intégrité (classification) d'un sujet détermine son niveau de confiance pour écrire, modifier ou supprimer le contenu d'un objet.

Le modèle Biba implémente deux règles d'intégrité qui empêchent un sujet de lire des informations d'objets de moindre niveau de sécurité *(pas de lecture vers le bas)* et de réaliser des opérations d'écriture dans des objets de niveau de classification supérieur *(pas d'écriture vers le haut)* comme représenté dans la figure 15.

Pour conserver l'intégrité des informations le modèle d'intégrité Biba vérifie l'exactitude de toutes les opérations d'écriture sur un fichier. Toutefois, cette approche présente une faiblesse de sécurité résultant de la possibilité d'inférer des informations de haut niveau à partir d'informations de bas niveau [60]. Ce modèle, de son côté, repose sur deux propriétés pour assurer l'intégrité des informations :

- ***Propriété d'intégrité simple*** : dans laquelle est fixé qu'un sujet *S* ne peut lire un objet de classe de sécurité inferieure à la sienne. En d'autres termes, si la classe de sécurité de *S* domine la classe de *O* ($L_S > L_O$) cela implique que *S* ne peut lire *O* (pas de lecture vers le bas) [17, 65].

- ***Propriété * (étoile)*** : qui stipule qu'un sujet *S* n'est pas autorisé de modifier ou d'écrire dans un objet *O* de classification supérieure. Ainsi, si la classe de sécurité de *O* domine la classe de *S* ($L_O > L_S$) cela implique que *S* ne peut écrire ou modifier *O* (pas d'écriture vers le haut).

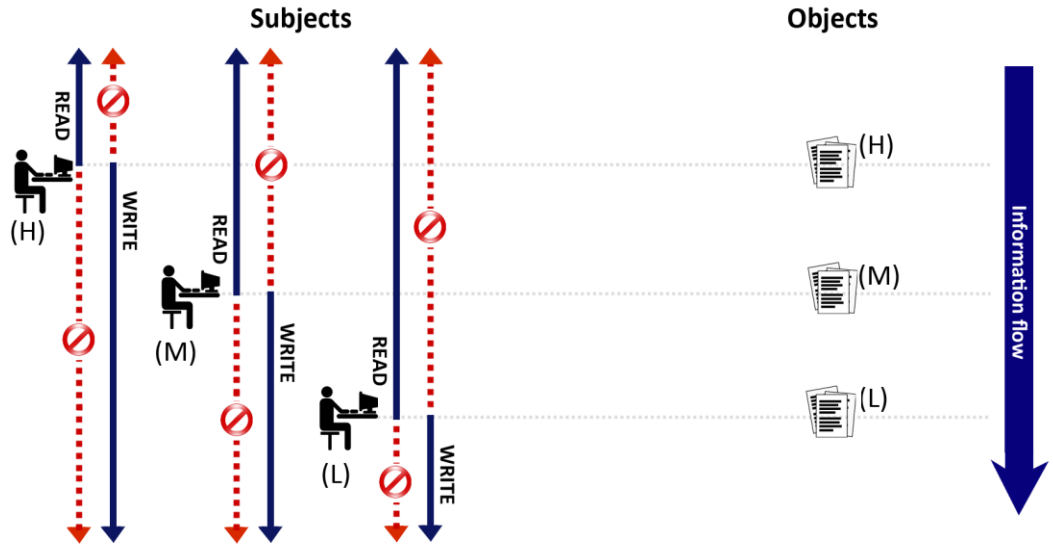


Figure 15. Modèle d'intégrité Biba

Le tableau ci-dessous compare le modèle Biba au modèle de confidentialité de Bell-LaPadula:

Modèle	Lecture	Écriture
BLP (Confidentialité)	No Read Up	No Write Down
Biba (Intégrité)	No Read down	No Write Up

Table 2. Comparatif des propriétés de sécurité BLP et Biba

Après Biba, d'autres modèles d'intégrité ont été développés et qui adressent principalement les problèmes d'intégrité de l'information en adoptant des approches différentes.

4.3.1.2.3 Autres modèles de la famille MAC

La famille de modèles de contrôle d'accès obligatoire inclut d'autres modèles tel Brewer-Nash [66] aussi connu sous le nom Muraille de Chine. C'est un modèle dynamique dont l'objectif principal est d'éviter les cas de conflits d'intérêts au sein d'une organisation suite aux tentatives d'accès des utilisateurs. D'autres modèles de contrôle d'accès obligatoire ont été développés pour préserver la confidentialité et l'intégrité des informations tels le modèle d'intégrité Clark-Wilson, le modèle de Graham-Denning, etc. mais ne sont pas directement reliés à cette recherche. Davantage de détails concernant ces modèles peuvent cependant être trouvés dans [46, 60, 17, 67].

4.3.2 Modèle de contrôle d'accès basé sur les règles (RuBAC)

RuBAC est un modèle de contrôle d'accès basé sur les règles et qui contrôle l'accès aux ressources en se basant sur des règles prédéfinies. Selon [63], il n'y a aucune définition formelle ni de standard reconnu pour ce modèle comme c'est le cas pour les autres modèles discutés plus haut. En fait, RuBAC s'applique à un grand nombre de systèmes qui renforcent le contrôle d'accès aux informations par un ensemble de règles définies au sein de l'organisation. Il agit en comparant les demandes d'accès aux règles d'accès préétablies et qui sont généralement sous forme de labels attachés aux différents objets tels que des fichiers ou du matériel. Un des exemples les plus utilisés serait la règle de contrôle d'accès d'ouverture de session dans les systèmes d'exploitation durant des périodes de temps prédéfinies (exemple : entre 8:00 et 17:00) ou encore l'impression exclusivement en noir et

blanc pour les utilisateurs appartenant à un département donné dans une entreprise. Les règles peuvent aussi être appliquées à des sujets tel la révocation d'accès à un utilisateur après un certain nombre de tentatives erronées d'accès. Les règles sont définies par l'autorité de sécurité de façon centralisée. RuBAC implémente le contrôle d'accès en instaurant un ensemble de règles prédéfinies qui décrivent les relations entre sujets et objets au sein d'un système (autorisations et restrictions appliquées aux sujets et aux objets). RuBAC n'est pas forcement un modèle basé sur l'identité puisque certaines règles peuvent, par exemple, être appliquées à tous les utilisateurs sans tenir compte de leur identité.

RuBAC est généralement implémenté comme supplément à d'autres modèles de contrôle d'accès (MAC, DAC, RBAC) vu son incapacité de gérer les relations directes entre sujets et objets ou entre différents sujets. D'autres faiblesses de ce modèle consistent en la difficulté de création des règles qui nécessitent des processus complexes dépendant de l'organisation [63] en plus de son inadaptation au renforcement des exigences de sécurité basées sur le concept du «besoin de connaître». Les applications les plus répandues du RuBAC dans le contrôle de flux sont les systèmes de routages et les pare-feux qui sur la base d'un ensemble de règles prédéfinies dirigent ou filtrent les paquets de données intrants et extrants du système.

4.3.3 Le modèle de contrôle d'accès basé sur les rôles (RBAC)

Le contrôle d'accès basé sur les rôles (RBAC) est un modèle général d'expression de politique de sécurité qui a été présenté la première fois par Ferraiolo et Kuhn en 1992 [68], et fut adopté comme standard international en 2004 sur la base des travaux de Sandhu, Ferraiolo et Kuhn [69]. RBAC est plus général que les modèles conventionnels du fait qu'il peut être configuré pour implémenter les modèles de contrôle d'accès MAC ainsi que DAC [70]. Les droits d'accès dans RBAC sont traduits en permissions qui relient un ensemble d'opérations (lecture, écriture, …) aux objets du système (fichiers, ressources, …). RBAC attribue ces permissions à des rôles qui généralement calquent la structure et les fonctions au sein de l'organisation. Par la suite, les sujets se verront affectés aux rôles qui leur sont

appropriés selon leurs responsabilités, compétences, autorités, etc. sur la base du concept du «besoin de connaître». Par conséquent ces sujets vont acquérir les permissions qui sont associées aux rôles auxquels ils sont affectés. Un rôle dans RBAC est donc un mécanisme pour associer un sujet à des permissions. L'avantage essentiel de ce modèle est que l'administration de sécurité est plus simple que dans le cas de gestion individuelle des permissions.

Par exemple, dans une banque le droit d'accès aux données des comptes clients (en lecture et écriture) seront des permissions assignées au rôle "Agent de guichet" alors que d'autres opérations tel que la modification et l'audit de ces mêmes comptes seront affectés au rôle "Auditeur". Ces rôles se verront assignés d'autres permissions propres à chacune de ces deux fonction. De même, on peut avoir un rôle plus général : "Employé" qui regroupera des permissions communes à tous les employés de la banque (connexion au réseau, accès aux ressources documentaires, …). A ce stade, les permissions de chacun de ces rôles pourront être attribuées à n'importe quel employé sur la base de sa fonction par son affectation au(x) rôle(s) approprié(s). Ainsi, tous les guichetiers se verront assignés au rôle d'employé et au rôle d'agent de guichet. Les auditeurs auront également le rôle Employé en plus du rôle d'Auditeur (Figure 16).

A cela s'ajoute la gestion des activations des rôles pour chaque sujet. En effet, chaque sujet est identifié par un identifiant unique et sera autorisé pour un rôle donné qui deviendra un rôle actif [44]. Pour raisons de simplification, nous avons ignoré le concept de sessions du RBAC qu'on considère être un concept secondaire par rapport aux fins de cette recherche.

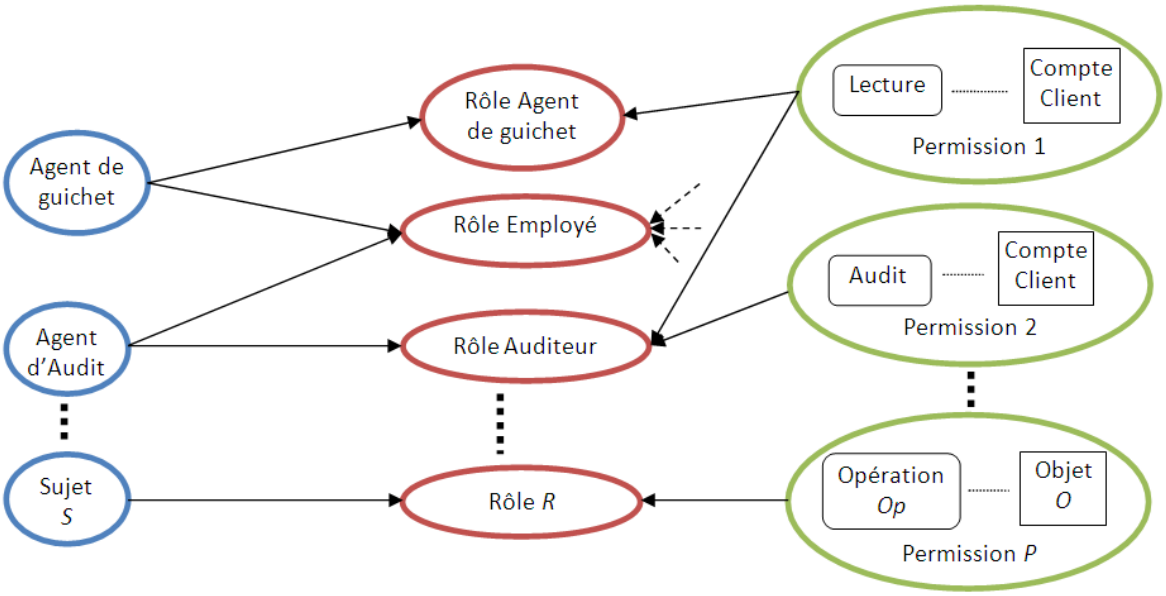


Figure 16. Structure simplifiée du modèle RBAC

On se retrouve ainsi dans un système de hiérarchie de rôles, dans lequel tout sujet est affecté à un ou plusieurs rôles qui lui sont attribués ou révoqués selon les changements organisationnels et fonctionnels au sein de l'organisation. Cette hiérarchie de rôles fait du RBAC un modèle général très adapté aux entreprises hiérarchiques vu qu'il calque parfaitement leur organisation et structure avec un avantage majeur qui est la réduction des efforts de gestion individuelle des droits d'accès. De plus RBAC permet à l'administrateur de sécurité une gestion plus aisée des droits et autorisations, vu que ses actions sont réalisées au niveau organisationnel généralement plus facile à décrire et à contrôler (avec des manuels de procédures par exemple) que si opérées au niveau individuel.

Les objets (documents, ressources, …) sont manipulés sur la base des rôles qui y requièrent accès. Par exemple, l'accès au guide des opérations financières de la banque se verra affecté au rôle "Agent de crédit". Ainsi, seuls les sujets affectés à ce rôle pourront avoir accès à cette ressource [46, 19]. Plusieurs extensions au RBAC ont été développées tel «RBAC over MAC» [59], VBAC [58], etc.

Contrairement aux modèles MAC, le modèle RBAC n'est pas développé dans une optique de contrôle de flux d'informations. En effet, ce modèle est incapable de restreindre

certains flux transitifs entre rôles. Par exemple, si un sujet S_1 dispose de rôles R_1 et R_2 et un deuxième sujet dispose du rôle *R2*, une information confidentielle accédée par S_1 sur la base du rôle R_1 peut facilement être transmise à S_2 via le rôle R_2 commun aux deux sujets. De plus, l'expression des exigences de sécurité du RBAC s'avère difficile surtout dans des environnements larges, distribués ou très dynamiques du fait qu'il ne s'adapte pas facilement à des situations où le nombre d'objets pris en charge augmente [55].

Afin d'assurer le contrôle de flux, une configuration du RBAC pour implémenter la politique de sécurité du MAC a été présentée dans les travaux d'Osborn et al. [70, 71]. Cette configuration est appliquée à certaines composantes du RBAC pour garantir son adaptation au MAC. Pour réaliser cet objectif, ces travaux se basent sur les concepts de contraintes et de hiérarchies de rôles. Ainsi, un rôle comprendra des permissions relatives à des objets auxquels sont attribués des labels de sécurité (classes). Par exemple un objet *O* se voit assigner le couple permission-classification : Lecture-Top Secret et ainsi de suite selon un graphe de hiérarchie de rôles. Bien que cette technique garantisse un contrôle de flux à certains niveaux de la hiérarchie, elle crée des situations de conflits de permissions et de rôles. Une analyse détaillée de certains de ces conflits est présentée dans [72].

D'autres travaux traitent l'implémentation des mécanismes de sécurité multi-niveaux dans RBAC en adoptant des approches d'héritages des permissions et de hiérarchies de rôles notamment les travaux de Crampton [73].

4.3.4 Modèles de contrôle d'accès basés sur les attributs (ABAC)

Avec l'évolution du monde des affaires et des communications, les organisations sont de plus en plus amenées à partager des ressources et échanger des informations entre elles et avec d'autres acteurs de leur environnement. Ceci a révélé l'incapacité des modèles traditionnels à garantir de façon satisfaisante la sécurité de ces ressources et la confidentialité de ces informations. Par conséquent, les modèles de contrôle d'accès ont, depuis les années 70, suivi une évolution de modèles limités à un seul domaine proposant

une gestion individuelle ou par classes des droits d'accès, vers des modèles de gestion par règles et par rôles pour arriver à un contrôle d'accès basé sur les attributs (Figure 13) [74].

ABAC est un modèle logique de contrôle d'accès basé sur les attributs qui implémente le contrôle d'accès aux objets par l'évaluation d'un ensemble de règles d'accès relativement à des attributs assignés aux entités du système (sujets et objets), aux opérations d'accès et à l'environnement à la suite d'une demande d'accès. Chaque attribut est une entité discrète et distincte qui peut être comparée à un ensemble de valeurs pour déterminer si oui ou non l'accès à un objet ou ressource peut être autorisé pour une politique de sécurité donnée [75]. Un sujet peut être un utilisateur, un demandeur (*Ang. requestor*) ou un mécanisme qui agit pour le compte de ces derniers [76]. Les conditions d'environnement sont aussi considérées comme des attributs et constituent des facteurs dynamiques indépendants des sujets et des objets. Ainsi, dans ce modèle, une demande d'accès d'un sujet *S* à un objet *O* est premièrement reçue par un mécanisme de contrôle d'accès basé sur les attributs. Ce mécanisme accède à une base de données d'attributs appliqués au sujet, à l'objet, à l'opération et à l'environnement puis les compare avec les règles d'accès extraites de la politique de contrôle d'accès. Sur la base de cette confrontation entre attributs et règles une décision est prise pour octroyer ou dénier le droit d'accès au sujet [76, 41]. La Figure 17 illustre ce processus.

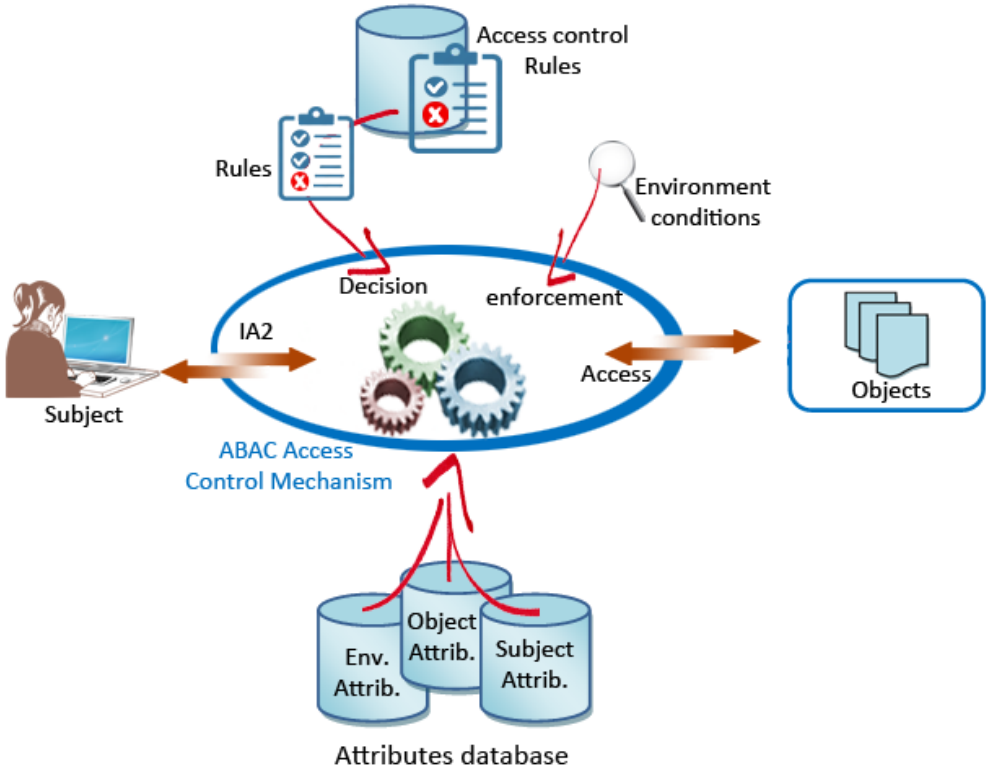


Figure 17. Modèle de contrôle d'accès ABAC

On reprendra l'exemple de la banque déjà cité pour illustrer les particularités de ce modèle. Ainsi, un "agent de crédit" a un ID, Mot de passe, Nom, Prénom, Fonction, Département, etc. qui représentent ses attributs. De l'autre côté, un dossier de crédit a les attributs : Numéro, Date, Bénéficiaire, Montant, Taux d'intérêt, et ainsi de suite. En même temps, une opération de lecture ou d'écriture a aussi des attributs tels : Type, Portée, Date, etc. A tous ces attributs s'ajoutent les attributs de l'environnement financier du genre : Date, Heure, Localité, Taux du marché financier, etc.

Dans cet exemple on considère une règle d'accès qui stipule qu'un "agent de crédit" authentifié du "département crédit aux particuliers" peut réduire *(opération)* le taux d'intérêt pour un dossier de crédit uniquement pour les dossiers de plus d'un an à condition que le nouveau taux ne soit pas inférieure au taux du marché financier majoré de 2 points à la date de cette transaction.

Maintenant, pour obtenir une autorisation d'accès pour exécuter cette opération, par un sujet *S,* celui-ci passe tout d'abord par une vérification de ses attributs (ID, Mot de passe, Département, ...), puis par la vérification des attributs de l'objet O -ici le dossier de crédit- (Numéro, Date, …), ensuite la vérification des attributs de l'opération (Type, Portée, Date…) et de l'environnement (Date, Heure, Taux du marché financier, …). Finalement, ces attributs sont comparés avec les valeurs exprimées dans la règle d'accès pour donner une décision d'autorisation d'accès en cas de concordance ou d'interdiction dans le cas contraire.

Il est à souligner ici que les règles d'accès du ABAC spécifient les combinaisons d'attributs sur la base desquelles un accès sera autorisé [13].

ABAC permet le contrôle d'accès en intégrant plus de variantes dans la décision d'accès offrant un éventail plus large quant aux combinaisons possibles offertes à l'administrateur de sécurité dans le but de couvrir encore plus de politiques et de scénarios d'accès. Avec les variétés d'attributs qui peuvent être assignés aux objets et aux sujets, ABAC offre une grande flexibilité relativement au nombre de sujets et d'objets qui peuvent être gérés par le système sans se préoccuper de l'aspect individuel des relations entre ces derniers. Un autre avantage majeur pour ces modèles est qu'ils sont aussi bien adaptés aux accès mono qu'inter-organisations [76]. Comparé au RBAC, le ABAC nécessite généralement moins d'efforts de configuration mais présente plus de difficultés quant à la gestion et au contrôle des autorisations utilisateurs.

ABAC est capable d'implémenter aussi bien des politiques IBAC que RBAC [76] et offre un contrôle d'accès plus complexe que ces derniers mais néanmoins avec un coût d'administration et de gestion additionnel engendré par cette complexité. Un autre facteur qui peut augmenter cette complexité et réduire les capacités de ce modèle est la méconnaissance des politiques à prendre en charge par ce modèle [55]. Plus de détails sur la famille de modèles ABAC peuvent être trouvés dans [77, 76].

Le Tableau 3 ci-dessous présente un comparatif résumé des propriétés des principales familles de modèles de contrôle d'accès traités dans cette section relativement aux droits d'accès, à l'implémentation du contrôle de flux et au support d'architectures multi-domaines.

	MAC	DAC	RBAC	RuBAC	ABAC
Autorité de sécurité	Centrale	Utilisateur	Généralement Centrale	Centrale	Centrale
Audit d'accès	Centrale	Utilisateur	Central	Centrale	Centrale
Propagation des droits d'accès	Centrale	Utilisateur	Généralement Centrale	Centrale	Centrale
Contrôle de flux d'information	OUI	NON	NON	OUI	NON
Multi-domaines	NON	NON	NON	NON	OUI

Table 3. Comparatif des modèles de sécurité

4.3.5 Nouveaux Modèles de contrôle de flux

De ce qui précède on constate que les modèles de contrôle de flux d'informations ont principalement été de la famille MAC et en particulier le modèle de Bell-LaPadula. D'autres modèles moins connus ont été développés plus récemment. Des exemples de ces modèles seraient le contrôle de flux d'informations basé sur les langages (Language-based information-flow control) et sur les étiquettes (*Tag Based Authentication*), etc.

4.3.5.1 Contrôle de flux basé sur les langages

Les mécanismes de sécurité appliqués aux langages de programmation ont été utilisés depuis un certain temps pour assurer la vérification et le respect des spécifications de ces langages plutôt que pour des raisons de protection de la confidentialité des informations. L'exemple typique est l'environnement d'exécution Java (*Ang. Java runtime environment*). Les modèles de contrôle de flux d'informations basés sur les langages sont des modèles qui reposent sur des langages de programmation pour proposer des solutions spécifiques au contrôle de flux d'informations par la vérification et la protection des types de données privés utilisées dans les programmes afin de garantir une sécurité de bout-en-bout [30].

L'objectif étant l'assurance que les programmes n'incorporent pas de bugs de sécurité ou d'implémentations qui induisent des flux d'informations illégaux [78]. Cette protection se fait de manière statique ce qui, cependant, constitue une faiblesse par rapport à d'autres modèles où elle pourrait être dynamique.

Dans cette famille de modèles les variables sont assignées, en plus de leur type, un type supplémentaire de sécurité précisant leur niveau de classification sous forme de label. En général, ces labels partiellement ordonnés sous forme de treillis tel dans cet exemple : {L,H} où on dispose de deux niveaux de sécurité ordonnés haut (H) et bas (L) avec $L \subseteq H$ stipulant que seuls les flux d'information allant de (L) vers (H) sont autorisés et que le système ne peut permettre la situation inverse.

Le compilateur s'assure à la compilation ou à l'exécution (*run-time*) que le programme ne renferme aucune possibilité de flux d'informations illégal en analysant les labels de sécurité des variables et les flux y afférant. Autrement dit, garantir qu'aucun flux de (H) vers (L) n'est possible. Une violation de cette règle de flux d'information dans le programme engendrera une erreur de compilation ou d'exécution (erreur de type). Au cas où des exceptions à cette règle de sécurité sont à considérer, une déclassification est requise mais s'avère généralement risquée surtout en présence de code non approuvé. Les travaux de Myers et Liskov [79, 80, 81] tentent résoudre ce problème -entre autres- en proposant un modèle décentralisé qui octroie des privilèges aux modules du programme qui peuvent chacun procéder à certaines déclassifications sur la base de leurs privilèges [82]. Une étude plus détaillée du contrôle de flux basé sur les langages est fournie dans les travaux de Sabelfeld, Myers et Liskov [30, 81, 80]. Plusieurs implémentations de ce modèle ont vu le jour tel JFlow, Jif, "taint-checking mode", SparkAda, DStar, etc. [83, 84, 82]. Cependant, et malgré un certain succès qu'a eu cette approche, ce modèle n'a pas été préconisé à large échelle pour plusieurs raisons [54] dont :

- Le coût de développement élevé de telles solutions logicielles dans de nouveaux langages pour des systèmes généralement larges et complexes.

- La discordance entre l'étendue du domaine à sécuriser (nombre de variables qui ont des exigences de sécurité de flux) et l'effort de développement nécessaire à cette fin souvent injustifié [82].
- Le besoin d'une bonne connaissance des exigences de sécurité et de la manière de les formaliser par le programmeur de telles solutions.
- La difficulté d'intégration de ces solutions dans des mécanismes de sécurité préétablis [85].
- L'inadaptation de cette approche aux environnements distribués et au Web [86].

Il faudra noter que certaines de ces limites sont aussi valables pour les modèles conventionnels de contrôle d'accès. La Section 4.4 traite ce sujet avec plus de détails.

4.3.5.2 Autres approches au contrôle de flux

D'autres modèles de contrôle d'accès basés sur les labels et les étiquettes ont été développés en recherche notamment dans les travaux portant sur l'authentification basée sur les étiquettes (*Tag Based Authentication*) [87, 88].

Dans ces articles, certaines nouvelles méthodologies ont été proposées. Cependant, elles proposent des applications spécifiques et ne traitent pas les problèmes du flux d'informations dans leur globalité comme le ferait un modèle de contrôle de flux. Généralement, ces travaux tentent de résoudre les problèmes de flux d'informations en couvrant des flux spécifiques, tels dans les systèmes de gestion de bases de données objets [89, 90], dans les systèmes distribués [91] et ainsi de suite. Ces recherches relèvent moins du domaine de notre présent travail mais pourraient être analysées pour de possibles apports futurs.

En plus des modèles traités dans cette section, un grand nombre de variantes et de modèles spécifiques ont été développés au cours des années. Une liste, probablement incomplète, des modèles de contrôle d'accès discutés en recherche est présentée dans

l'Annexe 1 (de ABAC au ZBAC). Il est à remarquer qu'il existe un antagonisme entre le pouvoir expressif d'un modèle de contrôle d'accès et la facilité du renforcement et d'implémentation de ses mécanismes [63]. Cette abondance d'approches nous amène à faire un choix restreint aux modèles conventionnels (MLS, RuBAC, RBAC, et ABAC) dans notre étude comparative et analytique des apports et des avantages du GBFC.

Dans la Section 4.4, on procédera à une analyse de certaines limites de ces modèles qui pourraient fournir une justification pour les occurrences de fuites d'informations constatées en pratique.

4.4 Limites des modèles de sécurité relatives au contrôle de flux

Après ce bref survol des principaux modèles de sécurité, nous pouvons distinguer deux principaux objectifs de ces derniers :

1- Gérer les droits d'accès aux données et prévenir tout accès illégitime ou modification accidentelle ou malveillante de l'information : *Contrôle d'accès*
2- Gérer et contrôler la diffusion et la propagation de l'information : *Contrôle de flux.*

Nous avons vu que les modèles mentionnés parviennent à réaliser le premier objectif avec succès mais continuent à souffrir de failles sérieuses quant à la gestion et au contrôle de flux d'informations. Les risques relatifs à une faille de contrôle de flux deviennent d'autant plus importants et augmentent proportionnellement avec la taille de l'organisation, la complexité du système de sécurité et le volume d'informations confidentielles à protéger. A ceci s'ajoute le temps de détection et de réponse à un cas de fuite d'informations, souvent assez long et qui peut atteindre des mois voire des années à découvrir et à traiter [92]. Le risque est d'autant plus grand quand on sait que "*Il suffit d'avoir une seule station de travail non protégée dans un réseau pour mettre tout le réseau à risque…. De plus, les*

risques et les coûts de déploiement des mesures de sécurité sont élevés et ne font qu'augmenter davantage" selon Richard Hunter le vice-président de Gartner Inc. [93].

Bien que les statistiques présentées dans la section 1.2.1 confirment l'ampleur de ce problème de fuites d'informations et de flux illégitimes. Cependant, il est surprenant que malgré cette réalité, le contrôle de flux d'informations jouit d'une importance secondaire dans les ouvrages académiques (et pratiques) de sécurité informatique à l'exception d'ouvrages ou d'articles spécialisés. En effet, sur 14 ouvrages de référence en matière de sécurité informatique listés dans le Tableau 4 ci-après, le contrôle de flux d'informations est mentionné de façon très limitée (moins de 70 mentions sur plus de 12.000 pages dans 8 ouvrages sur 14) et est généralement discuté de façon superficielle (Seuls deux ouvrages, les deux livres de M. Bishop, renferment des chapitres sur le flux d'information, et ils se concentrent sur le flux d'information dans les programmes [57, 26]). Le Tableau 4 fournit plus de détails relativement à ces constatations :

Auteurs	Titre de l'ouvrage	Edition	Nbre. de pages	Nbr. de citations
- Références et ouvrages Scientifiques				
John Vacca	Computer and Information Security Handbook [20]	2009	844	0
Jie Wang	Computer Network Security Theory and Practice [94]	2009	384	0
S. Bosworth, M. E. Kabay	Computer security handbook [95]	2002	1.224	2
Matt Bishop	Computer Security: Art and Science [57]	2002	1.154	19
David Salomon	Foundations of Computer Security [96]	2006	389	0
R. Focardi , R.Gorrieri	Foundations of Security Analysis and Design [97]	2001	406	6
Joseph Migga Kizza	Guide to Computer Network Security [98]	2013	521	2
John Vacca	Guide to Wireless Network Security [99]	2006	848	0
H. F. Tipton, M. Krause	Information Security Management Handbook [21]	2007	3.231	17
Matt Bishop	Introduction to Computer Security [26]	2005	747	17
Douglas W. Frye	Network Security Policies and Procedures [100]	2007	240	0
D. F. Ferraiolo, R. Kuhn, R. Chandramouli	Role-Based Access Control [44]	2007	384	1
- Références et ouvrages pratiques				
Shon Harris	CISSP Certification All-in-One Exam Guide [22]	2013	1.430	5
Thomas R. Peltier	Information security policies and Procedures. A practitioner's Reference [101]	1999	248	0
		Total	**12.050**	**69**

Table 4. Citations du contrôle de flux dans la littérature

Un des problèmes majeurs des modèles de contrôle d'accès relativement au contrôle de flux d'information est le problème de confinement qui se manifeste par un flux d'information illégitime indirect subséquent à un accès légitime par un sujet authentifié et ayant droit d'accès [102]. Ce flux est difficile à contrôler du fait qu'il existe même en conformité avec la politique de sécurité en place et peut prendre différentes formes et avoir recours à des canaux cachés ou d'autres mécanismes plus développés. Le problème de confinement est inhérent aux modèles de contrôle d'accès [103, 91] et reste une préoccupation majeure dans tout développement de politiques de sécurité. Les modèles de contrôle d'accès et de contrôle de flux existants se concentrent sur la protection des sujets et des objets dans le but de protéger la confidentialité des informations plutôt que d'appliquer les mesures de sécurité directement sur les informations elles-mêmes.

Une autre faiblesse majeure des modèles de sécurité classiques quant au contrôle de flux est que ceux-ci -à l'exception du ABAC- ont été développés dans une optique de systèmes localisés et n'ont pas pris en considération le développement rapide des technologies et des architectures distribuées qui renferment de multiples domaines de sécurité souvent hétérogènes et indépendants. Cette architecture engendre des fonctionnements et des opérations de gestion trans-domaines inadaptés pour les systèmes de contrôle d'accès existant qui, bien que fiables pour un contrôle d'accès localisé, se retrouvent inadaptés pour la gestion de sécurité multi-domaines. Encore, sont-ils moins adaptés à prévenir des flux illégitimes entre différents domaines interdépendants qui implémentent des politiques de sécurité différentes [43]. La réponse à cette faiblesse n'a pas pris la forme de proposition de nouveaux modèles plus adaptés à ce genre d'environnements mais seulement des formes de mises à jour, de combinaisons, de suppléments ou de nouvelles variantes de certains de ces mêmes modèles [104, 105, 106].

Le modèle d'accès discrétionnaire DAC, bien qu'efficace à traduire une politique de sécurité, facile à implémenter et très adapté aux besoins du sujet propriétaire de l'information, présente une faille majeure relative au contrôle de flux et au confinement des sujets détenteurs de l'information. Ceci découle de la propriété discrétionnaire du transfert

des droits d'accès gérés par le propriétaire de l'information qui perd tout contrôle sur sa propagation au delà de son propre système. Ceci rend DAC inefficace pour des infrastructures ou des environnements de travail distribués ou collaboratifs (bases de données distribuées, réseaux, web,…). De plus, ce modèle n'offre pas une vision globale du système et des données rendant très probable l'affectation erronée de privilèges et de droits d'accès à des sujets non autorisés [60]. A ceci s'ajoute la vulnérabilité de ce modèle devant les attaques par les Chevaux de Troie [39] et d'autres programmes malveillants. Il est cependant important de mentionner que ce modèle est très largement implémenté dans les systèmes d'exploitation, de gestion de bases de données et de communication de données [107, 32].

De nouvelles variantes du DAC tentent de contourner certains de ces problèmes, tel le Strict DAC qui stipule que seul le propriétaire de l'information a l'autorité d'attribuer les autorisations d'accès à un objet. Liberal DAC ajoute la possibilité pour le propriétaire de déléguer cette autorité à d'autres utilisateurs [44].

De plus, les modèles de la famille IBAC (MAC, DAC, …) se basent sur l'identité, sur la classification ou sur les rôles des sujets et des objets dans leurs processus de contrôle d'accès et confirment leur efficacité uniquement en cas d'implémentation dans des environnements statiques et restreints où les sujets et les objets sont faciles à cerner, à identifier et à gérer [55].

Les modèles de contrôle de flux conventionnels, en particulier ceux de la famille MAC, tentent de garantir la confidentialité et l'intégrité des informations en implémentant des règles de restriction de flux au sein du système. Cette solution, généralement facile à mettre en œuvre n'est cependant applicable que dans certains domaines limités dont l'organisation, le fonctionnement et la nature des informations justifient l'assentiment aux handicaps liés à ces restrictions [27, 17]. Pour cette raison, et à l'exception du domaine militaire, rares sont les domaines professionnels qui adoptent le contrôle d'accès obligatoire du fait de son aspect restrictif vis-à-vis de plusieurs applications. Même dans les domaines où MAC est

préconisé, des exceptions à ses restrictions de flux sont souvent considérées. L'exemple typique est le besoin d'approbation de flux vers des domaines ouverts sur l'internet ou de flux spéciaux n'adhérant pas aux directives du modèle [17]. De plus, le contrôle de flux dans ces cas est généralement mis en place à travers la surveillance détaillée des flux de données dans les programmes, chose qui peut s'avérer complexe et parfois inefficace [40].

De même, le RuBAC est un modèle qui s'est avéré efficace quant à la prévention des fuites d'informations en particulier pour les systèmes de petite taille notamment quand combiné avec d'autres modèles de sécurité. Cependant, il présente trois défaillances majeures qui limitent ses capacités vis-à-vis du contrôle de flux d'informations surtout pour des systèmes étendus ou dynamiques : la première étant la difficulté de cerner toutes les règles de sécurité à implémenter en plus du coût de leurs implémentations. La deuxième étant le changement continuel des composants des systèmes, de nos jours très dynamique et très ouverts, qui rendent laborieuse la tâche de gestion de ces règles en l'absence d'une vision globale du système. La dernière est que l'implémentation de ce modèle est quasiment impossible dans les architectures multi-domaines du genre réseaux distribués, structures infonuagiques, Internet et similaires [63].

Il est à souligner que l'évolution rapide des systèmes d'informations a complètement bouleversé la perception classique relative à la prévention de fuites d'informations. En effet, les modèles et les visions classiques ne sont plus adaptés aux environnements distribués dynamiques et collaboratifs actuels. En effet, l'information est produite et œuvrée localement en masse pour être rendue disponible globalement avec comme grand défi la protection de sa confidentialité et de son intégrité. Ce processus continuel et dynamique complique la gestion de la sécurité et des flux d'informations. Ces flux deviennent encore plus complexes quand ils sont opérés sur plusieurs domaines de sécurité hétérogènes. Cette complexité est proportionnelle au nombre et à la disparité des domaines et des sujets impliqués dans le flux.

Il est aussi à noter que les propriétaires de l'information et les autorités de gestion de sécurité sont généralement les plus aptes à décider de sa classification. Cette classification pourrait facilement entrer en conflit avec les directives adoptées par les modèles de sécurité instaurés au sein du système. De plus, on remarque que les besoins en sécurité de flux d'information peuvent être très disparates en fonction des données transférées (fichiers, e-mails, données privées, contenu sous copyright, etc.), des types d'utilisateurs (utilisateur unique, unités organisationnelles, réseaux sociaux, etc.) et de la portée du flux (domaines localisés, multi-domaines, …). Ceci rend toute solution limitée ou localisée inappropriée et très rapidement dépassée par le développement de la technologie [63, 108]. En effet, la majorité des recherches sur les fuites d'information et sur le contrôle de flux se concentre sur les formes problématiques et les manifestations liées à la circulation de l'information comme le confinement, l'inférence, les canaux cachés etc., qui ne représentent que des formes, des manifestations et des effets du problème principal qui est le flux lui-même. D'un autre côté, les politiques de contrôle de flux dans un domaine de sécurité sont basées sur des règles générales applicables dans l'ensemble du système sous forme de droits et autorisations claires que les utilisateurs comprennent. La connaissance des directives d'une politique de sécurité, par elle-même, peut faciliter sa violation.

Une autre faiblesse inhérente aux modèles et systèmes de sécurité actuels est qu'ils ne parviennent pas à contrôler la manière dont les informations sont exploitées après leur accès par un sujet donné. Ainsi, quand un utilisateur autorisé accède à des informations confidentielles, d'autres mécanismes sont nécessaires pour suivre et contrôler les activités postérieures opérées sur cette information. Ces activités concernent sa réplication (copie), sa modification, sa propagation et enfin sa destruction adéquate et sécuritaire pour empêcher toute communication transitive. De nouvelles techniques (contrôle d'utilisation UCON) [109] tentent de corriger cette situation par la mise en œuvre d'obligations à respecter par l'utilisateur, mais manquent d'autorité et de procédés d'application et de contrôle de leur respect, ce qui explique les mises en applications limitées ou quelquefois même inefficaces pour ce genre de méthodes.

Le modèle RBAC, bien qu'il soit considéré comme un cas de réussite dans le domaine du contrôle d'accès, ne renferme pas de mécanisme de contrôle de flux. Certaines recherches ont essayé de remédier à cette faille, principalement les travaux d'Osborn et al. présentés dans la 4.3.3 de ce chapitre. Mais les recherches dans ce sens sont bien peu nombreuses et continuent à présenter des limites quant aux conflits entres rôles et entre permissions. Une autre limite du RBAC réside dans la difficulté d'appliquer des critères de contrôle d'accès granulaires à chaque sujet vu que ceux-ci sont catégorisés sur la base de rôles [75]. De plus, le processus de conception de rôles s'avère être une tâche difficile sachant qu'il y a un effet de levier entre le besoin d'augmenter le niveau de granularité des rôles, nécessaire pour une meilleure sécurité, par rapport à la réduction du nombre de rôles, nécessaire pour une administration plus aisée. RBAC est moins adapté aux environnements distribués, supporte difficilement l'aspect discrétionnaire de contrôle d'accès (DAC) et manque de capacité d'implémentation des mécanismes de contrôle de séparation des tâches (*Separation of duty*) [63, 108].

Très similaire au RBAC, le modèle ABAC ne renferme pas de mécanisme explicite de contrôle de flux d'informations en plus d'autres limites dont certaines ont été soulevées dans la Section 4.3.4 de ce chapitre en addition à celles listées dans le rapport de la FICAM [108]. En effet, ce modèle se base sur une multitude d'attributs relatifs aux sujets potentiels, aux objets, aux opérations et à l'environnement et qui sont généralement disparates et conflictuels. Cette multitude d'attributs provenant de différents domaines rend l'administration de sécurité tâche ardue [75]. Outre ces limites, ABAC n'est pas supporté par les systèmes d'exploitation usuels et peut ne pas être adéquat pour certains environnements [108].

D'un autre côté, la vision classique relative à la protection de l'information via la protection des objets qui la renferment s'est avérée inefficace, particulièrement dans les cas où ces objets peuvent se retrouver à la portée de sujets malveillants. L'exemple typique pour ce genre de situation est le cas de perte de matériel ou de fuites d'informations initiées

par des sujets internes à l'organisation. Les statistiques des cas de fuites d'informations épaulent cette constatation [110, 111, 5].

En raison des difficultés mentionnées ci-dessus, très peu à été réalisé pour mettre en œuvre des architectures et des systèmes orientés contrôle de flux [30]. Les systèmes existants traitent la sécurité des flux d'information à travers les mécanismes de contrôle d'accès existants en conjonction avec des outils additionnels (add-on) pour intégrer les politiques de contrôle de flux. Ces combinaisons sont nécessaires sachant que les mécanismes de contrôle d'accès sont limités quant au contrôle de flux d'information, même s'ils réussissent à maintenir un contrôle d'accès acceptable [60, 26, 81]. Pour cela, dans un domaine de sécurité, le contrôle de flux est habituellement réalisé à travers les techniques de routage ou des mécanismes de sécurité du genre pare-feu ou logiciel antivirus additionnés aux programmes et techniques de cryptage. Cependant, ces outils présentent généralement des vulnérabilités inhérentes et des faiblesses continuelles devant le développement de nouvelles technologies de logiciels malveillants [20]. La majorité n'offrent pas une sécurité de bout-en-bout et sont inefficaces à l'égard d'utilisateurs validés, de logiciels authentiques ou de programmes légitimes accrédités. Ajoutons à cela le besoin continuel de mises à jour et de reconfigurations pour pouvoir garantir des niveaux de sécurité acceptables.

En l'absence de nouveaux modèles de contrôle de flux dédiés, les propos de D. E. Denning tiennent toujours [31]: « *Les systèmes ont besoin à la fois de contrôle d'accès et de contrôle de flux pour satisfaire toutes les exigences de sécurité* ».

Toutes ces limites indiquent clairement qu'il existe un besoin pressant pour de nouveaux modèles de contrôle de flux dévoués et efficaces.

Notre modèle, présenté au Chapitre 5, tente de répondre à ces défis en proposant une solution qui utilise la granularité et le référencement des données comme facteurs clés pour

la prévention des fuites d'informations et pour le maintien d'un contrôle de flux d'informations adéquat.

4.5 Sécurité et information granulaire

4.5.1 Concept d'information granulaire

Selon [112], la granularité, aussi connue sous le nom d'informatique granulaire, a été introduite en 1997. Zadeh [113] stipule que les éléments fondamentaux de l'informatique granulaire sont des granules tels que des sous-ensembles, des classes, des objets, des grappes et des éléments d'un domaine ou d'un univers. Ces granules sont des ensembles d'éléments sélectionnés selon leurs facteurs distinctifs, leurs similitudes et leurs fonctionnalités [112].

Les granules, dans leur forme atomique, sont composés d'éléments constitutifs d'un modèle spécifique. Par exemple, un granule dans un fichier image serait un pixel ou un ensemble de pixels, et dans un document texte, un granule peut être un paragraphe, une phrase, un mot, une date et ainsi de suite [114].

4.5.2 Granularité et sécurité de l'information

La granularité a été introduite dans certains modèles de contrôle d'accès pour spécifier le niveau de détails à appliquer aux permissions et privilèges à accorder aux sujets (RBAC) ou aux attributs à considérer dans le processus d'octroi des droits d'accès (ABAC). Le niveau de granularité à adopter est un facteur décisif dans le choix d'un modèle par rapport à un autre vu le coût d'administration élevé généralement engendré par un niveau de granularité élevé [75]. En pratique, le contrôle d'accès granulaire à l'information a été introduit dans les systèmes de gestion de bases de données pour gérer et contrôler l'accès aux colonnes dans les tables. L'accès est accordé sur la base de l'authentification et les rôles de l'utilisateur. Cependant, en dépit de l'intérêt de ce concept dans le domaine de sécurité de données et de contrôle d'accès, peu de travaux de recherches ont été menés sur l'utilisation

de granularité dans le contrôle de flux excepté pour les travaux de Thorleuchter et Van den Poel [115] qui ont proposé l'implémentation des concepts de granularité pour les modèles de sécurité multi-niveaux (MLS) en particulier le modèle de Bell-LaPadula. Leur technique vise à minimiser l'impact de la classification des informations sur leur disponibilité pour des sujets de moindre niveau de sécurité. Le concept de granularité est repris dans notre recherche mais avec plus de profondeur et avec une vision d'implémentation plus généralisée.

Dans ce chapitre, on a réalisé un survol des principales familles de modèles de contrôle d'accès aux informations en mettant l'accent sur leur capacité à garantir un contrôle de flux adéquat. Chacun des modèles renferme des avantages non réfutables mais par la même occasion souffre de limites le rendant inefficace quant à la prévention des fuites d'informations dans certaines situations. Ces limites constituent pour nous une plateforme sur laquelle on pourra se baser pour proposer un modèle axé sur le contrôle de flux qui tentera d'adresser au mieux ces limites. Le Chapitre 5, présentera en détail notre modèle et présentera son mode d'action et ses principaux avantages.

Chapitre 5 : Modèle de contrôle de flux basé sur la granularité

Dans le Chapitre 1, on a vu que les causes majeures derrière les flux illégitimes d'information sont :

En premier lieu, l'existence du flux en lui-même qui simplifie et favorise des transferts non autorisés d'informations au-delà des domaines de sécurité qui les régissent. En deuxième lieu, on a l'octroi de droits d'accès aux informations en tant qu'ensemble (fichiers, courriels, tables, etc.). En effet, dans la majorité des cas de flux d'informations, le transfert est opéré sous forme d'un flux total des éléments d'information confidentielle. En dernier lieu on constate le fait que l'information confidentielle transférée est reçue dans un format favorisant et facilitant sa réplication, sa reproduction et son transfert par le récepteur et par la suite son exploitation par les tiers en cas de flux illégitime.

On proposera dans ce chapitre notre solution pour combler ces lacunes sous forme d'un nouveau modèle et d'une nouvelle méthodologie qui permettront de minimiser les risques de flux illégitimes et garantiront un contrôle de flux d'informations renforcé.

5.1 Environnement du modèle

5.1.1 Atouts de l'architecture réseau

Quand on parle de flux d'information, l'une des principales causes de la vulnérabilité à la fuite d'informations est l'existence de l'architecture réseau. Cette cause de vulnérabilité renferme en elle-même le principal avantage et l'atout majeur pour la réussite des processus et des mécanismes de contrôle de flux d'informations.

Effectivement, le fait d'opérer dans un environnement réseau, que ce soit local ou étendu, signifie que le sujet expéditeur utilise le réseau pour les opérations de transmission et pourra décider des flux qui peuvent survenir pour l'information. De l'autre côté, le récepteur accède à l'information en lecture et écriture via le réseau après avoir franchi la barrière de sécurité à travers l'identification, l'authentification et l'autorisation. Dans une telle situation, on pourra envisager la possibilité d'accès distant aux informations de façon partielle et graduelle afin de préserver la confidentialité et prévenir toute fuite, tout en respectant le principe du « besoin de connaître ».

L'existence de cet environnement réseau sera donc utile pour réduire les transferts d'informations confidentielles en adoptant une architecture centralisée qui permet -au besoin- de minimiser et restreindre les flux qui peuvent s'avérer risqués.

5.1.2 Restriction de flux

L'une des raisons majeures du succès des systèmes mainframes du point de vue sécurité des flux de données est l'aspect centralisé d'accès aux données qui se fait via des terminaux ou des émulateurs de façon distante ce qui rend tout flux secondaire indirect (vers un troisième acteur) quasiment impossible [116]. Ceci s'explique par l'impossibilité de disposer de l'information en l'absence du serveur. En d'autres termes, il s'agit de l'absence ou de la restriction de flux.

Un proverbe arabe stipule que « *Un secret qui outrepasse deux personnes est un secret divulgué* ». Certes, le meilleur contrôle de flux d'informations n'est rien d'autre que l'absence du flux lui-même. Soit, un secret non divulgué reste un secret bien préservé.

Ceci devient d'autant plus évident lorsqu'on sait que dans notre monde actuel, avec la mondialisation des affaires, la globalisation des réseaux de communication et des réseaux sociaux, les risques reliés aux flux des informations sont devenus globaux et complexes.

5.1.3 Disponibilité et accessibilité de l'information

Qu'une information soit *disponible* pour un sujet donné signifie que les composants de cette information existent sur un support physique ou logique normalement accessible par le sujet. En d'autres termes, l'information, ou les composants de l'information existent en tant que tels indifféremment des droits d'accès qu'aurait le sujet relativement à celles-ci. A ce niveau, aucun contrôle des droits d'accès n'est opéré et l'information disponible n'est pas forcément accessible.

Pour qu'une information soit *accessible* par un sujet donné, celle-ci doit premièrement être disponible pour celui-ci et le sujet doit disposer des droits et privilèges nécessaires pour y accéder.

On prendra comme exemple l'accès à un fichier protégé sauvegardé sur le disque d'un utilisateur donné. Bien que l'utilisateur ait un contrôle complet sur le disque qui loge le fichier, il se trouve incapable d'ouvrir celui-ci en l'absence des droits d'accès. Dans ce cas les données sont disponibles mais non accessibles.

Dans les modèles de sécurité classiques, la disponibilité de l'information se traduit par son écriture dans un objet et l'accessibilité à cette information n'est rien d'autre que le droit d'accès (en lecture ou écriture) à l'objet qui la renferme. Dans le cas de flux d'information la disponibilité de l'information se manifeste par l'existence ou non du flux lui-même. Certes, un flux d'information implique une mise à disposition de l'information pour le sujet récepteur.

Le fait qu'un sujet ait droit d'accès à un objet et que l'information classifiée ait pu être écrite sur cet objet *(devient disponible)* entraine que le sujet ait accès à l'information à travers l'objet qui la renferme indifféremment de ses droits d'accès à l'information elle-même. Cette situation problématique nous suggère un abandon de la conception classique des modèles de sécurité à deux composants : (Sujet et Objet), pour une nouvelle perception où l'information est considérée un composant -à part entière- sur lequel appliquer

directement les critères de sécurité. On estime que cette solution est réalisable à travers le contrôle de la disponibilité de l'information indépendamment de l'objet qui l'héberge. Ceci conduit à un modèle à trois composants : Sujet, Objet, Donnée, permettant un contrôle de sécurité appliqué à l'information, en plus de l'objet qui la renferme et du sujet qui l'accède (Figure 18).

Figure 18. Modèle de sécurité à trois niveaux

5.2 GBFC : Description détaillée du modèle

Le modèle de contrôle de flux basé sur la granularité (GBFC) assure la sécurité des flux d'informations travers un processus impliquant un engin de gestion d'accès (EGA) qui est le composant de base du système. Les documents (ou ressources en général) sont accessibles dans leur forme granulaire assurant que, pour chaque granule, une étiquette de classification est affixée lors de sa création ou de sa modification [81].

A une demande d'accès à la ressource classifiée par un sujet *S*, celui-ci est tout d'abord authentifié et ses droits d'accès sont vérifiés par le système de contrôle d'accès en place (MAC, DAC, RBAC …) pour accorder ou refuser l'accès. Une fois autorisé, les droits

d'accès sont passés à l'EGA, et un ensemble de paramètres de sécurité applicables à l'information *Inf* sont chargés. Ces paramètres sont :

- Niveau de granularité $T\gamma$*:* Définit le niveau de granularité appliqué au document *(exemples : Granule = mot, Granule = phrase, Granule = paragraphe, etc.).* Ce paramètre définit le niveau d'atomicité du texte au sein du document et sert à définir les niveaux auxquels s'appliqueront les classifications du contenu granulaire à travers un processus de marquage *(tagging).* Les valeurs de $T\gamma$ dépendent du choix de l'administrateur de sécurité et peuvent être fixées de façon uniforme pour tout un document ou en fonction de sa structure et de ses composants. Dans une configuration simple, $T\gamma$ pourrait se faire affecter le niveau PHRASE pour tout le document par exemple. Si une configuration plus complexe est requise $T\gamma$ pourrait -par exemple- correspondre au niveau MOT pour certaines sections du document, au niveau PHRASE pour d'autres, et ainsi de suite (Figure 19). A ce stade de la recherche, on considère que pour un document, le même niveau de granularité est appliqué à tout son contenu, soit un niveau de granularité unique par document ou ressource. Il est à noter qu'un granule est considéré comme une entité indivisible sur laquelle les paramètres de sécurité sont appliqués en intégralité.

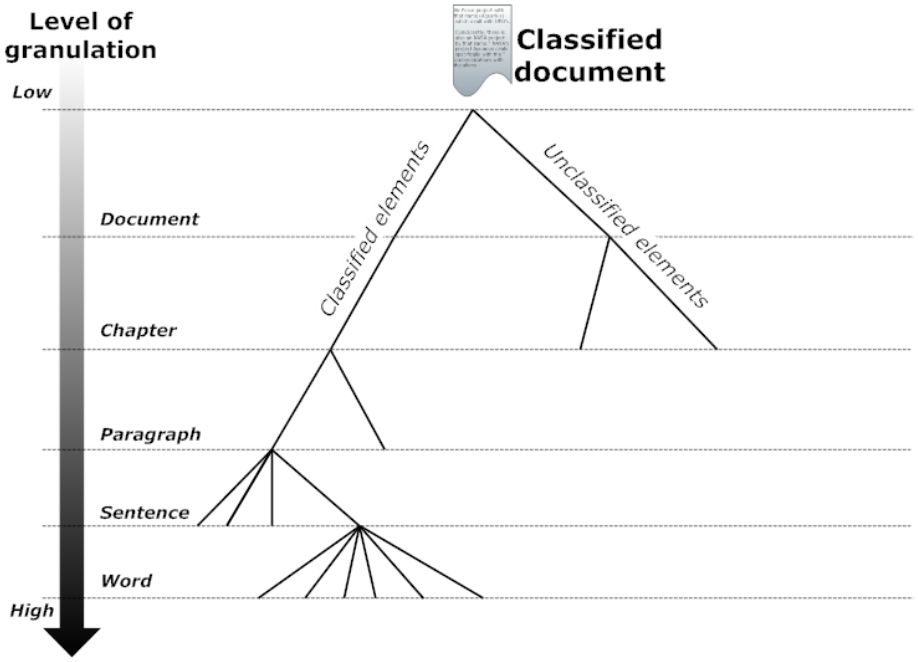


Figure 19. Classification granulaire

- Taux de disponibilité *Tα :* Énumère les différents seuils appliqués aux granules de texte et qui sont utilisés pour limiter le flux (disponibilité) des granules du document qui se verront remplacés par des références et accédés a travers des pointeurs. Afin de réaliser cette opération, ce taux se base sur deux critères :

- La *nature des données à exclure du flux* et qui feront l'objet de référencement et d'ajout à un index d'Allocation de Fichiers Volatile (AFV) qu'on définira dans l'encadré 1 ci-après. (exemples : noms, verbes, dates, etc.)
- Le *niveau de classification à adopter* pour appliquer la restriction de flux (exemple : Si *Tα* est fixé à SECRET, tous les granules classifiés de niveau SECRET et au delà seront référencés dans l'AFV. Tous les autres seront accessibles sans restrictions).

Notons que le niveau de classification d'un granule correspond au plus haut niveau de classification de ses composants élémentaires. Par exemple, si le niveau de granularité d'un document est défini comme étant PARAGRAPHE, et un seul mot du paragraphe est classifié TOP SECRET, le paragraphe tout entier est classifié TOP SECRET.

- **Taux de rafraîchissement** $T\rho$*:* Définit les critères et/ou la fréquence appliqués pour le rafraîchissement des références aux données classifiées au sein du document. Ce taux peut être une fréquence de rafraîchissement pour les environnements qui nécessitent des contrôles de sécurité périodiques. Il peut aussi correspondre à un ou plusieurs critères événementiels tel un licenciement ou une attaque malveillante, ... L'application de ce taux de rafraîchissement ajoute un aspect dynamique au modèle GBFC. Ceci garantit une sécurité accrue même dans des environnements et des situations très évolutifs où les critères de sécurité nécessitent une gestion dynamique. Plus de détails et d'exemples de cette action de rafraîchissement sont développés dans les sections 6.2.1.3 et 6.2.3 du chapitre 6.

- **Niveau de bruit** $T\nu$*:* Représente la quantité de bruit introduite dans le document pour remplacer les références aux granules classifiés non disponibles au sujet. Ce niveau de bruit définit le seuil de classification des granules à remplacer par du bruit en cas d'accès non autorisé.

Le tableau ci-dessous regroupe les paramètres de sécurité selon leur domaine d'action :

	Accès granulaire	**Limitation de flux**	**Disponibilité**
Paramètres de contrôle	- Niveau de granularité T_γ	- Taux de rafraîchissement T_ρ	- Taux de disponibilité T_α - Niveau de bruit T_ν

Table 5. Paramètres de sécurité du GBFC

Le Tableau 6 fournit le détail des quatre paramètres et les valeurs qu'ils prennent dépendamment du niveau de sécurité à renforcer (faible/élevé) :

Critères de Sécurité		**Niveau de sécurité**		**Exemples**
		Bas	**Haut**	
$T\gamma$		Document	Mot	*Mot, Phrase …*
$T\alpha$	Type de données	Tous	Aucun	*Noms, Verbes, Dates…*
	Classification	Non classifiée	Top Secret	*(TS), (S), (C), (U) …*
$T\rho$	Sur Événement	Aucun	Maximum	*Mise à jour, Infection, Échec du system…*
	Par Fréquence	Jamais	Élevée	*Mensuel, quotidien, …*
$T\nu$		Pas de bruit	Max bruit	*Type de données du Tα (Noms, Verbes, …)*

Table 6. Valeurs des paramètres de sécurité du GBFC

Après avoir chargé ces critères de sécurité, l'information *Inf* est chargée sur la base des attributs de sécurité des granules qui la composent. Le système accède alors chaque granule d'information gr_i et vérifie son niveau de classification. Si *S* a le droit d'accès à un granule classifié gr_i, le système crée une référence au contenu du granule et l'ajoute à l'index d'Allocation de Fichiers Volatile (une entrée est ajoutée à l'*AFV* pour chaque niveau de classification). Sinon, si *S* n'a pas le droit d'accès à gr_i le système crée une référence vide ou de bruit et l'ajoute à l'*AFV* sur la base du taux de bruit $T\nu$ prédéfini. Au cas où gr_i correspond à une donnée non classifiée (publique), le système ajoute gr_i sous forme d'une entrée d'index à l'index d'Allocation de Fichiers standard (*AF)* défini dans l'encadré 2 ci-après.

Encadré 1

Allocation de Fichiers Volatile *(AFV)* :

(*Ang. Volatile File Allocation VFA*)

Il s'agit d'une méthode d'allocation de fichiers temporaire qui assure le maintien et la sauvegarde des références aux données classifiées du fichier. Les données référencées sont localisées dans des serveurs ou autres sources de données brutes. Cette AFV est générée par l'Engin de Gestion d'Accès (EGA) sur la base du contenu classifié du document à accéder. C'est généralement une table d'indexes qui, dans notre modèle, sera volatile, et sera rafraichie selon un seuil défini par l'EGA dépendamment du niveau de classification des données.

Par la suite, le système construit l'*AFV* renfermant les références aux granules de données ou de bruit ainsi que l'*AF* pour les données non classifiées sur le système du sujet *S*. Une fois chargées sur le système du sujet, les références volatiles sur l'*AFV* sont actualisées sur la base de $T\rho$, $T\alpha$ et $T\nu$ et une re-granulation (optionnelle) de *Inf* est opérée. Le système est alors prêt à charger l'information suivante et procéder de la même manière jusqu'à la fin du document ou de la ressource.

La Figure 20 ci-dessous illustre ce processus :

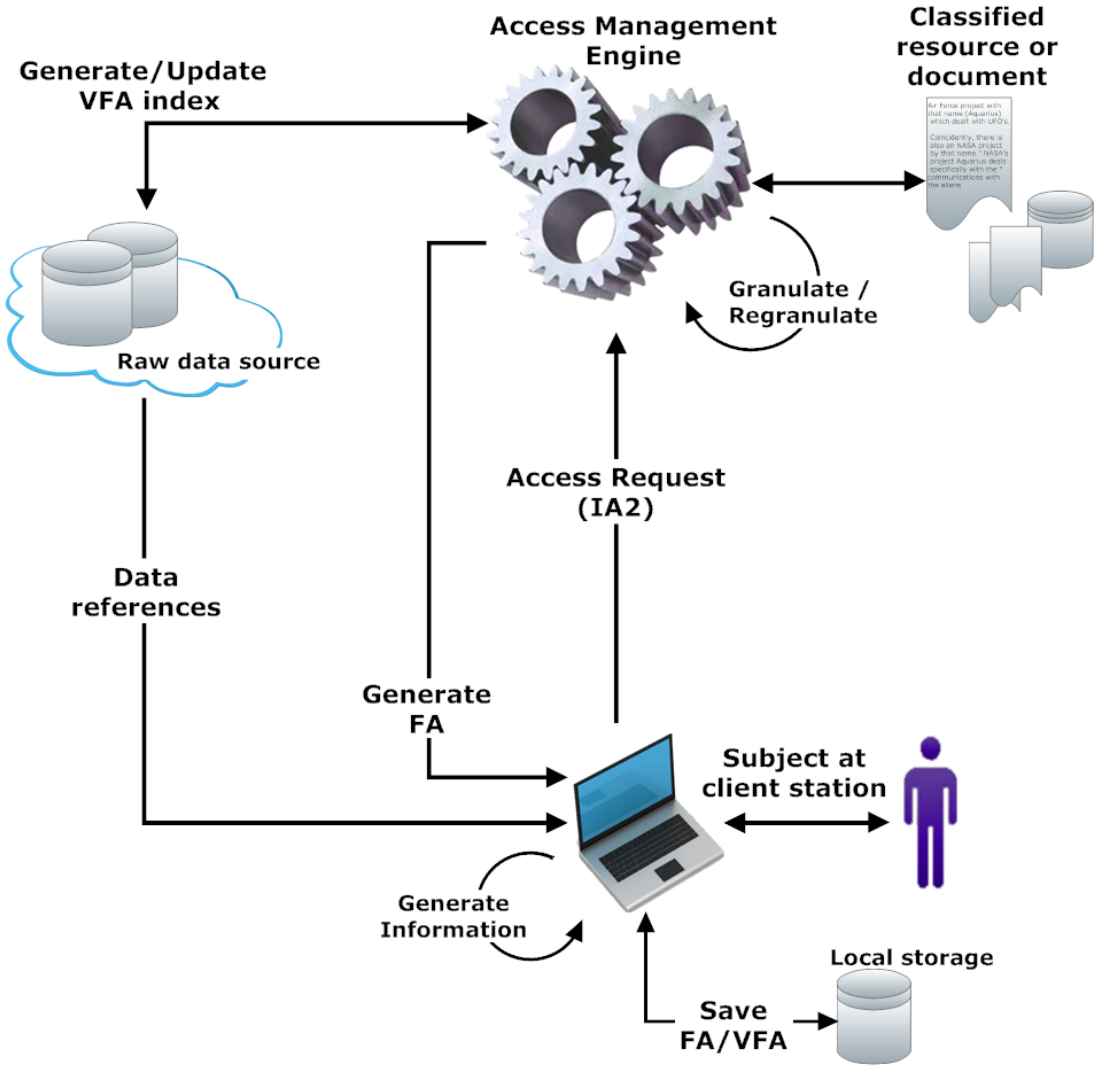


Figure 20. Processus de contrôle de flux du GBFC

Si le document est sauvegardé localement, puis rouvert par le même sujet, les références sont chargées localement puis transférées à l'EGA pour construire les liens vers les granules de données et permettre de recharger le contenu granulaire du document classifié.

Toutes reproductions, copies partielles ou transferts du document confidentiel sont réalisés de manière à conserver les informations classifiées confidentielles en ne copiant ou transférant que les références correspondant aux granules d'information réelle. Cela garantit que tout sujet non authentifié qui tente d'accéder au document aurait seulement accès aux références aux granules d'information qui ne peuvent pas être chargés sur le système client.

Lorsqu'un niveau de contrôle de sécurité plus élevé est nécessaire ces références sont remplacées par du bruit (injection de bruit) par l'action de l'EGA.

Encadré 2

Allocation de Fichiers *(AF)* : *(Ang. File Allocation FA*)

Il s'agit de la méthode d'allocation de fichiers classique sous forme d'indexes enregistrés sur des supports de stockage et qui renferment les adresses des blocs physiques correspondant au fichier logique afin de simplifier son accès et manipulation [122]. Cette Allocation de fichiers peut prendre plusieurs formes dépendamment de l'implémentation: FAT, index, NFS, etc. Dans notre modèle, l'AF renferme :

- Les informations techniques sur le fichier (type, entêtes, date de création, …)
- Références aux données publiques (non classifiées)
- Références de positionnement : Permettent une localisation des données du fichier sur le support de stockage afin de permettre un positionnement correct du prochain bloc de données à charger après le rafraichissement de *l'AFV*. De plus, ces références sont utilisées dans les opérations mise à jour en cas d'accès en écriture.

Les exemples ci-dessous illustrent l'utilisation des différents paramètres de sécurité de notre modèle:

Exemple 1.

$T\gamma$=Mot
$T\alpha$=((Noms, Verbes), (TS))
$T\rho$=(Mise à jours, Infections)
$T\nu$=(Noms)

Dans ce premier exemple, les informations classifiées dans le document seront granulées au niveau mot. Tous les noms et verbes TOP SECRET seront remplacés par des références. Le rafraîchissement des références est réalisé suite aux mises à jour ou suite à une infection. Seules les références aux noms seront remplacées par du bruit en cas d'accès illégal.

Exemple 2.

Tγ=Phrase
Tα=((TOUT), (TS))
Tρ=Aucun
Tν=TOUT

Ici, les informations classifiées dans le document sont granulées au niveau phrase. Tous les éléments de texte des phrases classés TOP SECRET seront remplacés par des références. Aucun rafraîchissement des références n'est opéré. Toutes les phrases classifiées seront remplacées par du bruit (phrases non pertinentes) en cas d'accès illégal.

Exemple 3.

Tγ=Mot
Tα=((Noms, Verbes, Dates, Abréviations, Adjectifs), (S))
Tρ= (Mise à jours, Mensuel)
Tν= (Noms, Verbes, Dates)

Les informations classifiées dans le document seront granulées au niveau mot. Tous les noms, verbes, dates, abréviations et adjectifs classés SECRET ou plus seront remplacés par des références. Le rafraîchissement des références est effectué suite aux mises à jour et périodiquement (tous les mois). Seules les références aux noms, aux verbes et aux dates seront remplacées par du bruit en cas d'accès illégal.

Le Tableau 7 présente les différents scénarios d'accès du GBFC relativement à l'authentification du sujet et au niveau du risque lors d'un flux d'informations confidentielles. Un exemple plus élaboré est offert dans la Section 5.4 de ce chapitre.

Sujet	À droit d'accès	N'a pas de droit d'accès.	Niveau de risque
Authentifié	Références pointent vers les granules d'information.	Reçoit le document déclassifié	**Pas de risque**
Non-Authentifié Accrédité		Références pointent vers nul, vide ou bruit	**Moindre risque**
Non-Authentifié Malveillant		Références pointent vers du bruit	**Haut risque**

Table 7. Scénarios d'accès après un flux d'informations

Le diagramme de flux du GBFC se présente ainsi :

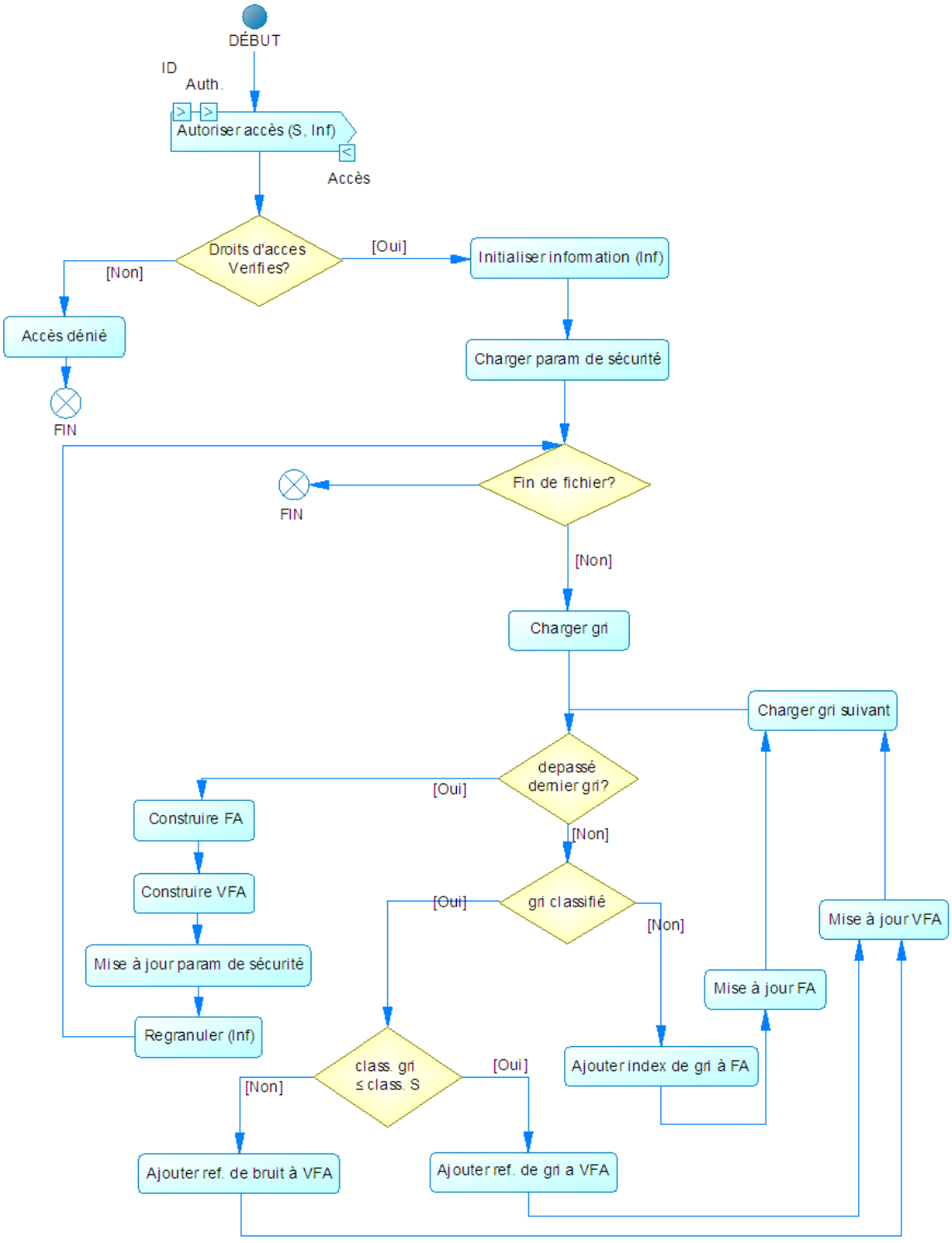


Figure 21. Diagramme de flux du GBFC *(version simplifiée)*

Ce diagramme de flux (Figure 21) illustre le processus d'accès aux données granulaires d'un document classifié pour le cas de sujets légitimes et illégitimes. Dans ce diagramme le scénario préconisé en cas d'accès illégitime est un scénario pessimiste (haut risque). Ainsi, toutes les références vers les granules classifiés pointent vers du bruit.

L'algorithme de base de notre modèle est dressé ci-dessous :

```
============================================================
Title:      Granularity Based Flow Control Algorithm
Author:   Omar Abahmane
Version:  1.1 (explicit noise handling version)
============================================================
1.      begin
2.      V:=AuthorizeAccess(S, Inf)
3.      if  V=False    then
4.          accessDenied()
5.      else
6.          initializeInformation(Inf)
7.          load Tγ, Tρ , Tα, Tν
8.          while(not EOF)
9.             for each gr_i ∈ Inf
10.              if  (gr_i.attr ∈ classified  and gr_i.attr <= S.attr)  then
11.                  addRef  (VFA, gr_i.ref)
12.                  updateVFA()
13.              else if  (gr_i.attr ∈ classified  and gr_i.attr > S.attr)  then
14.                  addRef  (VFA, noise.ref)
15.                  updateVFA()
16.              else
17.                  addIndex (FA, gr_i.idex)
18.                  updateFA()
19.              end if
20.            end for
21.            buildVFA()
22.            buildFA()
23.            refreshRef(Tρ, Tα, Tν)
24.            regranulate(Inf, Tγ)
25.         end while
26.     end if
27.     end
```

Le Tableau 8 présente un descriptif de cet algorithme.

Ligne	Action
2	*Subject S IA2 and Inf classifications verification*
3	*No access rights*
6	*Read document/Resource*
7	*Read document/Resource security variables*
10	*S has access right to gri ?*
11	*Create gri reference and add it to the Virtual File Allocation*
12	*Add an entry to the VFA for each level of classification*
13	*S has no access right to gri ?*
14	*Create noise reference and add it to the VFA based on $T\beta$*
16	*gri unclassified (public)*
17	*Add gri index entry to the File Allocation*
18	*Build FA for public data*
21	*Build VFA to load pack granules references or noise references on subject system*
22	*Build FA to load pack public granules on subject system*
23	*Refresh references based on $F\rho$, $T\delta$ and $T\beta$*
24	*(Optional) Regranulate Inf*

Table 8. Tableau descriptif de l'algorithme du GBFC

5.3 Avantages du modèle

Le modèle GBFC offre plusieurs avantages quant à la protection contre les flux illégitimes des informations confidentielles et au contrôle de flux en général. On traitera dans cette section certains de ces avantages qui seront abordés avec plus de formalisme dans le Chapitre 6 de cette thèse.

5.3.1 Maniabilité

L'implémentation du modèle repose sur quatre principaux axes :

- **Accès granulaire**
- **Limitation et restriction de flux**
- **Disponibilité**
- **Injection de bruit**

Ceci permet une maniabilité accrue grâce à la possibilité de configurer de façon indépendante chacun des paramètres de sécurité suivants :

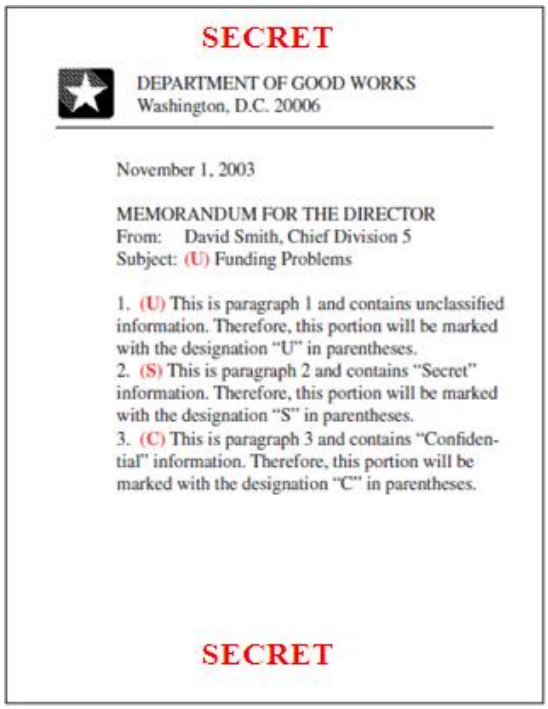
- **Niveau de granularité** $T\gamma$
- **Taux de disponibilité** $T\alpha$

- **Taux de rafraîchissement** $T\rho$
- **Niveau de bruit** $T\nu$

Cette maniabilité offre aux administrateurs de sécurité un environnement multicritères flexible permettant de facilement appliquer le niveau de sécurité souhaité afin de garantir un contrôle de flux d'informations optimale.

5.3.2 Limite d'accès et de reproduction d'information

Les procédures de classification des informations au sein d'organisations et de services à haut niveau de sécurité renforcent la classification de documents sur la base de leur contenu élémentaire. En effet, en cas de création d'un document dérivé à partir de plusieurs sources d'informations à différents niveaux de classification, les guides d'application des classifications aux informations (DoD par exemple) stipulent : le document dérivé devra être annoté en haut et en bas avec la valeur du plus haut niveau de classification de l'information trouvée dans n'importe quelle portion du document [117, 118, 43] (Figure 22).


SECRET

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

November 1, 2003

MEMORANDUM FOR THE DIRECTOR
From: David Smith, Chief Division 5
Subject: (U) Funding Problems

1. (U) This is paragraph 1 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.
2. (S) This is paragraph 2 and contains "Secret" information. Therefore, this portion will be marked with the designation "S" in parentheses.
3. (C) This is paragraph 3 and contains "Confidential" information. Therefore, this portion will be marked with the designation "C" in parentheses.

SECRET

Figure 22. Exemple de document classifié confidentiel

En d'autres termes, si un document de 100 pages, par exemple, comporte une seule phrase classifiée comme TOP SECRET *(TS)* et une page comme SECRET *(S)* et le reste est NON CLASSIFIÉ *(U)*, le document tout entier est classifié comme TOP SECRET.

C'est une application simple des directives du modèle de contrôle d'accès obligatoire (MAC) qui présente deux inconvénients majeurs:

1- L'accès à un document contenant des informations de haut niveau de classification ne peut être accordé à des sujets de moindre niveau de sécurité même en l'existence de données auxquelles ils devraient théoriquement avoir droit d'accès de part leur niveau d'autorisation et leurs droits d'accès. Cela est effectivement dû à l'existence de certaines données auxquelles ils n'ont pas droit d'accès dans le document.

2- Pour résoudre le problème d'accès mentionné en 1, il faudra procéder à une reclassification par la création de documents dérivés refermant les informations appropriées et adéquates pour chaque groupe de niveau de sécurité homogène. C'est-à-dire, la copie originale pour le niveau TOP SECRET, une copie dérivée pour le niveau SECRET (enlevées les informations classifiées TOP SECRET), une copie dérivée pour le niveau CONFIDENTIEL (enlevées les informations classifies TOP SECRET et SECRET), et ainsi de suite. On se trouvera à la fin avec autant de copies du document que de niveaux de classification qu'il renferme. Ceci engendre une charge de traitement supplémentaire pour créer ces copies de document dont l'existence représente par elle-même un risque de sécurité.

Notre méthode remédie à ces deux problèmes en proposant une structure granulaire du document qui, dans sa version originale pouvant être unique, est accessible par les sujets à différents niveaux de sécurité pour n'avoir accès qu'aux informations auxquelles ils ont droit tenant compte de leurs niveaux de classification. Ainsi, un sujet ayant un niveau TOP SECRET aura accès à la version intégrale, un sujet ayant un niveau SECRET aura accès au même document et mêmes informations excepté celles classifiées TOP SECRET (qui seront masquées), et ainsi de suite. Les informations non accessibles masquées pour un

sujet donné sont remplacées par des références vides ou nulles, ou par du bruit dépendamment du niveau de risque à considérer.

Il est à noter qu'à un haut niveau de granularité, les mots classifiés confidentiels peuvent être remplacés par des mots contextuellement et/ou grammaticalement similaires sous forme de bruit et qui offrent un sens relativement compréhensible. On arrive ainsi à dissimuler l'altération opérée sur le contenu du document devant un sujet non autorisé d'accès. D'autre part, en choisissant un niveau de granularité inférieur (niveau phrase par exemple), l'ensemble de la phrase peut être effacé du document ne laissant aucune évidence de l'existence d'un contenu classifié.

Un éditeur de texte approprié peut aider à la production et à l'organisation de ces documents granulaires selon une architecture client-serveur. Par exemple, les différents niveaux de classification peuvent être identifiés à l'aide de différentes couleurs ou d'étiquettes. Ceci introduit la notion de contrôle d'accès aux informations basé sur les vues (Voir Figure 23 ci-dessous).

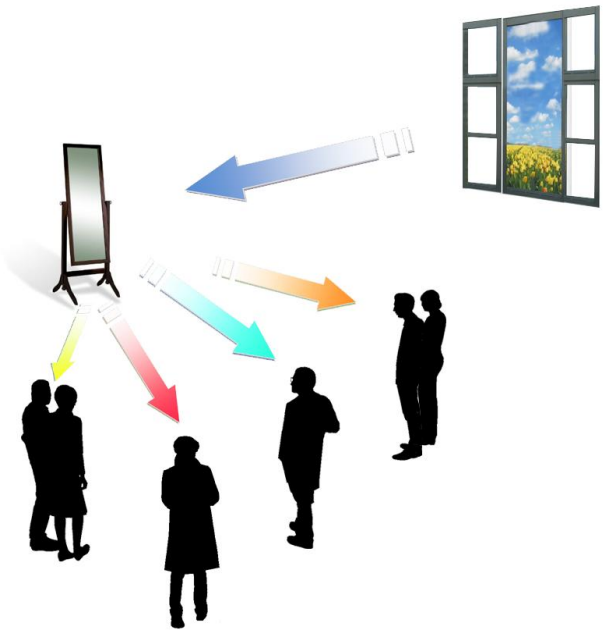


Figure 23. Accès à l'information basé sur les vues

Cette notion qui peut être comparée à une situation où un groupe de personnes localisées dans une chambre regardent tous le même paysage à travers un miroir (par analogie avec l'EGA). Le paysage n'est visible que via une fenêtre ouverte. L'image que chacun arrive à voir dépend de son emplacement et par rapport au miroir qui crée une image virtuelle du paysage. Cette image virtuelle peut changer ou même disparaitre dépendamment des actions entreprises sur le miroir d'un côté, et de l'état de la fenêtre (ouverte, fermée ou mi-ouverte) d'un autre côté.

5.3.3 Contrôle total

La notion de contrôle d'accès aux informations et de contrôle de flux basé sur les vues introduite précédemment permet aux administrateurs des systèmes de sécurité de maitriser l'accès aux informations car elle garantit, à tout moment, une maitrise totale de la localisation des ressources ou documents contenant des informations confidentielles. En effet, contrairement aux systèmes existants où on peut retrouver la ressource classifiée sur plusieurs supports de stockage, dont certains sont mobiles et difficiles à traquer, notre méthode permet un isolement immédiat et automatique des informations classifiées confidentielles à travers l'action de rafraîchissement. Cette action, traitée en détail dans le Chapitre 6, est entreprise en cas d'alerte de sécurité (attaques externe, infection par agents malveillants, risque imminent de fuite volontaire ou involontaire de données, etc.).

Cette situation est similaire à la fermeture de la fenêtre dans l'illustration précédente. Dans ce cas toutes les images virtuelles de la ressource à accéder perdent leurs références aux informations classifiées par le fait de l'isolement qu'elles subissent vis-à-vis du reste du réseau. On est certain que, une fois isolées, ces informations ne sont accessibles sur aucun autre support de stockage. Après le rétablissement de l'état de sécurité, l'accès réseau est rétabli, les références aux informations classifiées sont regénérées et les différents sujets ont de nouveau accès aux informations conformément à leurs droits et autorisations. La création de copies locales est possible pour les informations non

classifiées mais ne devrait pas être possible pour des données confidentielles à moins qu'une perte de contrôle central soit tolérée et avalisée par l'administrateur de sécurité.

5.3.4 Cas de perte d'informations

En cas d'accès distant, les modèles de sécurité actuels contrôlent l'accès aux informations via le processus d'identification, authentification et autorisation et renforcent la sécurité des flux d'informations en utilisant des dispositifs supplémentaires tel le cryptage [20]. Les données à haut niveau de classification sont généralement accédées sur des serveurs et sont rarement sauvegardées sur des systèmes et des supports mobiles (ordinateurs portables, téléphones mobiles, clés USB, …) par souci de perte. Cette crainte est tout à fait justifiée vu les statistiques relatives aux fuites d'informations dues aux pertes de matériel qui s'avèrent très élevées.

Dans, les situations où il est nécessaire de disposer d'informations classifiées confidentielles localement sur des supports de stockage, les organisations veillent à ce que ceux-ci soient les plus sécurisés possible afin qu'en cas de perte, les données ne soient pas accessibles pour des sujets non autorisés.

Cependant, et malgré ces précautions, la perte de matériel reste une des principales causes de fuite d'informations selon les études menées en Amérique du nord, en Europe et en Asie [110, 111, 5].

Avec notre modèle nous proposons une méthode capable de pallier à cette situation du fait de sa conception qui renforce le caractère centralisé de l'information. En effet, en cas de stockage d'un document ou d'une ressource sur un support local, les seules informations qui sont enregistrées sont celles non classifiées. Toutes les informations classifiées sont remplacées par des références aux données réelles. Ces références pointent vers des emplacements contenant des données volatiles dont l'existence dépend de la fréquence de rafraîchissement spécifiée au niveau de l'EGA. Ainsi, tant qu'aucun incident de perte n'est reporté, les références aux données volatiles sont maintenues et l'utilisateur peut accéder

sans problème. En cas de perte, le système procède au rafraîchissement des références aux données sensibles et bloque tout accès utilisant les anciennes références présentes sur le document perdu permettant par la même occasion la traçabilité de l'information et du matériel perdu.

D'autre part, les sujets autorisés ne connaîtront aucun problème d'accès du fait que leurs systèmes obtiennent automatiquement et de façon dynamique les références mises à jour via l'interface client-serveur GBFC qui rafraîchit immédiatement les références présentes dans les documents classifiés. Cette actualisation prend effet une fois que le document est ouvert ou de façon dynamique si elle se produit durant l'accès au document.

Dans des situations plus strictes, la fréquence de rafraîchissement peut être choisie de façon à ne couvrir que des sessions d'accès temporelles limitées, permettant ainsi une sécurité accrue des informations. De plus, durant chaque session, l'utilisateur n'aura accès qu'au contenu autorisé par la session active, soit un accès partiel et séquentiel à des sous ensembles de l'information intégrale. Ceci est très approprié pour des environnements où l'accès total à l'information confidentielle en intégralité présente des risques majeurs de sécurité et de fuites d'informations (exemple : informations bancaires et financières, …).

Un autre avantage de notre modèle consiste en la possibilité de traquer les informations perdues par le biais de l'EGA. En effet, en cas de tentative d'accès par un sujet non authentifié, l'EGA est contacté afin de charger les données classifiées au sein du document. Ce contact permettra de localiser la ressource, par son adresse IP par exemple, et confirmer le niveau de risque engendré par la perte afin de réagir en conséquence.

GBFC sert aussi comme une solution préventive de problèmes d'interception de données confidentielles au niveau des réseaux sans fil (WiFi par exemple) où il est possible d'intercepter des paquets de données circulant sur le réseau. Ce risque est bien présent au sein des organisations qui tentent généralement d'éviter ce problème par l'adoption des réseaux câblés lors de communication d'informations confidentielles. Vu la

forme granulaire que prennent les données dans notre solution et tenant en considération le remplacement du contenu classifié par des références numériques, l'interception de ces données ne permet en aucun cas leur exploitation sous leurs forme actuelles (références) en l'absence d'une validation explicite de l'EGA.

5.3.5 Implémentation et compatibilité

Notre modèle présente un avantage supplémentaire qui consiste en son adaptation facile aux environnements, systèmes et plateformes existantes, vu son implémentation quasiment indépendante du système de sécurité en place. En effet, le modèle repose sur un engin de gestion d'accès qui repose sur les systèmes de sécurité existants pour renforcer le contrôle de flux d'informations sur la base des droits d'accès de l'utilisateur et des classifications des données. Il entre en action aussitôt que l'accès est validé (Identification / Authentification). A ce stade, l'EGA vérifie les autorisations du sujet et procède à la création de la copie volatile de l'information sur la base du niveau de granularité préfixé et des droits d'accès granulaires. La figure ci-dessous illustre l'architecture globale représentant le positionnement du modèle de contrôle de flux basé sur la granularité par rapport aux principaux modèles de sécurité existants. Cette architecture s'avère encore plus avantageuse lorsqu'on se trouve dans des environnements de sécurité hétérogènes ou dans des réseaux étendus tel l'internet. De plus, bien que notre modèle est un modèle qui renforce un contrôle d'accès centralisé, il est conçu pour s'intégrer facilement aux divers modèles de contrôle d'accès aussi bien centralisés tel MAC, que décentralisés comme DAC ou hybrides comme RBAC. Il permet de consolider les méthodes de contrôle d'accès centralisées et construit un environnement de sécurité centralisé pour les méthodes qui ne le sont pas en vue de renforcer la sécurité et le contrôle de flux (Figure 24).

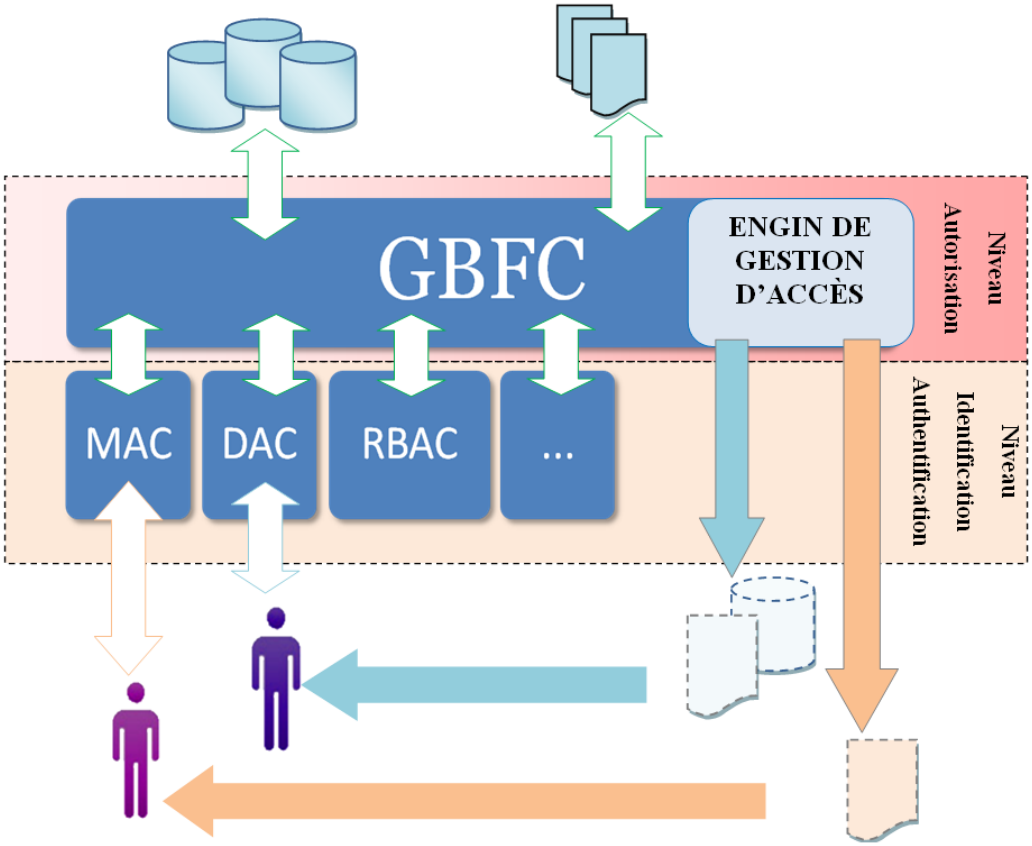


Figure 24. Implémentation et compatibilité du GBFC

Cette architecture permet également de mettre en œuvre le contrôle de flux pour les modèles de sécurité qui ne le supportent pas tels que DAC, ABAC-XACML et autres.

La Figure 24 décrit de façon sommaire le mécanisme d'intégration du GBFC avec certains models de contrôle d'accès conventionnels pour renforcer le contrôle de flux d'informations. Cette figure attribue les tâches d'identification et d'autorisations au modèles préétablis et déjà en place dans les organisations (se basant sur l'identité, les classifications, les rôles, les attributs, etc.), Par la suite, le modèle GBFC assure la fonction de gestion d'accès se basant sur les autorisations. Ceci est fait via l'analyse du couple *ID-&gr*$_i$ discutée dans la section 6.2.1.4 du chapitre 6. Aussitôt vérifié que le sujet est autorisé à accéder la ressource confidentielle (document, base de donnée,…), celle-ci est chargée par l'EGA, puis granulée et réorganisée selon les critères de sécurité du GBFC prédéfinis pour la ressource (création des références pour les granules confidentiels, rafraichissement

et injection de bruit) comme décrit dans le processus de la Section 5.2. Une fois les critères de sécurité sont appliqués à la ressource, les granules non classifiés sont renvoyés à la station client sans restriction d'accès ou de flux. Quant aux granules classifiés, seules les références correspondantes sont renvoyées à la station client pour permettre uniquement un accès indirect basé sur les références (détail de ce mécanisme fourni dans la section 5.2 et formalisé dans les Sections 6.2.1.2 et 6.2.2 du Chapitre 6). Il est à noter que les détails techniques et les mécanismes d'interactions entre notre modèle et les modèles conventionnel ne sont pas traités dans le cadre de cette thèse et pourront faire objet d'études individuelles plus détaillées par la suite. Il est aussi à préciser que la possibilité d'intégration du GBFC avec les divers modèles de contrôle d'accès existants est discutée et vérifiée dans la Section 6.3.1.1 du Chapitre 6.

5.3.6 Injection de bruit

Dans notre modèle, nous utilisons l'idée d'introduction et de combinaison de bruit avec les données comme un mécanisme de protection de l'information confidentielle. L'injection de bruit est un obstacle devant la reconstruction de l'information par déduction. En d'autres termes, la difficulté de reconstituer un document ou un texte est amplifiée par l'existence de données inexactes ou non pertinentes. Pour cette raison, nous avons introduit un paramètre $T\nu$ de niveau de bruit qui fixe le niveau de classification et les types de données qui seront remplacées par du bruit en cas d'accès illégitime. Plus ce niveau est élevé, plus est difficile la reconstruction de l'information initiale. $T\nu$ permet à l'administrateur de sécurité de catégoriser un document comme "sans bruit" pour les sujets de confiance qui ont besoin d'accéder aux données NON CLASSIFIÉES incorporées dans le document ou comme "total bruit" pour des sujets ou des environnements éventuellement offensifs.

À notre connaissance, notre modèle est le premier à introduire ce nouveau concept de dissolution d'information dans un environnement brouillé pour préserver la confidentialité.

Ce processus est assez simple à mettre en œuvre parce que l'EGA maintient le processus de rafraîchissement des références aux granules d'information confidentielle. Par conséquent, il peut remplacer ces références aux données par des références au bruit en cas de besoin. Le bruit se présente sous forme de données brutes sélectionnées de façon rationnelle (application des règles syntaxiques mot à mot comme dans l'exemple de la Section 5.4) ou de façon arbitraire (remplacé par des mots au hasard). Avec des informations dissoutes dans du bruit, les sujets malveillants sont confrontés à des informations pertinentes dissoutes dans un grand lot d'informations erronées ou non pertinentes rendant la distinction entre les deux tâche ardue. Cela rend très difficile, voire impossible tout effort d'inférer les éléments d'informations classifiées manquantes, répondant ainsi à un autre problème de sécurité important. Une recherche plus approfondie s'avère nécessaire dans ce sens.

Le niveau de bruit servira ainsi à dissuader toute utilisation malveillante de l'information par des sujets non autorisés. En effet, se basant sur la localisation -par exemple- d'un sujet qui tente d'accéder à un document classifié, l'administrateur du système de sécurité peut fixer un niveau de bruit très élevé pour une catégorie d'utilisateurs qu'il jugerait offensive en présence d'informations même non classifiées (inférence). D'autre part, il pourra fixer ce niveau à zéro pour tout accès émanant du réseau de l'organisation afin de permettre aux utilisateurs d'accéder aux données publiques auxquelles ils ont droit. Ou encore proposer une solution intermédiaire avec avertissement de présence de bruit pour d'autres utilisateurs non autorisés mais ayant essayé d'accéder de bonne fois (Tableau 7, plus haut).

5.4 Exemples d'implémentation

GBFC devrait être implémenté au niveau système d'exploitation pour pouvoir intégrer la puissance du système d'allocation de fichiers volatil. Toutefois, afin de démontrer l'idée de ce modèle un prototype de niveau application est une première étape. Ce prototype (détaillé dans le Chapitre 7) comporte une interface client-serveur (EGA / Client Éditeur)

permettant à l'autorité centrale de sécurité de gérer et contrôler les niveaux de granularité, les classifications et les autres paramètres de sécurité ($T\rho$, $T\alpha$, $T\nu$) et offrir à l'utilisateur final le droit d'accès dont il a besoin. Dans cette section, on présente diverses possibilités qu'offre le modèle de contrôle de flux basé sur la granularité relativement au contrôle de flux d'informations. La référence [119] est un exemple de document confidentiel classifié TOP SECRET qui a été déclassifié et que nous allons utiliser pour notre exemple, après une certaine simplification et manipulation. Nous considérons le paragraphe extrait après que nous l'ayons traité avec l'outil de classification pour protéger les informations confidentielles qu'il renferme. Le résultat est un paragraphe dans lequel sont insérées des étiquettes de sécurité correspondant aux niveaux de classifications appliqués au contenu.

(TS) Every individual in a command center responsible for the preparation of emergency action must be familiar with the procedures in the EAP ***(/TS)***. ***(U)*** Command center training and evaluation programs will be developed to ensure that individuals charged with the preparation and transmission of emergency action messages are qualified in this task ***(/U)***. ***(S)*** These individuals and programs are subject to review by the OJCS ***(/S)***.

On fixe les paramètres de sécurité comme suit :

$T\gamma$=Mot
$T\alpha$= ((Noms, Verbes, Abréviations, Dates), (S))
$T\rho$= (Mise à jour, Mensuel)
$T\nu$= (Noms, Verbes, Abréviations)

Considérons pour notre exemple 4 sujets ayant les droits d'accès suivants :

- TSungani TOP SECRET (TS)
- Sue SECRET *(S)*
- NAolin Non-autorisé / Accrédité (Authentifié ou non, de bonne foi)
- NAHacker Non-authentifié / Non accrédité (éventuellement sujet malveillant)

TSungani à droit d'accès à l'intégralité du texte du document.

Sur la base de ses droits d'accès, Sue arrivera à visualiser le texte comme suit:

Command center training and evaluation programs will be developed to ensure that individuals charged with the preparation and transmission of emergency action messages are qualified in this task. These individuals and programs are subject to review by the OJCS.

Se basant sur les niveaux de classifications spécifiés plus haut, les données chargées réellement sur le système de Sue seront :

Command center training and evaluation programs will be developed to ensure that individuals charged with the preparation and transmission of emergency action messages are qualified in this task. These 2F08A829 and 2355EA66 2435F450 3D502CE9 to 324AF563 by the 25466F31.

Il faudra noter que les valeurs de ces références (en hexadécimal dans cet exemple) sont fixées et gérées par l'EGA en ne sont ni accessibles ni visibles aux sujets du système. Comme le niveau de granularité est réglé au niveau Mot, les références aux informations classifiées (SECRET et plus comme fixé par $T\alpha$) seront créées pour chaque valeur figurant dans Tα.

Un sujet authentifié ayant droit d'accès de niveau SECRET (Sue) pourra lire les données réelles référencées par les chiffres ci-dessus. Dans le cas de stockage, copie ou transfert les références sont maintenues et aucune donnée classifiés n'est enregistrés ou copiée localement.

Si Sue transfert délibérément ou non ce document à NAolin, le texte NAolin recevra sera:

Command center training and evaluation programs will be developed to ensure that individuals charged with the preparation and transmission of emergency action messages are qualified in this task. These *NULL* and *NULL NULL NULL to NULL* by the *NULL*.

Étant donné que NAolin est un sujet accrédité mais non-autorisé, les références aux informations classifiées ont été remplacés par *NULL*. Si nous avons besoin d'un niveau de sécurité plus restrictif pour éviter que des données non classifiées soient transférées à des sujets non autorisés, il suffira de définir la Tα à NON-CLASSIFIÉ. Dans ce cas, tous les noms, verbes, abréviations et dates dans le texte seront remplacés par NULL.

Les informations que NAHacker recevra au cas où il obtient l'accès au document seront sous cette forme :

Every aspect in a database solution responsible for the system of agent toolkit integrates call familiar with the languages in the GUI. Command center training and evaluation programs will be developed to ensure that individuals charged with the preparation and transmission of emergency action messages are qualified in this task. These networks and algorithms draw concept to function by the EBML.

Une fois que ce sujet est identifié comme une menace pour l'organisation, en possession du document classifié, l'EGA remplace les éléments de données pertinentes référencées dans le document par du bruit qui va submerger les données non-classifiées accessibles. Dans cet exemple, les composants de bruit (noms, verbes, abréviations) ont été générés à partir d'un dictionnaire d'informatique. Des mécanismes de génération de bruit plus sophistiqués connus dans la pratique de la sécurité d'information peuvent être utilisés en cas de besoin.

Le Tableau 9 ci-dessous illustre le travail accompli par l'EGA pour la gestion et le chargement des références aux informations classifiées confidentielles sur les systèmes des trois utilisateurs et qui sont soumises via l'allocation de fichiers volatile.

Sujet	Loaded Refs.	Noise Refs.	Classified Data Refs.	Classified Data	Noise
Sue	**2F08A829**		**2F08A829**	individuals	
	2355EA66		**2355EA66**	programs	
	2435F450		**2435F450**	are	
	3D502CE9		**3D502CE9**	subject	
	324AF563		**324AF563**	review	
	25466F31		**25466F31**	OJCS	
NAolin	**534490A2**	**534490A2**	2F08A829	individuals	NULL
	534490A2	**534490A2**	2355EA66	programs	NULL
	534490A2	**534490A2**	2435F450	are	NULL
	534490A2	**534490A2**	3D502CE9	subject	NULL
	534490A2	**534490A2**	324AF563	review	NULL
	534490A2	**534490A2**	25466F31	OJCS	NULL
NAHacker	**6F67890A**	**6F67890A**	34443501	individual	Aspect
	7B450021	**7B450021**	356099EF	command	Database
	60A89E45	**60A89E45**	390040B1	center	Solution
	67454B89	**67454B89**	23546609	preparation	System
	645109C4	**645109C4**	238709B1	emergency	agent
	6A450910	**6A450910**	32118CD0	action	Toolkit
	62019B34	**62019B34**	34667500	must	Integrates
	679809CC	**679809CC**	356387E3	be	Call
	61026B10	**61026B10**	3490A34F	procedures	Languages
	62AE4530	**62AE4530**	3337810C	EAP	GUI
	73442000	**73442000**	2F08A829	individuals	Networks
	6938CC23	**6938CC23**	2355EA66	programs	Algorithms
	6B324109	**6B324109**	2435F450	are	Draw
	7318F453	**7318F453**	3D502CE9	subject	Concept
	64009A43	**64009A43**	324AF563	review	Function
	629000CF	**629000CF**	25466F31	OJCS	EBML

Table 9. Gestion des références par l'EGA *(Index du VFA)*

Dans ce même exemple il suffira de changer les paramètres de sécurité pour :

*Tγ=**Paragraphe***
*Tα= ((**Dates**), (**S**))*
Tρ= (Mise à jour, Mensuel)
*Tν=(**S**)*

pour que tout paragraphe qui contient une date classifiée *(S)* soit remplacé par un autre paragraphe de données sous forme de bruit.

Un autre scénario :

$T\gamma$= ***Paragraphe***
$T\alpha$= ((***Dates***), (***Tout***))
$T\rho$= *(Mise à jour, Mensuel)*
$T\nu$=(***U***)

donnera comme résultat que tout paragraphe renfermant une date quelconque (de n'importe quel niveau de classification) sera complètement remplacé par un paragraphe de bruit.

Notons que les éléments de texte (mots, paragraphes, etc.) utilisés comme bruit sont choisis à partir de dictionnaires spéciaux conçus à cette fin. Le choix de bruit se fait sur la base de la catégorie du document (objectif, domaine, mots clés, …) pour opérer un choix de remplacement le plus proche possible de la structure et du contenu du document. Ceci se fera à travers l'application de méthodes et de techniques informatiques du genre traitement automatique du langage naturel (NLP) afin de dissimuler toute manipulation de l'information aux usagers non autorisés (noyer l'information dans du bruit). Cette manipulation introduit un autre domaine de recherche relié à l'application de notre modèle, mais qui ne sera pas développé dans le cadre de cette thèse. On retiendra ce sujet comme perspective de perfectionnement et de travaux futurs sur le modèle.

Chapitre 6 : Modèle logique GBFC

Ce chapitre est dédié à une formalisation logique du modèle de contrôle de flux basé sur la granularité. Autrement dit, la description informelle du chapitre précédent sera présentée en forme précise ce qui permettra de comprendre à fond le fonctionnement du GBFC.

Dans le Chapitre 4, on a souligné certaines des limites des principaux modèles de contrôle d'accès vis-à-vis de l'implémentation du contrôle de flux d'informations. Nous esquisserons une comparaison entre GBFC et ces modèles pour ressortir les avantages de notre modèle et sa capacité à s'intégrer et compléter ces derniers.

Dans notre présent projet de recherche, et dans ce chapitre en particulier, on tentera de proposer une analyse qui appuiera la synthèse faite dans la Section 4.4 du Chapitre 4 et nous servira de méthode formelle de vérification de notre modèle dont le formalisme sera développé par la même occasion. Le présent chapitre tentera donc de développer et d'asseoir les fondements logiques du GBFC et de valider ses capacités par rapports aux modèles existants quant au contrôle de flux et à la prévention de flux illégitimes. A la lumière de ces développements, nous proposons une vérification formelle de notre hypothèse de recherche. Cette vérification est obtenue en faisant une énumération de tous les scenarios possibles d'accès à l'information et nous montrons pour chacun des scénarios que notre modèle arrive à satisfaire l'hypothèse de travail : «prévenir les flux illégitimes dans les divers scénarios d'accès à l'information ». Ainsi, en Section 6.1, on dressera une plateforme de base pour le développement du modèle logique de contrôle de flux basé sur la granularité. Dans la Section 6.2, on dressera le modèle logique du GBFC et de ses mécanismes de sécurité et de contrôle de flux. Par la suite, on adoptera un formalisme général de représentation de chacune des principales familles de modèles de contrôle d'accès afin de pouvoir les comparer avec notre modèle et comparer leurs différents composants (Section 6.3). Finalement, on proposera une analyse de divers scénarios de contrôle de flux couverts par notre modèle (Section 6.4).

6.1 Définitions

Comme mentionné en introduction, cette section dresse un ensemble de définitions de base, de règles et de notations qui seront retenues pour la suite de notre analyse.

6.1.1 Opérations d'accès

Afin de pouvoir disposer d'un modèle cohérent et qui s'intègre dans un cadre de recherche plus général, on adoptera dans cette recherche la notation proposée dans [120] avec quelques adaptations :

Nous utilisons les notations *S* et *O* pour designer respectivement sujets et objets en considérant l'ajout d'indexes et d'apostrophes pour référer aux différentes instances de ces éléments (exemples : *S, S', O_1, O_2,* etc.).

- Soit *X* une information. Le fait que *X* est écrite dans un objet *O* est représenté par la notation $X \in O$. Nous supposons aussi qu'un objet *O* contient une seule information à un moment donné.

Il est à noter que dans les définitions suivantes nous utiliserons des polices différentes pour distinguer la lecture/écriture d'un objet de la lecture/écriture d'une information (respectivement R/W contre $\mathcal{R}/\mathcal{W}$).

Soit les relations suivantes :

1- R(*S* ; *O*) : Un sujet *S* a exécuté une opération de lecture (*Read*) R à partir d'un objet *O*.

2- W(*S* ; [O_1 ,] O_2) : Un sujet *S* a exécuté une opération d'écriture (*Write*) dans un objet O_2 [de l'information contenue dans O_1] (optionnel). W(*S* ; O_1 , O_2) est donc la succession de deux opérations (lecture de O_1 suivie d'une écriture dans O_2) sous forme de copie du contenu d'un objet dans un autre.

3- Étant donné que notre modèle implémente le contrôle d'accès et le contrôle de flux d'informations en prenant en considération en plus des deux composants Sujet et Objet le troisième composant qui est l'information (comme décrit dans la Section 5.1.3 du Chapitre 5), nous préconisons que l'accès en lecture à un objet *O* qui contient l'information, par un sujet *S*, correspond à un accès en lecture à cette information elle-même (*S* a lu *X* à partir de *O*) qu'on notera $\mathcal{R}(S; X, O)$.Notons que la mention de l'objet dans cette opération est optionnelle (exemple : $\mathcal{R}(S; X)$ voudra dire que le sujet *S* a lu l'information *X*).

$$\mathcal{R}(S; X, O) \stackrel{\text{def}}{=} \mathrm{R}(S; O) \mid X \in O. \quad (1)$$

4- Par analogie, une opération d'écriture par un sujet *S* [du contenu d'un objet *O*] dans un objet *O*' correspond à l'écriture d'une information *X* [que contient *O*] dans *O'* par ce sujet, notée : $\mathcal{W}(S; X, [O,] O')$. Encore une fois, les crochets [ ] dénotent la partie optionnelle de cette relation.

$$\mathcal{W}(S; X, [O,] O') \stackrel{\text{def}}{=} \mathrm{W}(S; [O,] O') \mid X \in O. \quad (2)$$

De plus :

5- On désigne par CR(*S* ; *O*) la possibilité pour un sujet *S* d'exécuter une opération de lecture CR (*Can Read*) à partir d'un objet *O*.

6- On désigne par CW (*Can Write*) CW(*S* ; *O*) la possibilité pour un sujet *S* de réaliser une opération d'écriture dans un objet *O*. Pour raison de simplification on désignera par CW(*S* ; O_1 , O_2) la possibilité de "copier" une information présente dans O_1 dans l'objet O_2. Cette possibilité peut être réalisée par une séquence d'opérations de lecture R(*S*; O_1) suivie d'une opération d'écriture W(*S ;* O_2) et qui donne lieu à une copie de l'information $X \in O_1$. Ceci peut être réalisé avec une seule opération W(*S*; O_1, O_2).

7- La relation d'autorisation sujet-information correspond au droit d'accès à cette information *X* par le sujet *S* : Auth(*S* ; *X*). Pour notre recherche, on considère qu'un sujet *S* est autorisé à accéder (a le droit d'accès à) une information *X* s'il peut lire tout objet *O* qui renferme *X :*

$$\mathrm{Auth}(S; X) \stackrel{\text{def}}{=} X \in O \Longrightarrow \mathrm{CR}(S; O) \quad (3)$$

La relation de non autorisation :

$$\mathrm{NotAuth}(S; X) \stackrel{\text{def}}{\cong} X \in O \Longrightarrow \neg \mathrm{CR}(S; O) \quad (4)$$

8- La possibilité de réaliser une opération de lecture d'une information *X* par un sujet *S* à partir d'un objet *O* telle que décrite (dans les définitions des opérations d'accès) plus haut (Alinéa 3) est notée : $\boldsymbol{\mathcal{CR}}(S; X, O)$.

Compte tenu de notre méthodologie basée contrôle de flux, nous adoptons une approche pessimiste concernant le droit d'accès, en supposant qu'une autorisation de lecture implique une autorisation d'écriture. Ce qui signifie qu'un accès en lecture d'un sujet *S* à l'information *X* représente un accès total à celle-ci.

Supposition pessimiste :

$$\forall S, O, \ \mathrm{CR}(S; O) \Rightarrow \exists O' \neq O \mid \mathrm{CW}(S; O, O') \quad (5)$$

Ce choix est entièrement justifié par le fait que les exigences des environnements de travail modernes nécessitent un contrôle assez étendu des informations dans la réalisation des diverses tâches. A cette raison s'ajoute le fait que dans la quasi totalité des situations (copies, modifications, enregistrements,…), les sujets se retrouvent dans des conditions d'accès aux informations multi-domaines, multi-applications et multiservices avec des architectures d'accès distants et Internet.

Dans le contexte de la logique du contrôle d'accès, on définit ci-après les notions de disponibilité, de confidentialité et d'accessibilité de l'information. Par la suite on définit les notions d'accès en lecture/écriture selon un point de vue contrôle de flux en analysant les situations de flux légitime et illégitime.

6.1.1.1 Information disponible

Dans la Section 5.1.3 du Chapitre 5 on a défini la *disponibilité* d'une information dans un domaine de sécurité comme étant le fait qu'elle existe sur un support physique ou logique de ce domaine. En d'autres termes, il existe au moins un objet dans le domaine, sur lequel est écrite cette information :

Définition 1.

D'une façon générale, une information X est *disponible* $\stackrel{\text{def}}{=} \exists\, O \mid X \in O.$ *(6)*

6.1.1.2 Information accessible

De même, pour qu'une information soit *accessible* pour un sujet donné, celle-ci doit premièrement être disponible pour celui-ci et le sujet doit disposer des privilèges nécessaires pour lire cette information.

Définition 2.

X est *accessible* par $S \stackrel{\text{def}}{=} X$ est disponible et $\text{Auth}(S; X)$ *(7)*

$$\stackrel{\text{def}}{=} (\exists\, O \mid X \in O) \wedge (\text{si } X \in O \text{ alors } \text{CR}(S; O)) \text{ selon } (3) \text{ et } (6)$$

Cette définition implique que : $(\exists\, O \mid X \in O) \wedge \text{CR}(S\,;\, O)$, puisque effectivement ici $X \in O$

Il est à noter qu'une information non disponible ne peut être accessible car $\forall\, O \mid X \notin O$

6.1.2 Opérations de flux d'information

6.1.2.1 Flux d'information et flux illégitime

GBFC ainsi que d'autres modèles de contrôle d'accès et de contrôle de flux d'informations opèrent selon des modèles de transition d'état. Ainsi pour illustrer ce mode d'opération nous utiliserons pour la suite de cette recherche la notation t_{n-1}, t_n, t_{n+1}, t_{n+2}, et ainsi de suite, pour illustrer le passage d'un état a un autre.

Dans un contexte de flux d'information on définit ci-après les concepts de contrôle de flux et de fuites d'informations.

Définition 3.

On dit qu'il existe un flux d'information $X \in O$ de l'objet O vers un autre objet O' si et seulement si il existe un sujet qui exécute une lecture à partir de l'objet O contenant l'information puis écrit ce contenu dans le second objet O'

1- Il existe un *flux d'information de X à O'* $\stackrel{\text{def}}{=} X \in O \wedge \exists S, O' \neq O \mid \mathrm{W}(S; O, O')$ *(8)*

2- Un *flux de X est possible* $\stackrel{\text{def}}{=} X \in O \wedge \exists S, O' \neq O \mid \mathrm{CW}(S; O, O')$ *(9)*

Définition 4.

Considérant la définition du *flux illégitime* offerte dans la Section 3.4.1 du Chapitre 3, il existe un flux illégitime d'une information X initié par un sujet S d'un objet O vers un second objet O' si et seulement si : à un état t_{n-1}, X continue d'être disponible dans O, S a copié X dans un objet O' et à un état subséquent t_n, il existe au moins un sujet S' qui n'a pas droit d'accès à X mais qui a lu à partir de O'.

1- A l'état t_{n-1}, $\forall O, S, X \in O, \exists O' \neq O \mid \mathrm{W}(S; O, O')$ *(10)*

2- A l'état t_n, $\exists S' \mid \mathrm{NotAuth}(S'; X) \wedge \mathrm{R}(S'; O')$ *(11)*

Il est à souligner que toutes les définitions offertes dans cette section (Section 6.1) formalisent les diverses opérations d'accès aux objets et les concepts d'autorisations des sujets, de la disponibilité et d'accessibilité de l'information. Ces définitions sont offertes dans le contexte des modèles de sécurité classiques qui préconisent l'utilisation des objets et des sujets pour ces opérations et ces concepts. Ces définitions seront reprises dans le contexte du GBFC dans la Section 6.2.2, pour souligner la différence entre notre modèle et les modèles conventionnels.

6.2 Modèle logique du GBFC

GBFC est un modèle de sécurité multicritères qui implémente le contrôle de flux d'information à travers son aspect granulaire. L'accès à l'information est alors réalisé sur la base de références gérées par le système d'exploitation et qui pointent vers ces granules. Nous parlons de Reference-Based Access Control (détaillé dans la section 6.2.2) pour décrire notre mécanisme d'accès aux granules du GBFC se basant sur les références. Au plus haut niveau des exigences de sécurité, l'administrateur peut appliquer un contrôle de disponibilité pour empêcher les flux d'informations en empêchant l'accès direct aux granules et peut accroître le niveau de confidentialité en injectant des granules de bruit à la place de granules classifiés pertinents afin de décourager l'accès illégitime (Figure 25).

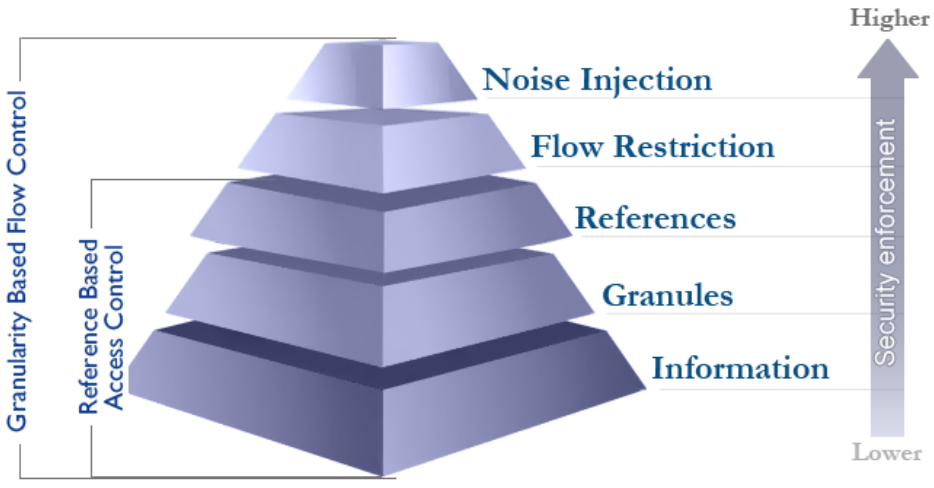


Figure 25. Architecture multi-niveaux du GBFC

6.2.1 Critères de sécurité GBFC

6.2.1.1 Granularité

Dans notre modèle, l'information est manipulée et traitée dans sa forme granulaire (voir Section 5.2 du Chapitre 5). Par conséquent, notre domaine de base est l'information. En

général, une information $X=\{x_1, x_2, x_3, \ldots, x_n\}$ est un ensemble ordonné de n composants atomiques (normalement les mots pour un document texte). Se basant sur les concepts de l'informatique granulaire, et tenant en compte les besoins et exigences de sécurité dans un domaine, l'information est décomposée ou regroupée sur la base du niveau de granularité $T\gamma$ exprimé par l'administrateur de sécurité. Cette granulation de l'information dépend du niveau de détails à prendre en considération et du niveau de sécurité à lui appliquer. De ce fait, l'ensemble des données à considérer dans notre modèle est l'information $X=\{x_1, x_2, x_3, \ldots, x_n\}$ avec $|X|=n$. L'ensemble des granules $Gr_X=\{gr_1, gr_2, gr_3, \ldots, gr_m\}$ constitue une partition de X avec $|Gr_X|=m$ et $m \leq n$. le nombre de sous-ensembles gr_i va de *1* (cas où $Gr_X=gr_1= X$) à m (cas où $m=n$, i.e. le plus haut niveau de granulation). Gr_X est considéré comme partition valide si tous ses éléments sont non vides *(12)*, disjoints deux à deux *(13)* et couvrent tout l'ensemble de données X *(14)* :

- $\forall\, i \in \{1, ..., m\},\ gr_i \neq \emptyset$ *(12)*
- $\forall\, i, j \in \{1, ..., m\},$ si $i \neq j$ alors $gr_i \cap gr_j = \emptyset$ *(13)*
- $\bigcup_{i=1 \ldots m}\ gr_i = X$ *(14)*

La fonction de granulation se définit donc ainsi :

$f:\ X \longrightarrow Gr_X$
$f(x_n) = gr_i \mid x_n \in gr_i$ *(15)*

Donc, à chaque élément d'information $x_i \in X$, il existe un et un seul granule gr_i dans la partition Gr_X qui contient x :

$\forall\, x_n \in X,\ \exists!\ gr_i \in Gr_X \mid x_n \in gr_i$ *(16)*

Dorénavant, et pour la suite de cette recherche, on traitera toute opération de lecture et d'écriture d'information confidentielle sous la forme granulaire selon l'approche GBFC. Ceci veut dire que nous représenterons l'information confidentielle par un granule gr_i avec la possibilité de généralisation des divers concepts et opérations à l'ensemble des granules composant l'information X. Ainsi, les opérations d'accès et les relations qui portent sur X porteront, dans le cadre du GBFC, sur des granules ou des références aux granules

d'informations. Par exemple, des notations telles que : Auth(S; X), $\mathcal{R}(S; X, O)$, $\mathcal{W}(S; X, O)$, $\mathcal{CR}(S; X, O)$ correspondraient respectivement -dans notre modèle- à des notation du genre : Auth(S; gr_i), $\mathcal{R}(S; \&gr_i, O)$, $\mathcal{W}(S; \&gr_i, O, O')$, $\mathcal{CR}(S; \&gr_i, O)$ où $\&gr_i$ dénote la référence au granule gr_i.

6.2.1.2 Contrôle de Disponibilité

GBFC opère selon une architecture client/serveur qui permet de garantir la disponibilité des informations sans pour autant mettre à risque leur confidentialité. Au niveau du serveur, l'Engin de Gestion d'Accès (EGA) permet l'accès via des pointeurs (notés *pr*) aux granules d'informations classifiés gr_i (Section 5.2, Chapitre 5). Ces pointeurs *pr* sont créés et gérés au niveau du serveur et chargés et sauvegardés sous forme de références numériques sur les stations de travail clients dynamiquement et après chaque mise à jour ou rafraîchissement. Ces références $\&gr_i$ sont démunies de toute relation avec les granules d'informations correspondants en l'absence de l'action de référencement opérée par l'EGA. Cette action de référencement crée la relation entre la référence présente sur la station client et le pointeur vers l'information présent au niveau du serveur (Section 5.2, Chapitre 5). En l'absence de cette action de référencement les références dont les sujets disposent sur leurs systèmes peuvent pointer vers du vide ou vers du bruit en cas de risque d'accès ou de flux d'informations illégitimes.

Ces trois composants de base : granule d'information (gr_i) référence au granule ($\&gr_i$) et pointeur vers le granule (*pr*) sont chargés sur des objets au niveau du serveur (pour gr_i et *pr*) et sur les stations clients (pour $\&gr_i$) et sont accédés à travers l'accès à ces objets qui les contiennent. Ces objets peuvent être des fichiers, des secteurs sur disques, des positions mémoires ou autres selon le type et l'utilisation de ces différents composants (Figure 26). Ces trois composants ainsi que les objets qui les renferment sont gérés par le système d'exploitation et ne sont pas perceptibles par les sujets qui accèdent à l'information.

Nous devons, dorénavant, supposer l'existence d'objets *O* contenant des références et nous utiliserons la notation $\&gr_i \in O$ pour dénoter le fait que la référence $\&gr_i$ est écrite dans l'objet. GBFC préconise que tout accès à un granule confidentiel gr_i se fait via sa référence qu'on note $\&gr_i$. L'utilisation de cette notation est analogue à celle de *X* dans la Section 6.1 et de gr_i dans la Section 6.2.1.

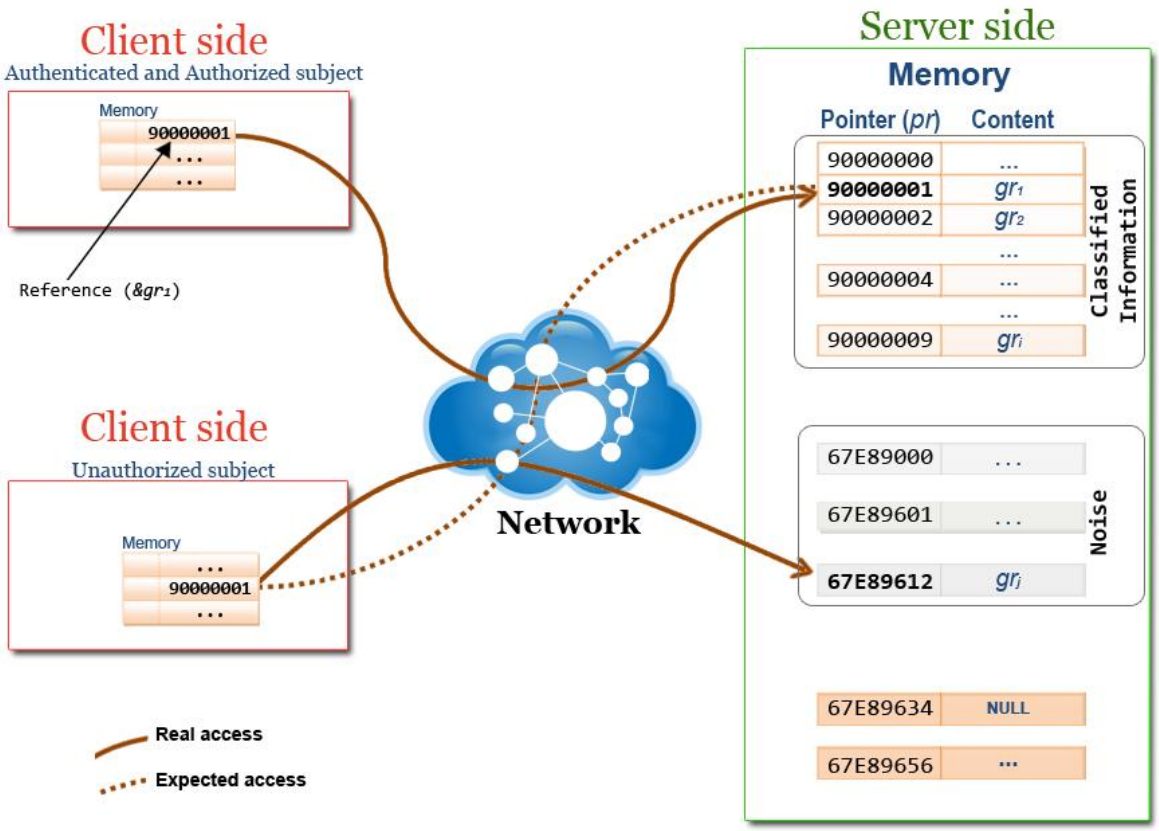


Figure 26. Accès à travers les références

Les granules sujets de cette action de référencement sont des granules classifiés dont la nature et les niveaux de classification sont préfixés dans le taux de disponibilité $T\alpha$.

La fonction de disponibilité (*b*) appliquée aux granules d'information gr_i (voir équation *15*, Section 6.2.1.1) se définit comme suit : $b(gr_i)$

Avec $b(gr_i) = \&gr_i$ *(17)*

Le contrôle de disponibilité est appliqué à un granule gr_i si son niveau de classification ou son niveau de sécurité $L(gr_i)$ est supérieur ou égal au niveau de classification défini dans

le paramètre de disponibilité $T\alpha$ (noté $L_{def}(T\alpha)$). Ce contrôle est concrétisé à travers la permission d'accès à ce granule uniquement via une référence chargée dans un objet au niveau du client et qui correspond au pointeur à gr_i au niveau du serveur. Ainsi, l'EGA du GBFC associe à chaque granule d'information classifié logé dans la mémoire du serveur un pointeur pr ($pr \rightarrow gr_i$), puis crée une référence $\&gr_i$ qui est chargée sur les stations de travail client pour permettre d'accéder le contenu du granule (Figure 26). Dans la Figure 26, nous voyons qu'à chaque granule gr_i présent sur le serveur correspond un pointeur pr unique qui lui est associé et qui sert comme adresse qui pointe vers celui-ci. Parallèlement à cela, la référence au granule d'information $\&gr_i$ est aussi une adresse vers le granule d'information mais qui est chargée sur la station client. Pour un accès légitime, la valeur de la référence est égale à la valeur du pointeur ($\&gr_i = pr$) à travers une action de l'EGA discutée en détail dans la Section 6.2.1.4 et décrite par la Figure 29. Dans le cas d'un accès illégitime, la référence présente sur la station client et qui est utilisée durant la tentative d'accès est modifiée par l'EGA pour ne plus pointer vers le granule d'information mais vers un granule de bruit par exemple, empêchant ainsi l'accès au sujet non autorisé.

Ces références aux granules d'information sont chargées par le système d'exploitation via l'index d'allocation de fichiers (VFA) discuté précédemment.

De cette manière, le contrôle de disponibilité est opéré sur un granule gr_i

si $L(gr_i) \geq L_{def}(T\alpha)$
et $\exists\ O \mid \&gr_i \in O$ et $\&gr_i = pr$ et $pr \rightarrow gr_i$ ($\&gr_i$ étant la référence vers gr_i au niveau du client et pr étant le pointeur vers gr_i au niveau du serveur).

Rappelons à ce point que $T\alpha$ est le niveau de disponibilité qui est établi par l'administrateur de sécurité de sorte que si $L(gr_i) \geq L_{def}(T\alpha)$, le granule gr_i doit être protégé et il est par conséquent uniquement accessible via sa référence $\&gr_i$ (cf. Section 5.2, Chapitre 5).

Dans cette recherche, nous utilisons le terme «*référence*» pour désigner l'adresse que le sujet utilise pour accéder au granule d'information (chargé sur le poste client). Et par «pointeur», nous entendons : l'adresse mémoire du granule d'information qui est associée à la référence à une session donnée. En d'autres termes, une référence est du côté sujet et un pointeur est du côté serveur. Ces deux mots doivent être considérés dans leur contexte le plus général et ne devraient pas être confondus avec les termes correspondants utilisés en langages de programmation (Figure 27). Aussi nous utiliserons les symboles → et ↛ pour designer les états d'un pointeur par rapport à un granule respectivement: « pointe vers » et « ne pointe pas vers ».

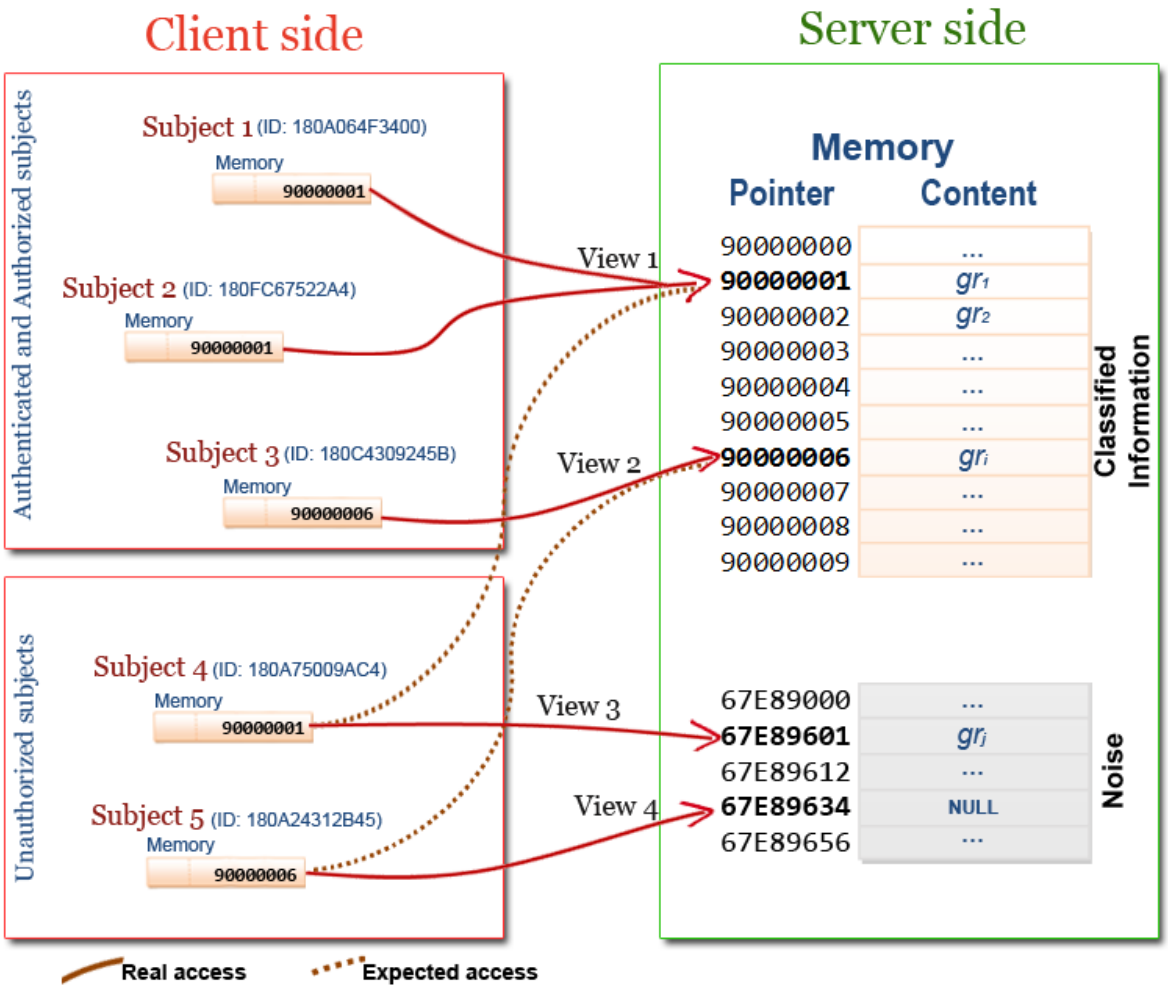


Figure 27. Accès à l'information via des références et des pointeurs

Il faut toutefois préciser que tout granule d'information non soumis au référencement (i.e. $L(gr_i) < L_{det}(T\alpha)$) est accessible directement via l'allocation de fichiers (FA) sans l'utilisation de références. L'accès dans les deux cas est géré par le système d'exploitation et toutes les références et les pointeurs sont imperceptibles par les sujets qui accèdent à l'information.

Pour un granule d'information gr_i, une mise à jour de la référence vers ce granule ($\&gr_i$) peut rendre ce granule d'information classifié indisponible et ceci lorsque la valeur de $\&gr_i$ est égale à la valeur d'un pointeur qui ne pointe pas vers gr_i :

$\&gr_i = pr_k$ et $pr_k \nrightarrow gr_i$ implique que gr_i n'est pas disponible

6.2.1.3 Action de Rafraîchissement

L'action de rafraîchissement (décrite dans la Section 5.2 du Chapitre 5) est un processus éventuel de restriction de flux qui a lieu quand un critère de rafraîchissement défini dans $T\rho$ est satisfait. Cette action consiste en une modification de la valeur du pointeur (pr) vers gr_i. Les références correspondantes au niveau des clients autorisés d'accès sont par conséquent mises à jour pour avoir la même valeur que celle de pr. Le rafraîchissement peut être chronologique et/ou être basé sur des événements qui se produisent. Pour décrire cette action nous représentons l'évolution du système comme une séquence d'états. Par exemple :

A l'état t_0, $\&gr_i = pr_0$ avec $pr_0 \rightarrow gr_i$;
A l'état t_1, $\&gr_i = pr_1$ avec $pr_1 \rightarrow gr_i$ et $pr_1 \neq pr_0$;
A l'état t_2, $\&gr_i = pr_2$ avec $pr_2 \rightarrow gr_i$ et $pr_2 \neq pr_1$;
….
A l'état t_k, $\&gr_i = pr_k$ avec $pr_k \rightarrow gr_i$ et $pr_k \neq pr_{k-1}$; (pr_k étant la valeur du pointeur pr à l'état t_k).

Des exemples d'applications du processus de rafraîchissements sont donnés dans la Section 6.2.3 de ce Chapitre et dans la Section 8.1 du Chapitre 8.

Pour qu'une action de rafraîchissement ait lieu durant une session t_{k+1}, il doit y avoir au moins un critère de rafraîchissement c qui est vrai durant l'état précédent t_k.

Comme règle générale, il y a une action de rafraîchissement si au moins un des critères ou des conditions c énumérés dans le taux de rafraîchissement $T\rho$ est satisfait entre deux états consécutifs t_{k-1} et t_k:

$$(\exists\ c \in \{T\rho\} \mid c = \text{TRUE}) \Rightarrow \&gr_i = pr_k \ \text{ avec } \ pr_k \rightarrow gr_i \text{ et } pr_k \neq pr_{k-1} \text{ et } pr_{k-1} \nrightarrow gr_i \quad (18)$$

Autrement dit, si à un état t_{k-1} une des conditions listées dans $T\rho$ est satisfaite, le système (EGA) procède à une action de rafraîchissement à l'état consécutif t_k.

Similaire à la fonction de disponibilité, l'action de rafraîchissement est une fonction de la disponibilité car elle porte sur les granules classifiés sujets d'un contrôle de disponibilité. Le rafraîchissement est une actualisation des valeurs des références aux granules classifiés à travers la mise à jour des pointeurs à ces granules au niveau du serveur. Ces mises à jour libèrent les anciens pointeurs et leur accordent de nouvelles valeurs distinctes des précédentes.

Fonction de rafraîchissement $h(\&gr_i)$ est une fonction composée de la fonction de disponibilité $b(gr_i)$ (voir équation *17*, Section 6.2.1.2) :

$$h(\&gr_i) = pr_k \ \mid \ pr_k \neq pr_{k-1} \ \textit{et} \ pr_k \rightarrow gr_i \text{ et } pr_{k-1} \nrightarrow gr_i \quad (19)$$

Partant de la Figure 27, et après exécution d'une action de rafraîchissement, on obtient une vue du système similaire à celle de la figure ci-après dans laquelle on remarque les changements opérés sur les pointeurs vers les granules confidentiels et sur les références correspondantes:

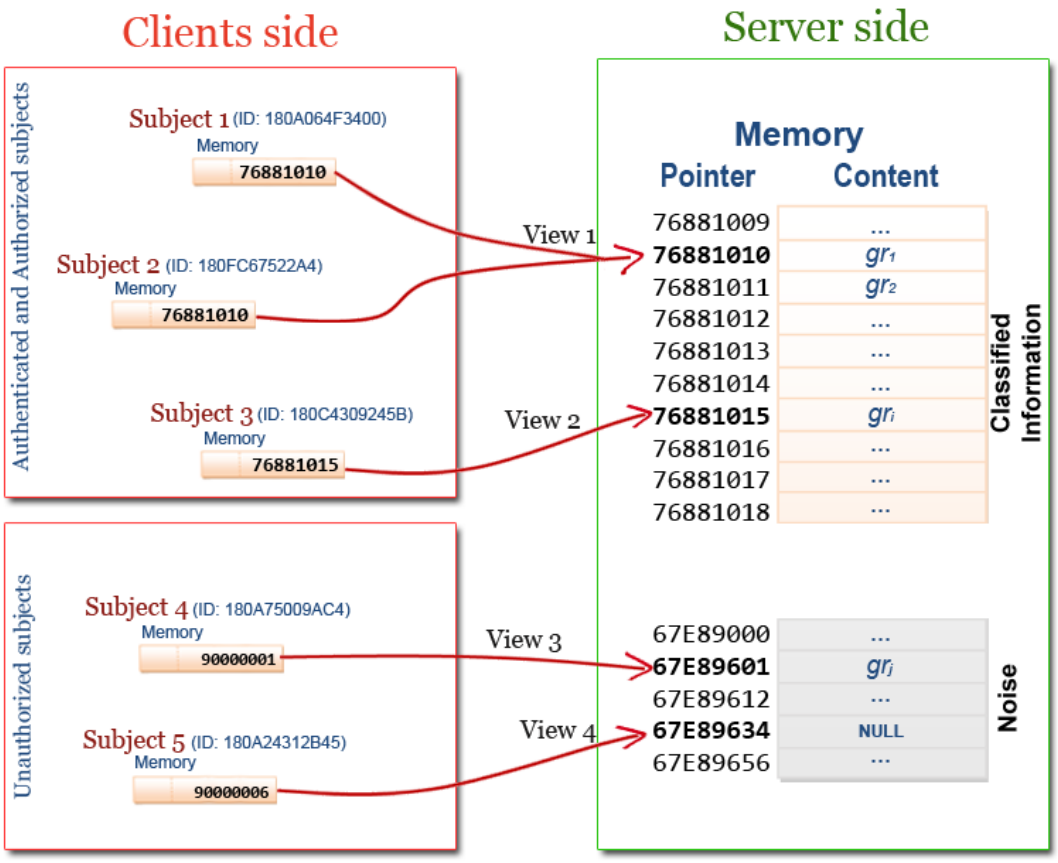


Figure 28. Vue du système après l'action de rafraîchissement

Dans la Figure 28, on constate que l'action de rafraîchissement a mis à jour les pointeurs vers les granules d'information classifiés au niveau du serveur. Suite à cette action, l'EGA s'est chargé de mettre à jour dynamiquement les références de ces granules sur les stations clients des sujets autorisés pour pointer vers les granules correspondants. Les anciennes références dont disposent les sujets non autorisés ne sont plus valables, du fait qu'elles n'ont pas été mises à jour, et leur utilisation dans une opération d'accès les redirige vers des granules nuls ou vers des granules de bruit. Cette notion de références qui pointent vers du bruit sera expliquée en détail dans la section suivante.

6.2.1.4 Injection de bruit

L'injection de bruit, comme décrite dans la Section 5.3.6 du chapitre précédent, est un mécanisme de protection de l'information confidentielle qui consiste en l'introduction de

granules de bruits dans un document confidentiel. Cette action dissuasive rend difficile pour un sujet non autorisé malveillant la distinction entre informations pertinentes et bruit. De point de vue logique c'est une fonction comparable à la fonction de rafraîchissement, qui modifie la référence à un granule d'information gr_i pour pointer vers un granule de bruit sélectionné gr_j (cas du sujet 4 de la Figure 27).

Fonction d'injection de bruit $I(\&gr_i)$ est une fonction composée de la fonction de disponibilité $b(gr_i)$ (voir équation *17*, Section 6.2.1.2) :

$$I(\&gr_i) = \&gr_j \mid \&gr_j \neq \&gr_i \quad \text{avec} \quad \&gr_j = pr_k \text{ et } pr_k \nrightarrow gr_i \text{ et } pr_k \rightarrow gr_j \quad (20)$$

Pour un sujet donné, une fois que la référence au granule classifié gr_i est changée pour pointer vers du bruit, ce granule n'est plus accessible. L'action d'injection de bruit est une réaction à une tentative d'accès illégitime par un sujet/usager suspect malveillant. Pour réaliser cette action on dispose au niveau du serveur d'un ensemble homogène de granules de bruit qui sont sélectionnés de façon rationnelle (Section 5.3.6 du Chapitre 5), qui sont comparables dans leur structure syntactique aux granules de l'information confidentielle (mot par mot, phrase par phrase, paragraphe par paragraphe, …) et qui renferment un sens qui rend difficile leur distinction par rapport à l'information confidentielle.

Soit N un ensemble de granules de bruit similaire à Gr_X :

$N=\{gr_j \mid j=1 \ldots q\}$ avec $q \geq m$ ($|N| \geq |Gr_X|$)
et $\forall\, i, j \in \{1, \ldots, q\}$, $\forall\ gr_i \in Gr_X, \exists\, gr_j \in N \mid gr_i \cong gr_j$ (gr_i similaire à gr_j)

Injection de bruit pour $gr_i \Rightarrow \&gr_i = pr_j \mid pr_j \nrightarrow gr_i \wedge pr_j \rightarrow gr_j$ avec $gr_j \in N$

$\Rightarrow gr_i$ non accessible

Ainsi, a l'issue de cette action d'injection de bruit, $\&gr_i$ ne pointe plus vers le granule confidentiel $\&gr_i$ mais vers un deuxième granule $\&gr_j$ qui est un granule de bruit et cela via le nouveau pointeur pr_j.

GBFC identifie chaque sujet par un identifiant unique qui est utilisé pour décider du droit d'accès et des autorisations dont dispose le sujet vis-à-vis des granules d'informations classifiés auxquels il sollicite l'accès. Au moment d'une demande d'accès, l'EGA reçoit du client son identifiant (*ID*) et la référence au granule auquel il demande l'accès ($\&gr_i$) -entre autres-. Ce couple $ID\text{-}\&gr_i$ est analysé pour déterminer :

1- L'identité du sujet et l'identité du granule
2- Les attributs du sujet/rôle (localisation …) et ses autorisations ou permissions
3- La classification du granule et les critères de sécurité à lui appliquer
4- L'identification d'un granule de bruit correspondant -si besoin-
5- Le résultat de la demande d'accès

Dans le cas où le sujet est identifié comme posant un risque potentiel à la confidentialité de l'information, le résultat de la demande d'accès est négatif et l'EGA redirige cette demande pour pointer vers un granule de bruit. En effet, comme montré dans la Figure 29, c'est la combinaison $ID\text{-}\&gr_i$ qui est utilisée pour déterminer si la référence dont dispose le sujet pointe effectivement vers le granule d'information gr_i ou vers un granule de bruit ce que nous représentons par la notation (ID_S - $\&gr_y$) où ID_S représente l'identité du sujet et $\&gr_y$ la référence au granule d'information auquel il requiert accès.

Dans la Figure 29, on décrit ce processus en ayant les trois premiers sujets qui sont authentifiés et autorisés à accéder aux granules confidentiels et les deux derniers qui ne le sont pas. L'EGA accorde accès aux sujets autorisés sur la base de leurs identité (*ID*) et sur la base de la références au granules (*&gr*). Quant aux sujets 4 et 5 (non authentifiés et/ou non autorisés), l'EGA annule et met à jour les références aux granules d'information dont ils disposent pour pointer vers du vide ou vers un granule de bruit :

Pour le sujet 1 : $\text{Auth}(S_1 ; gr_1)_{(ID1\text{-}\&gr1)} \Longrightarrow \&gr_1 = pr_1 \wedge pr_1 \rightarrow gr_1$

Pour le sujet 2 : $\text{Auth}(S_2 ; gr_1)_{(ID2\text{-}\&gr1)} \Longrightarrow \&gr_1 = pr_1 \wedge pr_1 \rightarrow gr_1$

Pour le sujet 3 : $\text{Auth}(S_3 ; gr_i)_{(ID3\text{-}\&gri)} \Longrightarrow \&gr_i = pr_i \wedge pr_i \rightarrow gr_i$

Pour le sujet 4 : $\text{NotAuth}(S_4 ; gr_1)_{(ID4\text{-}\&gr1)} \Longrightarrow \&gr_1 = pr_j \wedge pr_j \nrightarrow gr_1 \wedge pr_j \rightarrow gr_j$

Pour le sujet 5 : $\text{NotAuth}(S_5 ; gr_i)_{(ID5\text{-}\&gri)} \Longrightarrow \&gr_i = pr \wedge pr \nrightarrow gr_i \wedge pr \rightarrow \text{Null}$

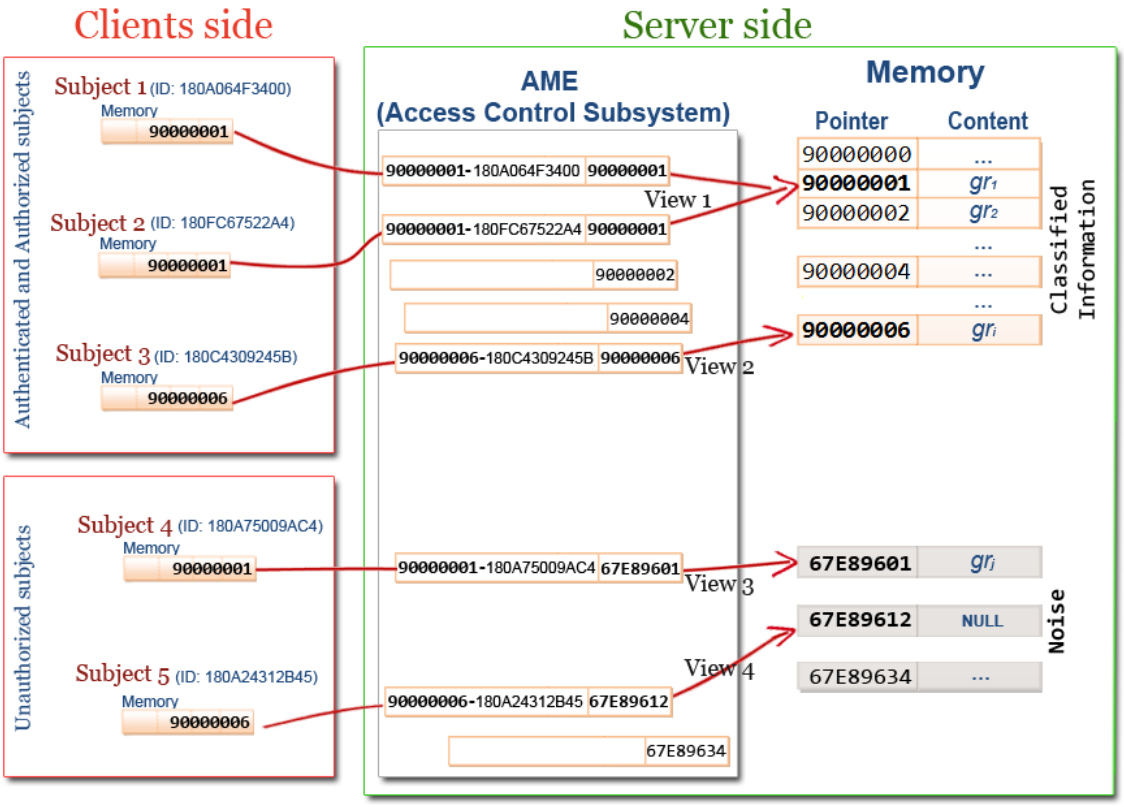


Figure 29. Contrôle d'accès basé sur les références par l'EGA

La figure 29 montre la même situation qu'à la figure 27 de la Section 6.2.1.2 quant à l'action de l'Engin de Gestion d' Accès du GBFC relativement à l'octroi ou au rejet d'accès aux granules confidentiels respectivement aux sujets autorisés et aux sujets non autorisés.

En synthèse de cette Section (6.2.1) du chapitre, nous avons présenté le modèle logique du GBFC à travers la définition des 4 fonctions fondamentales de ce modèle, à savoir :

- La fonction de granulation *f* qui prend comme argument un élément d'information x_i et lui fait correspondre un granule gr_i (Section 6.2.1.1).
- La fonction de disponibilité *b* qui prend en argument un granule d'information gr_i et retourne sa référence $\&gr_i$ (Section 6.2.1.2).
- La fonction de rafraîchissement *h* qui prend en argument la référence à un granule d'information $\&gr_i$ et retourne un nouveau pointeur à ce granule (Section 6.2.1.3).

- La fonction d'injection de bruit *l* qui prend en argument la référence à un granule d'information $\&gr_i$ et retourne un pointeur à un granule de bruit gr_j (Section 6.2.1.4).

Toutes ces fonctions sont implémentées et gérées par l'EGA au niveau du serveur.

6.2.2 Contrôle d'accès basé sur les références (RefBAC)

Dans la section 1 de ce chapitre, nous avons proposé une description formelle des diverses opérations d'accès aux objets et des concepts d'autorisation des sujets, de disponibilité et d'accessibilité de l'information dans le contexte des modèles de sécurité conventionnels. Vu que notre modèle introduit la composante information dans son approche (Section 5.1.3 du Chapitre 5), nous proposons ci-dessous un ensemble de définitions qui décrivent et formalisent les divers concepts de sécurité et les principales opérations d'accès aux informations selon GBFC. Ces définitions seront utilisées de façon explicite ou implicite dans la Section 6.4 pour vérifier et prouver la capacité de notre modèle à garantir le contrôle de flux d'informations.

Soit X une information confidentielle de niveau de classification L_X. Le niveau de classification est un ensemble de critères et de conditions pris en considération dans les autorisations d'accès (classes, règles, rôles, attributs, etc.).

Pour qu'un sujet S accède à X:

1- S doit avoir le niveau d'autorisation nécessaire : $L_S \geq L_X$.

2- X doit être disponible pour S à travers les références à ses granules (gr_i).

Dans notre modèle, $X=\{x_1, x_2, x_3, \dots, x_n\}$ et l'accès à x_i implique l'accès au granule gr_i de x_i (gr_i étant membre de Gr_X) se basant sur $T\alpha$.

En conséquence, S a le droit d'accès à $X=\{x_1, x_2, \dots, x_n\}$ sous sa forme granulaire $Gr_X=\{gr_1, gr_2, \dots, gr_m\}$ sachant que $\forall\, x \in X,\ \exists!\, gr_i \in Gr_X \mid x \in gr_i$:

$$\text{Auth}(S; gr_i) \stackrel{\text{def}}{=} \text{si } \&gr_i \in O \text{ alors CR}(S; O) \text{ avec } \&gr_i = pr \wedge pr \rightarrow gr_i \quad (21)$$

Ceci prenant en considération que dans notre modèle, le granule confidentiel gr_i (logé dans le serveur) ne peut être accédé qu'à travers sa référence $\&gr_i$ (chargée sur la station client).

Cette approche présente une méthodologie novatrice basée sur ***2 niveaux de contrôle de sécurité : central et local***.

1- Le contrôle de sécurité *local* est appliqué sur l'objet *O* qui renferme la référence au granule d'information confidentielle accessible par le sujet *S* ($\&gr_i \in O$ et CR(S; O)).
2- De l'autre côté, le contrôle au niveau *central* est appliqué à travers la gestion et le contrôle des références aux granules par l'administrateur de sécurité de manière centralisée ($\&gr_i = pr \wedge pr \rightarrow gr_i$).

La relation de non-autorisation se définit comme suit:

$$\text{NotAuth}(S; gr_i) \stackrel{\text{def}}{=} \&gr_i \in O \wedge \neg\text{CR}(S; O) \text{ ou } \&gr_i \neq pr \vee pr \nrightarrow gr_i \quad (22)$$

Ainsi, la prévention d'accès à un granule d'information confidentiel peut être opérée au niveau client par la prévention de lecture par le sujet non-autorisé de l'objet contenant la référence du granule : $\neg\text{CR}(S'; O)$. De même, cet accès peut être empêché au niveau central par la mise à jour de la référence au granule pour qu'elle ne pointe plus vers celui-ci : $pr \nrightarrow gr_i$.

A noter que le contrôle d'accès local est possible seulement quand l'EGA peut contrôler les opérations d'accès sur le système client, ce qui peut ne pas être les cas dans des situations d'accès illégitime.

6.2.2.1 Opérations de lecture

L'accès aux informations classifiées à travers les références aux granules correspondants nous permet de définir l'opération de lecture dans le modèle GBFC comme suit :

$$\mathcal{R}(S; \&gr_i, O) \stackrel{\text{def}}{=} \&gr_i \in O \wedge \mathrm{R}(S;O) \quad (23)$$

Ainsi, dans notre modèle, la lecture de l'information confidentielle *X* correspond à la lecture de tous les objets qui renferment les références ($\&gr_i$) aux granules gr_i de ses composants *x*.

6.2.2.2 Opérations d'écriture

Similaire à l'opération de lecture des granules classifiés qui se fait à travers les références à ces granules, l'écriture de son côté se fait via ces références. Ainsi, dans notre modèle, l'équivalent d'une opération d'écriture d'une information *X* par un sujet *S* dans un objet *O'* est l'écriture des références aux granules de ses éléments *x*, et se définit ainsi :

$$\mathcal{W}(S; \&gr_i, O') \stackrel{\text{def}}{=} \exists O \,|\&gr_i \in O \wedge \mathrm{W}(S; O, O') \text{ avec } \&gr_i = pr \wedge pr \rightarrow gr_i \quad (24)$$

En d'autres termes, il s'agit de l'écriture dans l'objet *O'* de la référence $\&gr_i$ qui pointe vers le granule d'information confidentiel gr_i.

6.2.3 Action de rafraîchissement et contrôle de flux

Basé sur les deux scénarios d'état sécurisé et d'état non sécurisé, l'action de rafraîchissement est utilisée pour assurer la sécurité et prévenir les fuites d'informations. C'est l'engin de gestion d'accès (EGA) qui assure cette action par une actualisation des références aux granules d'information sur la base des critères spécifiés énoncés dans le taux de rafraîchissement $T\rho$.

6.2.3.1 Cas d'accès légitime

Pour les sujets autorisés, l'action de rafraîchissement est réalisée à travers la mise à jour des références chargées ou enregistrées dans les objets de la machine client. Cette mise à jour affecte à ces références de nouvelles et différentes valeurs qui pointent vers les granules demandés. Cette action de rafraîchissement des références sur les postes clients est subséquente à un changement de la valeur du pointeur vers le granule au niveau du serveur et s'opère de façon dynamique au moment de l'accès à l'information classifiée par le sujet (Tableau 10).

6.2.3.2 Cas d'accès illégitime

En cas d'accès illégitime par un sujet non autorisé, l'EGA procède par une mise à jour de la référence au granule classifié pour pointer vers un nul ou vers un granule de bruit dépendamment du niveau du risque et dépendamment des critères définis dans *Tv*. Notons que, quel que soit la valeur de la nouvelle référence, le fait que le sujet ne soit pas autorisé engendre que cette référence ne pointe plus vers le granule classifié au niveau du serveur (décision basée sur l'évaluation du couple *ID-&gr*$_i$ citée dans la Section 6.2.1.4).

Que ce soit dans le cas d'un accès légitime ou illégitime, une fois qu'une action de rafraîchissement a lieu, les anciennes références vers les granules d'informations classifiés ne pointent plus vers ces granules en l'absence d'une actualisation par l'EGA (Tableau 10). Ceci offre un niveau supérieur de contrôle qui peut être appliqué à des informations sensibles pour lesquelles une action de rafraîchissement peut, par exemple, empêcher de re-visionner des parties de l'information une fois vues par un sujet (lecture unique). Cette action de rafraîchissement peut aussi être cruciale dans les cas de licenciements, d'attaques malveillantes, de fusions ou d'acquisitions d'entreprises où l'on voudrait qu'une information soit inaccessible à tous les niveaux d'une organisation, etc.

Accès autorisé	Accès non autorisé
At state t_n: $\&gr_i = pr_0$ and $pr_0 \rightarrow gr_i$	At state t_{n+2} (with a refresh action performed): - $\&gr_i = pr_2$ and $pr_2 \nrightarrow gr_i$ - $pr_2 \neq pr_0$ and $pr_0 \nrightarrow gr_i$
At state t_{n+1} (with a refresh action performed) : - $\&gr_i = pr_1$ and $pr_1 \rightarrow gr_i$ - $pr_1 \neq pr_0$ and $pr_0 \nrightarrow gr_i$	With the option that : $pr_2 \rightarrow gr_j$ (gr_j being a noise granule) based on the parameter Tv.

Table 10. Accès à l'information après une action de rafraîchissement

Dans cette table on montre les résultats d'une action de rafraîchissement dans les cas:

1- d'un accès légitime (autorisé) : passage de l'état t_n à t_{n+1} (colonne de gauche)
2- d'un accès illégitime (non autorisé) : passage de l'état t_n à t_{n+2} (colonne de droite)

Il est à préciser que le mécanisme de rafraîchissement est un composant essentiel du GBFC qui permet, en plus du contrôle d'accès total à l'information, d'assurer les fonctions d'ajouts ou de modification de granules confidentiels aux documents. En effet, au besoin, l'administrateur de sécurité peut procéder par une action de rafraîchissement pour isoler complètement une information confidentielle du réseau (information indisponible). Ceci correspondrait à une réaction immédiate à l'éventualité ou à la tentative d'un accès illégitime dans le domaine militaire par exemple. L'action de rafraîchissement peut aussi être basée sur l'occurrence d'événements, tel qu'un accès par utilisateur. Un exemple pratique serait le cas de document dont le contenu est protégé par droit d'auteur où l'on voudrait qu'une fois un utilisateur ait accédé à une page, celle-ci ne soit plus accessible (lecture unique) ou encore une réaction à la copie de l'information confidentielle par un deuxième sujet et ainsi de suite.

Le rafraîchissement est aussi relié aux opérations d'ajout, de modification ou de suppression de contenu confidentiel au sein d'un document. Par exemple, une fois qu'un sujet de classification *TS* aura inséré un paragraphe dans un document, ce paragraphe peut

être automatiquement classifié *TS* par l'EGA. Cela engendrerait la création de nouveaux pointeurs et de nouvelles références vers ce paragraphe et par conséquent l'exécution d'une action de rafraîchissement afin de rendre le nouveau paragraphe disponible aux autres sujets ayant droit d'accès. Ceci dépendrait des critères de sécurité appliqués au document en question et de la configuration du système relativement à ce genre d'opérations. Cette famille d'opérations, qui relèvent de l'aspect gestion d'intégrité de l'information par le GBFC, ne sont pas traitées dans le cadre de cette thèse et nous y consacrerons un développement à part entière dans le futur de cette recherche.

6.3 GBFC et Modèles de contrôle d'accès

Dans le Chapitre 1 de cette recherche, on a défini le droit d'accès comme étant l'autorisation de réaliser une opération *Op* (lecture ou R, écriture ou W) par un sujet *S* sur un objet *O*. Ceci est représenté sous forme de règle d'accès : $Ar< S, O, Op >$ dont les composants sont *S, O* et *Op*. On adoptera cette notation pour représenter les composants d'une règle d'accès pour un modèle de sécurité donné avec certaines adaptations par rapport aux notations préconisées par plusieurs articles dont [34, 63, 106, 121, 17, 16].

Ce triplet (Sujet, Objet et Opération) est présent dans la majorité des modèles de contrôle d'accès en addition à d'autres composants spécifiques à chaque modèle. Les composants des règles d'accès de chaque famille de modèles traités ci-après sont adressés avec plus de détails dans la sous-section correspondante dans le Chapitre 4 (Section 4.3) et sont généralement listés dans les articles et travaux de recherches qui y sont référencés. On propose ci-dessous une représentation formelle, générale et simplifiée des règles d'accès (*Ar*) pour chacune de ces principales familles de modèles de contrôle d'accès afin de pouvoir les comparer avec notre modèle :

Multilevel security (MLS exemple : MAC)

Ar_{MLS}<*S, O, L, Op*>

où :
S : Sujet
O : Objet
L : Classification qui peut prendre les formes :
L_S : Autorisation du sujet *S*
L_O: Classification de l'objet *O*
Op(S ; O) : Opération (R ou W) du sujet *S* sur l'objet *O*

Rule Based Access Control (RuBAC)

Ar_{RuBAC}<*S, O, Ru, Op*>

où :
S : Sujet
O : Objet
Ru : Ensemble de règles reliées au droit d'accès et qui peuvent prendre les formes :
Ru_S : Règle appliqués au sujet *S*
Ru_O : Règle appliqués à l'objet *O*
Op(S ; O) : Opération (R ou W) du sujet *S* sur l'objet *O*

Role Based Access Control (RBAC)

Ar_{RBAC}<*S, O, R, Op*>

où :
S : Sujet
O : Objet
R : Rôle assigné au sujet *S*
Op(R; O) : Permission (privilège) assignés au rôle *R* sur l'objet *O* (soit : R ou W)

Pour raisons de simplification, nous supposons ici un système RBAC dans un état spécifique dans lequel les relations entre sujets et rôles, ainsi que rôles et permissions sont fixes. On ignorera donc le concept de sessions dans RBAC. De plus, on se limitera aux deux permissions de base pour notre recherche : lecture et écriture (R et W).

Attribute Based Access Control (ABAC)

Ar_{ABAC}<*S, O, A, C, Ru, Op*>

où :
S : Sujet
O : Objet
A : Ensemble d'attributs pris en compte dans l'évaluation du droit d'accès et qui peuvent prendre les formes :
A_S : Attribut du sujet *S*
A_O : Attribut de l'objet *O*
A_E : Attribut de l'environnement
C : Ensemble de conditions d'environnement ayant un impact sur le droit d'accès
$Ru_{(A,C)}$: Ensemble de règles et de relations ayant un impact sur le droit d'accès
Op(S ; O) : Opération (privilège) du sujet *S* sur l'objet *O* (soit : R ou W)

Granularity Based Flow Control (GBFC)

Ar_{GBFC}<*S, O, gr, Op*>

où :
S : Sujet
O: Objet
gr : Granule d'information
Op(S ; O) : Opération (R ou W) du sujet *S* sur l'objet *O*

Le Tableau 11 résume et compare les composantes des divers modèles de contrôle d'accès avec les composants du modèle de contrôle de flux basé sur la granularité. Dans ce tableau, x désigne les composantes de base et ~ les composants optionnels. On distingue la présence des composants de base (*S, O, Op*) dans la majorité des modèles en plus des autres composants. RuBAC et RBAC utilisent une appellation spécifique pour les opérations : il s'agit de "permissions" dans ces deux modèles. Une autre spécificité du nommage dans RBAC est la considération des règles d'accès comme étant des "contraintes". On constate aussi un développement formel et chronologique et de la caractéristique d'agrégation ascendante partant des modèles MLS vers le modèle GBFC avec la possibilité d'intégration des composantes des modèles antérieurs.

	S	***O***	***Op***	***gr***	***L***	***Ru***	***R***	***A***
MLS ***(MAC)***	x	x	x		x			
RuBAC	~	x	x *(permissions)*		~	x		
RBAC	x	x	x *(permissions)*		~	~ *(contraintes)*	x	
ABAC	~	x	x		~	~	~	x
GBFC	x	x	x	x	~	~	~	~

Table 11. Composantes des divers modèles de contrôle d'accès et du GBFC

Ce tableau montre que le modèle GBFC est un modèle qui inclut les principales composantes des modèles classiques. Les composants optionnels (marqués par ~) sont pris en charge par notre modèle lors de l'intégration avec les autres modèles de contrôle d'accès. Les mécanismes détaillés de cette prise en charge ne sont pas adressés dans le cadre de ce projet de recherche et seront sujets de développements futurs.

6.3.1 Intégration du GBFC aux modèles existants

Dans la Section 6.2 nous avons mené une analyse logique détaillée et proposé le modèle logique de contrôle de flux basé sur la granularité et qui pourra s'intégrer et s'adapter aisément avec les modèles de contrôle d'accès existants. La possibilité d'intégration avec les divers modèles en application dans le domaine de la sécurité des informations détermine son niveau de faisabilité et ses potentialités d'implémentation en technologie et en entreprise.

On prendra ici un exemple simplifié du modèle GBFC appliqué à la famille des modèles de sécurité multi-niveaux. L'application du GBFC aux modèles MLS résultera d'une règle d'accès qui comprend les éléments suivants :

S : Sujet
O : Objet
gr: Granule d'information
L : Classification qui peut prendre les formes :

L_S : Autorisation du sujet *S*
L_O: Classification de l'objet *O*
Op(S ; O) : Opération (R ou W) du sujet *S* sur l'objet *O*

La règle d'accès pour cette combinaison des deux modèles met en action des sujets qui exécutent des opérations d'accès sur des granules d'information logés dans des objets. La possibilité de réalisation de ces opérations dépend des classifications appliquées aux objets et des autorisations d'accès dont disposent les sujets. Cette règle sera alors notée de la manière suivante: $\boldsymbol{Ar_{GBFC\text{-}MLS}<S, O, L, gr, Op>}$

6.3.1.1 Généralisation d'intégration aux modèles conventionnels

Nous avons montré que le modèle GBFC est basé sur l'accès aux granules d'information confidentiels à travers des références volatiles écrites dans des objets accessibles par les différents sujets. Cette notion d'objet existe dans tous les modèles de contrôle d'accès (MAC, RuBAC, RBAC, ABAC, …). Ces modèles appliquent des classifications, des permissions ou des privilèges pour l'accès à ces objets. Dans notre modèle on se base sur le même concept en accédant aux granules d'information confidentiels à travers des références écrites dans les objets accessibles par des sujets. Cette similarité d'accès aux informations à travers l'accès aux objets rend notre modèle compatible avec les modèles classiques du fait que la seule différence de fond est qu'au lieu d'utiliser l'objet pour loger l'information ($X \in O$ dans les modèles classiques) on y loge des références aux granules classifiés dans notre modèle ($gr_i \in O$). Ceci permet, par conséquent, à notre modèle de se greffer au dessus des modèles de contrôle d'accès conventionnels et de tout autre modèle de sécurité qui utilise les objets. Cette superposition du GBFC avec ces modèles est décrite avec plus de détails dans la section 5.3.5 du chapitre 5 (Figure 24).

Cette superposition permet à notre modèle une intégration aisée à ces différents modèles tout en renforçant le contrôle de flux qui constitue une lacune pour la plupart.

Au delà de cette simple logique, il faudra souligner que les mécanismes et les détails d'intégration du GBFC avec les autres modèles en application n'est pas parmi les objectifs de cette étude, mais un domaine d'études supplémentaire et une perspective de recherche assez large pour l'avenir.

Notons que, par exemple, la notion de rôles dans RBAC est analogue à la notion de vues dans GBFC (cf. Chapitre 5, Section 5.3.2) et le concept de sessions est aussi présent dans celui-ci à travers l'action de rafraîchissement. Toutes ces constatations et ces similarités offrent des chances à notre modèle pour une considération future en tant que modèle général indépendant qui offre un contrôle d'accès basé sur les références et un control de flux basé sur la granularité et sur le contrôle de disponibilité de l'information.

6.4 Contrôle de flux : Prévention de fuites d'informations

6.4.1 Scénarios de contrôle de flux

Soit une information confidentielle *X*, un sujet authentifié et autorisé *S* et un sujet non autorisé *S'*. Pour empêcher *S* d'initier un flux de l'information *X* vers *S'* c'est-à-dire prévenir tout flux illégitime de l'information *X* du sujet *S* vers le sujet *S'*, on devra étudier en détail les divers scénarios d'accès à l'information (en lecture et écriture) par *S*. Ainsi, quelque soient les sujets *S* et quelque soient les objets *O* contenant *X*, les scénarios possibles sont dressés dans le tableau suivant :

¬CR			
¬CR ∧ CR	**CR**		
¬CR ∧ ¬CW	**CR ∧ ¬CW**	**¬CW**	
¬CR ∧ CW	**CR ∧ CW**	**¬CW ∧ CW**	**CW**

Table 12. Scénarios possibles d'accès à l'information par un sujet

En analysant ces scénarios, on constate que certains sont impossibles (¬CR ∧ CR et ¬CW ∧ CW), d'autres ne sont pas normalement envisageables dans le contexte de flux et de fuites d'informations (¬CR ∧ CW). Les autres scénarios peuvent être regroupés sous forme de combinaison équivalentes ou d'implications de scénarios dressées dans le Tableau 13 ci-après. On en dérive par la suite, les 5 situations possibles dont le détail et le formalisme sont dressés dans le Tableau 14.

Combinaisons équivalentes	**Implication**	**Action ***
¬CR , ¬CR ∧ ¬CW , ¬CR ∧ CW	¬CR	**1**
CR	**CR ∧ ¬CW** ou **CR ∧ CW**	**2 et 3**
¬CW	¬CR ∧ ¬CW ou CR ∧ ¬CW	**2**
CW	CR ∧ CW	**3**
¬CR ∧ CR , ¬CW ∧ CW	**Combinaisons impossibles**	**-**

* Actions listées ci-dessous

Table 13.Combinaisons des scénarios d'accès

Ainsi, et sur la base de cette étude combinatoire et analytique de ces scénarios, on estime que pour parvenir à empêcher la fuite d'informations (flux illégitime comme défini dans la Section 3.4.1 du Chapitre 3) de *S* vers *S'* seules les actions suivantes sont envisageables :

1- On empêche *S* de lire l'objet qui contient *X* (ce qui implique qu'il ne peut pas écrire *X*, donc pas de flux)

2- On permet à *S* de lire mais pas d'écrire *X* (Cas de lecture seule, pas de flux)

3- On permet à *S* de lire et d'écrire *X* :

a. On permet à *S* de lire et d'écrire *X* dans le même objet *O* (modification, pas de flux)

b. On permet à *S* de lire et d'écrire *X* dans tout objet *O'* (copie : flux) :

i. On empêche *S* d'écrire *X* sur tout objet que *S'* peut lire

ii. On empêche le sujet non autorisé *S'* de lire *X* à partir de tout objet qui la contient

Note : on exclut le scénario **¬CR ∧ CW** de toute considération pour deux raisons :

- Il s'agit d'un cas particulier de CW
- Il s'agit du cas d'écriture sous forme d'*ajout* (*Ang. append*) ou de modification d'informations dans un objet sans lecture de l'information confidentielle qu'il contient. Il est à rappeler ici, qu'un flux d'information X ne peut se réaliser que par une succession d'opération de lecture de X suivie d'une opération d'écriture de celle-ci. C'est donc un cas où une fuite d'information ne peut exister du fait que l'information confidentielle ne peut être lue par le sujet. En d'autres termes, une information qui ne peut pas être lue ne peut pas être écrite. Ce scénario rejoint donc le scénario de ¬CR.

Il est à noter que dans le scénario 3-b.ii on ne tente pas d'empêcher le sujet autorisé d'initier le flux illégitime, mais on va au delà en proposant une solution curative (après un flux illégitime) qui consiste en la prévention de lecture de l'information objet du flux par les sujets non autorisées.

Comme synthèse, on estime que les modèles de sécurité classiques tentent d'empêcher un sujet S ayant accès à une information $X \in O$ de la transférer à un autre sujet non autorisé S' en adoptant l'une des solutions listées dans le tableau suivant :

1-	Empêcher S de lire X, en lui interdisant de lire O $\forall S, O,$ if $X \in O$ then $\neg\text{CR}(S; O)$ *(25)*
2-	Permettre à S de lire mais pas d'écrire X $\forall S, O,$ if $X \in O$ and $\text{CR}(S; O)$ then $\forall O', \neg\text{CW}(S; O')$ *(26)*
3.a-	Permettre à S de lire et d'écrire X, mais pas de le copier sur un autre objet O' $\forall S, O,$ if $X \in O$ and $\text{CR}(S; O)$ then $\forall O' \neq O, \neg\text{CW}(S; O, O')$ *(27)*
3.b.i-	Empêcher S d'écrire X sur tout objet que S' peut lire $\forall S, O, S', O',$ if $X \in O$ and $\text{CR}(S'; O')$ then $\neg\text{CW}(S; O, O')$ *(28)*
3.b.ii-	Empêcher S' de lire X à partir de tout objet qui la contient $\forall S', O',$ if $X \in O'$ then $\neg\text{CR}(S'; X, O')$ *(29)*

Table 14. Scénarios de contrôle de flux par les modèles de contrôle d'accès

Ces cinq actions sont classées de la plus restrictive, et la plus facile à implémenter (Scénario 1) vers la moins restrictive étant par la même occasion la moins réalisable (Scénario 3.b.ii). Aussi, nous soulignons ici que les trois premiers scénarios sont trop restrictifs et ne permettent pas l'existence d'un flux d'information. On mènera dans la section suivante une analyse approfondie de ces cinq scénarios afin d'en ressortir les principales remarques vis-à-vis de la possibilité d'atteindre l'objectif d'origine qui est la prévention de fuites d'informations.

6.4.2 Analyse des scénarios de contrôle de flux

Par rapport aux modèles conventionnels de contrôle d'accès, le modèle GBFC gère différemment le contrôle du flux d'informations et offre une implémentation de la sécurité à un niveau plus bas : granules d'information gr_i. Ces granules ne sont accessibles par les sujets qu'à travers leurs références $\&gr_i$. Ceci constitue un avantage majeur par rapport aux modèles de contrôle d'accès actuels qui implémentent la sécurité de l'information au niveau objet. Ainsi, dans notre modèle, la composante information devient l'élément clé dans le contrôle de flux. L'information confidentielle X sera remplacée dans notre modèle par le granule d'information confidentiel gr_i dans les différents scénarios.

Avec cette différence de fond, on analyse la capacité du modèle de contrôle de flux basé sur la granularité à prévenir les fuites d'informations et garantir un contrôle de flux plus adapté aux diverses situations et scénarios d'accès dans une organisation (Table 14).

Il est à souligner que les divers scénarios sont représentés dans une logique dynamique de transition d'états dans laquelle des opérations initiées par les sujets ou par l'administrateur de sécurité du système déclenchent les transitions d'un état à un autre pour arriver à un état final du système dans lequel le scénario est validé.

La preuve de notre hypothèse de travail du Chapitre 1, Section 1.4 est dressée dans notre analyse du scénario 3.b.i (Section 6.4.2.4) et d'une façon plus générale dans l'analyse du scénario 3.b.ii (Section 6.4.2.5).

6.4.2.1 Scénario 1 : Interdiction de lecture.

Empêcher *S* de lire $\&gr_i$, en lui interdisant de lire *O* :

$\forall S, O,$ if $\&gr_i \in O$ then $\neg \mathrm{CR}(S; O)$ *(25)*

Il s'agit du scénario où on prévient un flux illégitime d'une information par l'interdiction à tout sujet de la lire. C'est un cas extrême de restriction de flux par interdiction d'accès à l'information. Ce cas est simple à mettre en œuvre dans les systèmes de sécurité centralisés et constitue la solution idéale en cas de fuite d'information, étant évident que l'on voudrait empêcher un sujet malveillant de lire l'information. Cependant, il est inadapté aux besoins des organisations dont le fonctionnement repose sur l'accès à l'information et qui donnent priorité à sa disponibilité. Un exemple pratique de ce scénario est le cas où l'administrateur s'aperçoit d'une attaque malveillante et décide d'empêcher l'accès aux informations confidentielles jusqu'à résolution du problème.

Les modèles classiques emploient généralement des techniques additionnelles (cryptage, etc.) pour implémenter ce scénario comme action curative suite à un flux illégitime. Pourtant, une fois que l'information confidentielle est présente sur un support mobile, l'administrateur de sécurité perd pratiquement tout contrôle d'accès et d'usage sur celle-ci.

GBFC implémente ce scénario avec succès grâce à son aspect centralisé qui garde les informations confidentielles au niveau du serveur et y octroie accès à travers des références volatiles contrôlées par l'EGA. En effet, à l'accès, l'information n'est jamais chargée en tant que telle sur un poste client ou un support de stockage. Au besoin, l'administrateur de sécurité peut totalement isoler l'information du réseau en exécutant une action de rafraîchissement de ses références (cf. Section 6.2.1.3 et 6.2.3) pour que tous les usagers, ou sujets, légitimes ou non, perdent accès à travers les anciennes références dont ils disposent.

Soit un granule d'information confidentiel gr_i tel qu'à l'état t_n, $\&gr_i = pr_k$ et $pr_k \rightarrow gr_i$. A la suite d'une attaque malveillante par exemple, l'administrateur de sécurité décide d'intervenir avec une action de mise à jour du pointeur vers gr_i au niveau du serveur à l'état ultérieure t_{n+1} tel que : $pr_k \nrightarrow gr_i$ comme montré dans le tableau suivant :

At state	On the client side	On the server side
t_n	$\&gr_i \in O \wedge \&gr_i = pr_k$	$pr_k \rightarrow gr_i$
t_{n+1}	$\&gr_i \in O \wedge \&gr_i = pr_k$ No change	$pr_k \nrightarrow gr_i$ *(By the action of the security administrator)*
Final state	$\&gr_i \in O \wedge \&gr_i = pr_k \wedge pr_k \nrightarrow gr_i$	

Nous voyons ici qu'à l'état final, bien que le client dispose de la référence au granule confidentiel, cette référence ne pointe plus vers le granule en question, ce qui rend ce granule indisponible.

6.4.2.2 Scénario 2 : Interdiction d'écriture.

Permettre à *S* de lire mais pas d'écrire $\&gr_i$:

$\forall S, O,$ if $\&gr_i \in O$ and $\mathrm{CR}(S; O)$ then $\forall O', \neg\mathrm{CW}(S; O')$ *(26)*

Il s'agit généralement des cas d'accès en lecture seule à des contenus non supposés être modifiés, reproduits ou sauvegardés par les sujets qui y accèdent. L'accès à des informations sous droit d'auteurs et aux informations de vie privée en sont deux exemples courants. En pratique, on retrouve ce scénario dans certains accès aux documents en format PDF (Portable Document Format) ou dans les méthodes d'accès aux contenus protégés par droits d'auteurs sur le web (Google books et services similaires).

Ce scénario est idéal pour permettre l'accès tout en empêchant le flux d'informations. Ce scénario est comparable au scénario 1 dans son aspect restrictif et dans son inadaptation aux conditions et aux environnements de travail contemporains. En effet, le besoin d'accès

aux informations à partir de multiples sources et la nécessité de manipulation, de mise à jour et de sauvegarde des données rendent la mise en œuvre de ce scénario limitée à des cas particuliers d'accès.

Notre modèle arrive à implémenter ce scénario du fait qu'après un accès en lecture, toute action d'écriture ou de modification se fait à travers des références gérées dynamiquement et qui peuvent être rafraichies à l'accès :

Soit un granule d'information confidentiel gr_i tel que à l'état t_n $\&gr_i \in O$ et $\&gr_i = pr_k$ et $pr_k \rightarrow gr_i$.

A l'état t_{n+1}, le sujet S initie une opération d'écriture W(S; O') au niveau de sa station client. En réponse à cette opération, l'EGA vérifie l'identité du sujet et la nature du granule d'information concerné par cette opération puis réagit à l'état t_{n+2} par une annulation du pointeur vers le granule en question au niveau du serveur ($pr_k \nrightarrow gr_i$) empêchant ainsi le sujet d'écrire une référence valide du granule sur l'objet O ($\&gr_i \in O \wedge \&gr_i = pr_k \wedge$ W(S; O) $\wedge$ $pr_k \nrightarrow gr_i$). Une mise à jour de la référence chez le client est envisageable à la suite de cette action, pour de nouveau permettre l'accès en lecture du granule d'origine.

At state	**On the client side**	**On the server side**
t_n	$\&gr_i \in O \wedge \&gr_i = pr_k$	$pr_k \rightarrow gr_i$
t_{n+1}	$\&gr_i \in O \wedge \&gr_i = pr_k \wedge$ **W(S; O')**	$pr_k \rightarrow gr_i$ No change
t_{n+2}	$\&gr_i \in O \wedge \&gr_i = pr_k \wedge$ W(S; O') No change	Assessment of the client request and authorizations by the AME : Auth(S ; gr_i)$_{(ID\text{-}\&gri)}$
t_{n+3}	$\&gr_i \in O \wedge \&gr_i = pr_k \wedge$ W(S; O') No change	$pr_k \nrightarrow gr_i$
Final state	$\&gr_i \in O \wedge \&gr_i = pr_k \wedge$ **W(S; O')** $\wedge$ $pr_k \nrightarrow gr_i$	

A l'issue de ce scénario on se retrouve dans un état où l'écriture de la référence du granule d'information classifié entraine l'annulation de cette référence (référence égale à la valeur d'un pointeur qui ne pointe pas vers le granule en question). Notons que ce scénario traite l'aspect intégrité de l'information qui n'est pas abordé en détail dans ce projet de recherche.

6.4.2.3 Scénario 3.a : Interdiction de réplication.

Permettre à *S* de lire et d'écrire $\&gr_i$, mais pas de le copier sur un autre objet *O'*

$\forall S, O,$ if $\&gr_i \in O$ and $\mathrm{CR}(S; O)$ then $\forall O' \neq O, \neg \mathrm{CW}(S; O, O')$ *(27)*

Ce scénario est généralement implémenté par les modèles de contrôle d'accès qui imposent des restrictions sur les opérations d'écriture par les sujets et contrôlent la nature d'accès aux objets via des procédés de classification (certains modèles de la famille MAC). De cette façon, ces modèles empêchent la reproduction (copie) de l'information classifiée dans des objets inappropriés. Les autres modèles (RBAC et ABAC) tentent d'intégrer ces restrictions à travers l'implémentation des directives du MAC.

Étant un modèle dédié au contrôle de flux, GBFC applique ce scénario par le contrôle des opérations d'écriture qui se font par le biais des références aux granules classifiés. Ainsi, la copie d'une information classifiée dans un objet par un sujet autorisé n'est rien d'autre que la copie des références aux granules de cette information. Tout accès postérieur au contenu du nouvel objet est un accès aux références qui y sont écrites et qui subissent des rafraîchissements par l'EGA.

Partant d'un état initial t_n où on a : $\&gr_i \in O \wedge \&gr_i = pr_k$ avec $pr_k \rightarrow gr_i$
A l'état $t_{n+}1$, l'initiation d'une opération d'écriture par un sujet autorisé *S* de la référence au granule d'information confidentiel $\&gr_i$ contenue dans l'objet *O* dans un second objet *O'* : W(*S*; *O*, *O'*) qui correspond dans notre modèle à $\boldsymbol{\mathcal{W}}(S; \&gr_i, O')$ engendre la vérification de l'identité du sujet et de la nature du granule d'information concerné par cette opération par

l'EGA. Cette vérification est suivie par une transition à un nouvel état t_{n+2} où le pointeur vers le granule en question est mis à jour pour ne plus pointer vers celui-ci ($pr_k \nrightarrow gr_i$) empêchant de cette façon le sujet de copier une référence valide du granule sur l'objet *O'* ($\&gr_i \in O \wedge \&gr_i = pr_k \wedge W(S; O, O') \wedge pr_k \nrightarrow gr_i$)

At state	**On the client side**	**On the server side**
t_n	$\&gr_i \in O \wedge \&gr_i = pr_k$	$pr_k \rightarrow gr_i$
t_{n+1}	$\&gr_i \in O \wedge \&gr_i = pr_k \wedge W(S; O, O')$	$pr_k \rightarrow gr_i$ No change
t_{n+2}	$\&gr_i \in O \wedge \&gr_i = pr_k \wedge W(S; O, O')$ No change	Assessment of the client request and authorizations by the AME : Auth(S ; gr_i)$_{(ID\text{-}\&gri)}$
t_{n+3}	$\&gr_i \in O \wedge \&gr_i = pr_k \wedge W(S; O, O')$ No change	$pr_k \nrightarrow gr_i$
Final state	$\&gr_i \in O \wedge \&gr_i = pr_k \wedge W(S; O, O') \wedge pr_k \nrightarrow gr_i$	

Résultat d'application de ce scénario :

Suite à un flux de l'information $\&gr_i$ initié par le sujet autorisé *S* de l'objet *O* vers l'objet *O'*, l'EGA empêche la copie de la référence au granule confidentiel dans *O'* par la mise à jour au niveau du serveur du pointeur vers le granule en question ($pr_k \nrightarrow gr_i$). *Cette* mise à jour rend la référence copiée dans *O'* sans valeur car elle est égale à la valeur d'un pointeur qui ne pointe pas vers gr_i.

6.4.2.4 Scénario 3.b.i : Confinement

Empêcher *S* d'écrire $\&gr_i$ sur tout objet que *S'* peut lire :

$\forall S, O, S', O',$ if $\&gr_i \in O$ and $CR(S'; O')$ then $\neg CW(S; O, O')$ *(28)*

A travers ce scénario on empêche un sujet autorisé d'écrire l'information confidentielle sur tout objet accessible par un sujet non autorisé. En d'autres termes, créer une situation de

confinement du sujet qui accède à l'information. C'est la motivation et l'objectif de ce projet de recherche et la problématique que nous adressons et à laquelle nous remédions à travers le modèle de contrôle de flux basé sur la granularité.

Tous les modèles de sécurité traités dans cette recherche présentent des vulnérabilités plus ou moins importantes vis-à-vis de ce problème. En effet, pour résoudre ce problème, on doit exercer un contrôle très restrictif sur les sujets accédant l'information et avoir une autorité absolue sur les objets susceptibles de contenir l'information confidentielle. Malheureusement, ce genre de contrôle restrictif est peu -si pas- envisageable par les entreprises ni même par les administrations et services civils et militaires qui ne peuvent plus fonctionner ou opérer correctement sans échange et sans partage d'informations (nouvelles réglementations et lois sur le partage d'informations, la cybersécurité, les gouvernements et les services électroniques, etc.). C'est bien pour cette raison que ce problème de confinement existe toujours après tant d'années et prend encore plus d'ampleur, statistiques à l'appui. Ce problème est aussi relié au problème de flux implicites encore connu sous le nom d'inférence qui de son côté subsiste malgré les efforts.

En adoptant notre approche pessimiste énoncée dans la section 6.1.1:

$$\forall S, O,\ \mathrm{CR}(S; O) \Rightarrow \exists O' \neq O \mid \mathrm{CW}(S; O, O') \qquad (5)$$

on peut avancer que tout ce qu'il faut pour avoir un flux illégitime c'est :

- Un sujet autorisé d'accéder à l'information;
- Un objet accessible par un sujet non autorisé et qui est susceptible de recevoir l'information.

Ces deux conditions sont généralement remplies dans les environnements de travail multi-applications et multiservices de nos jours où on opère continuellement en ligne.

Par ses composantes et son mode d'action, notre modèle propose une solution à ce problème de confinement :

- Soit un granule d'information classifié gr_i
- Soit un sujet S autorisé à accéder au granule gr_i : Auth$(S; gr_i)$
- Soit un sujet S' non autorisé à accéder au granule gr_i : NotAuth(S'; gr_i)
- Soit deux objets O et O' tels que : $O \neq O'$, CR(S; O), CW(S; O') et CR(S'; O')

État t_n : à cet état initial le sujet autorisé S dispose dans l'objet O de la référence $\&gr_i$ qui pointe vers le granule d'information confidentiel ($\&gr_i \in O$) : $\&gr_i = pr_k$ et $pr_k \rightarrow gr_i$

État t_{n+1} : Le sujet S initie une écriture de la référence au sein de l'objet O dans un second objet O' : W(S; O, O') qui donne lieu à la copie de cette référence dans ce deuxième objet : $\&gr_i \in O'$

État t_{n+2} : L'opération d'écriture de l'état précédent déclenche au niveau de l'EGA (serveur) un processus de vérification de l'identité et des autorisations du sujet ainsi que des critères de sécurité appliqués au granule confidentiel.

État t_{n+3} : Étant donné que S est un sujet autorisé à exécuter cette opération d'accès, l'EGA maintient la référence au granule confidentiel par le biais du pointeur pr_k ($pr_k \rightarrow gr_i$) permettant ainsi à S de copier cette référence (valide) dans O'.

État t_{n+4} : S' qui est une sujet non autorisé initie une lecture de gr_i à travers sa référence $\&gr_i \in O'$: R(S'; O')

État t_{n+5} : Comme dans l'état t_{n+2}, l'EGA analyse les autorisations de S' sur la base du couple (ID-$\&gr_i$).

Note : On a déjà mentionné dans la 6.2.1.4 que le modèle GBFC identifie un sujet comme posant un risque potentiel à la confidentialité de l'information sur la base de la combinaison (ID-$\&gr_i$) envoyés à l'EGA lors de la demande d'accès (Figure 29).

- L'EGA identifie S' comme sujet non autorisé à accéder gr_i

État t_{n+6} : Par conséquent, l'EGA met à jour $\&gr_i$ pour ce sujet : $\&gr_i = pr_k \wedge pr_k \nrightarrow gr_i \wedge pr_k \rightarrow$ Null.

De cette façon L'EGA annule la référence au granule classifié une fois que le sujet est identifié comme non autorisé pour ainsi rendre le granule indisponible pour le sujet. On aura donc : NotAuth(S'; gr_i)$_{(ID\text{-}\&gr_i)}$ $\wedge \mathcal{R}(S'; \&gr_i) \Longrightarrow \&gr_i = pr_k \wedge pr_k \nrightarrow gr_i \wedge pr_k \rightarrow$ Null.

1- *S'* perd toute référence vers le granule confidentiel gr_i
   - $pr_k \nrightarrow gr_i$
   - Possibilité que $pr_k \rightarrow gr_j$ (gr_j étant un granule de bruit)
2- *Résultat :* la référence correcte vers gr_i n'est pas disponible sur *O'* et par conséquent gr_i est indisponible pour *S'*

Conclusion : Pour un sujet *S'* | NotAuth(*S'* ; gr_i)

$\mathcal{W}(S; \&gr_i, O') \wedge R(S'; O') \Longrightarrow \&gr_i = pr_k \wedge pr_k \nrightarrow gri$ (pour *S'*)

$\Longrightarrow \neg(S'; gr_i, O')$

At state	**On the client side**	**On the server side**
t_n	$\&gr_i \in O \wedge \&gr_i = pr_k$	$pr_k \rightarrow gr_i$
t_{n+1}	$\&gr_i \in O \wedge \&gr_i = pr_k \wedge W(S; O, O')$	$pr_k \rightarrow gr_i$ No change
t_{n+2}	$\&gr_i \in O \wedge \&gr_i = pr_k \wedge W(S; O, O')$ No change	Assessment of the client request and authorizations by the AME: Auth(*S* ; gr_i)$_{(ID\text{-}\&gri)}$
t_{n+3}	$\&gr_i \in O \wedge \&gr_i = pr_k \wedge W(S; O, O')$ No change	$pr_k \rightarrow gr_i$
t_{n+4}	$\&gr_i \in O' \wedge \&gr_i = pr_k \wedge R(S'; O')$	$pr_k \rightarrow gr_i$ No change
t_{n+5}	$\&gr_i \in O' \wedge \&gr_i = pr_k \wedge R(S'; O')$ No change	Assessment of the client request and authorizations by the AME : NotAuth(*S'* ; gr_i)$_{(ID\text{-}\&gri)}$
t_{n+6}	$\&gr_i \in O' \wedge \&gr_i = pr_k \wedge R(S'; O')$ No change	$pr_k \nrightarrow gr_i \wedge pr_k \rightarrow$ Null
Final state	$\&gr_i \in O' \wedge \&gr_i = pr_k \wedge R(S'; O') \wedge pr_k \nrightarrow gr_i \wedge pr_k \rightarrow$ Null	

Résultat d'application de ce scénario :

Suite à un flux de l'information $\&gr_i$ initié par le sujet autorisé *S* de l'objet *O* vers l'objet *O'*, le sujet non autorisé *S'* ne peut pas avoir accès à gr_i par accès à *O'* qui renferme la référence à ce granule. En effet, $\neg(S', gr_i, O')$ car la référence qu'il peut lire de l'objet *O'* ($\&gr_i \in O'$) est égale à la valeur d'un pointeur ($\&gr_i = pr_k$) qui ne pointe pas vers gr_i. Autrement dit, le sujet non autorisé *S'* a lu la référence au granule d'information confidentiel, cette lecture déclenche un processus de validation des autorisations de *S'*. Cette vérification entraine une annulation du pointeur vers gr_i pour ce sujet qui, par conséquent, ne peut pas accéder au granule d'information.

Observation 1. (voir hypothèse de travail dans le Chapitre 1, Section 1.4.)

On a ainsi démontré que **toute tentative du sujet *S* de transférer -de façon volontaire ou non- une information confidentielle à un sujet non autorisé *S'* rend cette information inaccessible pour *S'*.** Cette démonstration vérifie bien et confirme notre hypothèse de travail avancée dans le Chapitre 1. Ceci est, bien entendu, réalisé grâce à notre modèle basé sur la granularité et qui est dédié au contrôle de flux d'informations.

6.4.2.5 Scénario 3.b.ii : Contrôle total multi-domaine

Empêcher tout sujet de *lire* l'information à partir de n'importe quel objet contenant l'information confidentielle :

$\forall S', O',$ si $\&gr_i \in O'$ alors $\neg(S', gr_i, O')$ *(29)*

Notre modèle permet l'implémentation aisée de ce scénario qui n'est adressé explicitement par aucun des modèles de contrôle d'accès conventionnels. En effet, ces modèles contrôlent l'accès aux informations confidentielles uniquement par le contrôle des sujets et des objets appartenant au domaine de sécurité qu'ils couvrent.

Les modèles existants ne parviennent à remédier à cette situation qu'à travers des mécanismes additionnels tel le cryptage de données ou des procédés similaires surtout en l'absence d'un modèle de contrôle d'accès centralisé.

GBFC implémente ce type de contrôle multi-domaine total sans besoin de mécanismes additionnels du fait que quel que soit le domaine de sécurité de l'objet qui contient le granule d'information et quel que soit le domaine auquel appartient le sujet, une tentative d'accès par celui-ci est identifiée comme tentative d'accès illégitime par l'EGA. Par conséquent, la référence au granule dont dispose ce sujet ($\&gr_i \in O'$) est mise à jour pour pointer vers du nul ou vers du bruit :

En effet, $R(S'; O') \wedge NotAuth(S'; gr_i) \Longrightarrow \&gr_i = pr_k \wedge pr_k \nrightarrow gr_i$

$\Longrightarrow gr_i$ indisponible pour S'

At state	**On the client side**	**On the server side**
t_n	$\&gr_i \in O' \wedge \&gr_i = pr_k$	$pr_k \rightarrow gr_i$
t_{n+1}	$\&gr_i \in O' \wedge \&gr_i = pr_k \wedge R(S'; O')$	$pr_k \rightarrow gr_i$ No change
t_{n+2}	$\&gr_i \in O' \wedge \&gr_i = pr_k \wedge R(S'; O')$ No change	Assessment of the client request and authorizations by the AME : NotAuth $(S'; gr_i)_{(ID\text{-}\&gri)}$
t_{n+3}	$\&gr_i \in O' \wedge \&gr_i = pr_k \wedge R(S'; O')$ No change	$pr_k \nrightarrow gr_i \wedge (pr_k \rightarrow Null \vee pr_k \rightarrow noise)$
Final state	$\&gr_i \in O' \wedge \&gr_i = pr_k \wedge R(S'; O') \wedge pr_k \nrightarrow gr_i \wedge (pr_k \rightarrow Null \vee pr_k \rightarrow noise)$	

Résultat d'application de ce scénario :

S' ne peut pas lire gr_i suite à son accès à O' ($\neg(S'; gr_i, O')$) car la référence qu'il peut lire de l'objet O' ($\&gr_i \in O'$) est égale à la valeur d'un pointeur ($\&gr_i = pr_k$) qui ne pointe pas vers gr_i ($pr_k \nrightarrow gr_i$).

Observation 2.

Il est à noter que ce dernier scénario rejoint le scénario précédent comme preuve de notre hypothèse de travail, étant donné que ce scénario couvre un cas plus général de fuite d'information dans lequel on remédie à un tel flux illégitime par la prévention d'accès au granule d'information confidentiel par le sujet non autorisé. Ceci est évidemment fait à travers l'annulation de cette référence au niveau du serveur ($\&gr_i = pr_k \wedge pr_k \nrightarrow$ gri $\wedge$ ($pr_k \rightarrow$Null $\vee$ $pr_k \rightarrow$bruit)), avec possibilité de la rediriger vers un granule de bruit comme mesure dissuasive pour toute tentative d'accès illégitime.

En conclusion, nous avons présenté, dans ce chapitre, les fondements mathématiques et logiques du modèle de contrôle de flux basé sur la granularité et montré sa capacité à s'adapter avec les autres modèles de contrôle d'accès pour leur apporter cette fonctionnalité vitale de contrôle de flux. En effet, nous avons passé en revue les différents scénarios d'actions de contrôle de flux et nous sommes arrivés à la conclusion que GBFC arrive à passer ces défis avec succès comparé aux modèles conventionnels.

Il est évident, selon nous, qu'avec des travaux de recherche additionnels futurs ce modèle prouvera ses capacités et ses exploits une fois mis en application. Chose que nous essayons de survoler à travers un prototype logiciel du modèle dans le chapitre qui suit.

Chapitre 7 : Implémentation du GBFC

Une des raisons de réussite du modèle de contrôle d'accès basé sur les rôles (RBAC) est le succès qu'ont connu ses diverses implémentations dans plusieurs secteurs économiques et professionnels. En effet, une bonne implémentation d'un modèle est capable de ressortir ses atouts et ses limites favorisant ainsi la compréhension de ses diverses facettes. Dans ce chapitre, nous présentons brièvement un prototype logiciel du modèle de contrôle de flux basé sur la granularité sous forme d'une version limitée dont l'objectif est de servir à des fins de démonstration. Ce prototype, bien que limité à certaines fonctionnalités, est établi pour appuyer la faisabilité technique du modèle tout en offrant un outil d'évaluation de sa performance.

7.1 Engin de gestion d'accès

Dans la Section 5.2 du Chapitre 5 on a décrit l'Engin de Gestion d'Accès du GBFC. C'est un système logiciel qui implémente les mécanismes de base permettant de gérer les fonctionnalités principales du contrôle de flux basé sur la granularité. Il s'agit de trois sous-systèmes assurant les trois principales fonctions décrites ci-dessous :

1- Un *sous-système de Contrôle d'accès* (*Ang. Access Control Subsystem*) qui permet de gérer les critères de sécurité et les droits et mécanismes d'accès aux composants granulaires.
2- Un *sous-système de gestion de granularité* (*Ang. Granularity Management Subsystem*) qui se préoccupe des fonctions de granulation de l'information.
3- Un *sous-système de contrôle* (*Ang. Control Subsystem*) qui régit les interactions entre les composants de l'EGA ainsi que les liens de celui-ci avec les divers systèmes externes

La Figure 30 illustre la structure générale de l'EGA (*Access Management Engine*).

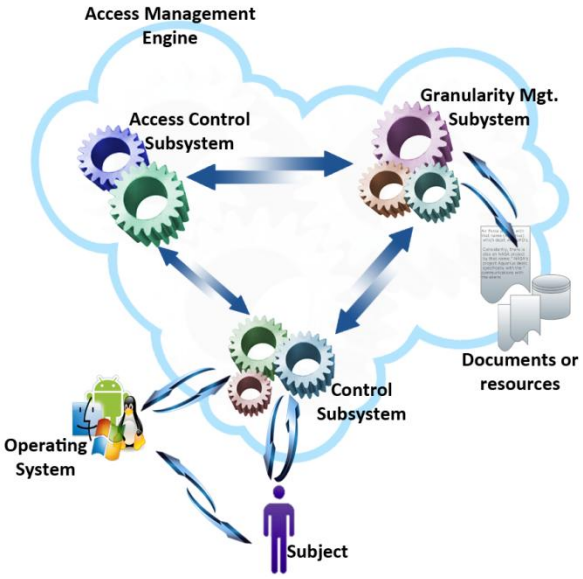


Figure 30. Structure générale de l'Engin de Gestion d'Accès

7.1.1 Système d'exploitation et Allocation volatile de fichiers (VFA)

Dans notre présent projet de recherche nous avons proposé une technique novatrice permettant de garantir l'implémentation du GBFC dans le système d'exploitation. Cette technique consiste en une allocation de fichiers volatile (VFA) qui permet de gérer l'accès aux granules d'information à travers des références volatiles.

Cette technique permettra de garantir une protection continue des informations confidentielles et profitera de plusieurs avantages et considérations technologiques actuellement en application tels la puissance de traitement des nouveaux systèmes, les réseaux et les innovations reliées au protocole internet ainsi que des technologies des mémoires d'ordinateur à usage unique.

L'allocation volatile de fichiers (VFA) est une technique d'allocation de fichiers similaire au système d'allocation de fichiers réseau (NFS) [122] avec comme différence que le VFA offre une gestion dynamique des index (références dans GBFC) en plus d'un niveau de granularité adapté à celui choisi par l'administrateur de sécurité dans le serveur.

7.1.2 Modélisation et développement du prototype GBFC

Notre recherche comporte, en plus du modèle logique présenté dans le chapitre 6, un prototype logiciel fonctionnel de simulation et de test des fonctionnalités du GBFC. Ce prototype est développé sur un logiciel de traitement de texte qui est Microsoft Word. Le choix de ce logiciel provient du fait que c'est un logiciel à grande présence dans le domaine du traitement du texte que ce soit personnel ou professionnel. C'est aussi un logiciel simple, toutefois puissant et qui offre un environnement favorable au développement de solutions logicielles annexes ou complémentaires telle que la nôtre. La technologie qui nous permettra de développer notre prototype (décrite dans la Section ci-dessous) est VSTO qui est aussi une technologie de Microsoft et qui s'intègre parfaitement avec l'environnement de traitement de texte choisi.

7.1.2.1 Visual Studio Tools for Office (VSTO)

Les outils de Visual Studio pour Office (VSTO) sont des solutions de programmation de Microsoft destinées au développement de logiciels pour les applications de la suite Microsoft Office. VSTO offre un environnement de développement simple et robuste permettant de se servir de certains langages de programmation de MS Visual Studio (VB .Net et C#) pour développer des programmes qui réalisent des fonctions spécifiques aux besoins des usagers des logiciels de MS Office (MS Word, Excel, …). Ces programmes sont sous forme de suppléments (add-ons) facilement intégrables dans ces logiciels et qui permettent soit :

- D'ajouter de nouvelles fonctionnalités non disponibles au sein des applications de la suite Office.
- De regrouper un ensemble de fonctionnalités existantes dans le but d'accélérer le traitement des données et améliorer le rendement de l'usager.

VSTO offre un ensemble d'avantages, tels la programmation orientée objet, les contrôles, les classes, la facilité de déploiement, etc. [123].

7.2 Prototype logiciel GBFC

7.2.1 Conception

Avec cette vision assez détaillée du modèle nous proposons une traduction des fonctionnalités du GBFC en prototype logiciel afin de disposer d'un environnement d'application et de test des diverses capacités du modèle. On a commencé par une phase de modélisation logicielle UML [124, 15, 125, 126] en développant le diagramme des cas d'utilisation qui décrit de façon générale l'ensemble des interactions entre les divers acteurs et le système. Ces interactions sont listées de manière simplifiée dans le Tableau 15 ci-dessous. Généralement, un diagramme de cas d'utilisation permet d'illustrer l'ensemble des séquences d'actions que le système performe et qui produisent un résultat de valeur pour un acteur particulier. Il est donc utilisé pour structurer les comportements dynamiques au sein d'un modèle [124]. Il reste à noter que pour des raisons d'allégement et de simplification les acteurs de certaines actions sont omis du tableau et du diagramme. Les acteurs de ces actions sont les mêmes que ceux concernés par les actions auxquelles elles sont des prérequis (include).

Num.	Cas d'utilisation	acteur	prérequis
1	Gérer les paramètres de sécurité ($T\gamma$,$T\alpha$,$T\rho$,$T\nu$)	Admin. de sécurité	
2	Appliquer les critères de sécurité	Admin. de sécurité	1
3	Identification / Authentification	Utilisateur	
4	Autorisation	Utilisateur	3
5	Demande d'accès	Utilisateur	4
6	Générer AF	Système d'exploitation	
7	Générer AFV	Système d'exploitation	
8	Donner accès à la ressource	B.D. des ressources	1, 6, 7
9	Accès à la ressource	Utilisateur	4,8

Table 15. Cas d'utilisations GBFC

Le diagramme simplifié de cas d'utilisation est dressé dans la Figure 31.

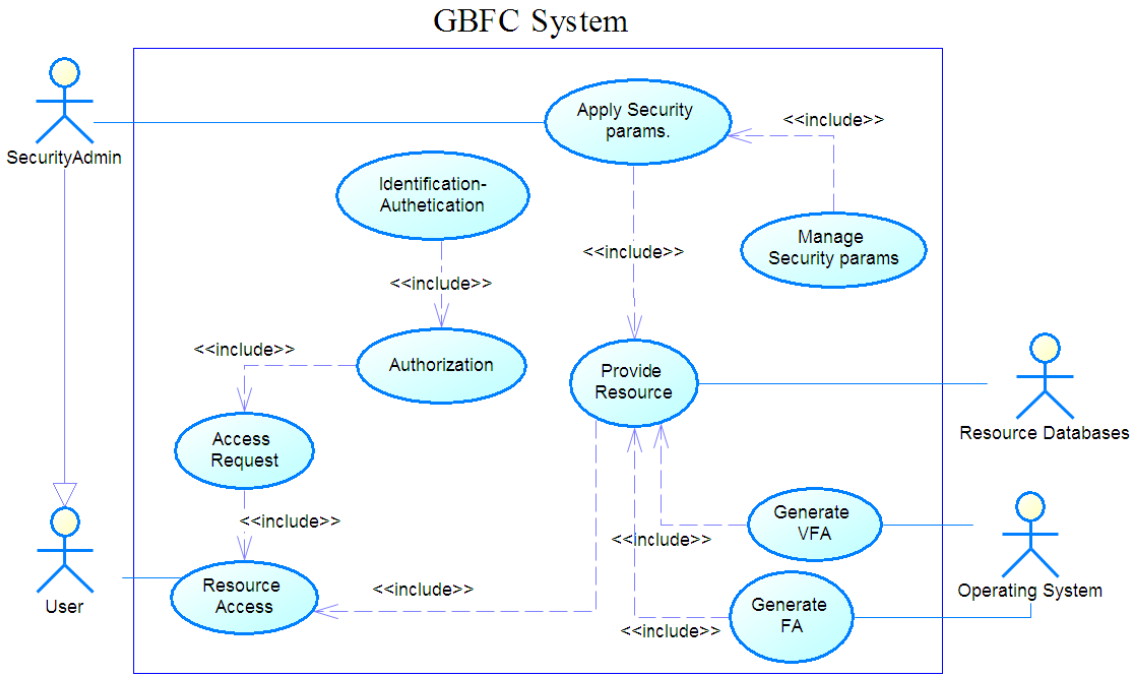


Figure 31. Diagramme de cas d'utilisation

Se basant sur le diagramme de cas d'utilisation on parvient à cerner les différentes fonctionnalités du prototype à développer. Ainsi, l'étape suivante est de proposer des interfaces utilisateurs adaptées aux exigences et actions de chaque acteur vis-à-vis du système. On dispose alors de deux principales interfaces : une pour l'administrateur de sécurité et une pour les autres usagers du système.

7.2.2 Développement

Le développement de notre prototype est effectué sur une plateforme logicielle de traitement de texte existante qui est Microsoft Word. Ce choix nous permet une intégration simple, tout en ayant l'opportunité d'utiliser un environnement de développement offrant les ressources nécessaires pour réaliser ce projet qui est : le VSTO (décrit avec plus de détails dans la Section 7.1.2.1). VSTO permet d'intégrer des fonctionnalités additionnelles et personnalisées au sein de MS Word dans des *Rubans* supplémentaires conçus par les développeurs. De ce fait, pour les deux interfaces utilisateurs de notre prototype on dispose d'un ruban GBFC comme montré dans la prise d'écran de la Figure 32. Pour chacune des deux catégories d'utilisateurs le ruban intègre les divers contrôles adaptés à leurs droits

d'accès, leurs autorisations et leurs fonctions dans le système. On se limitera, tout de même, à une implémentation du GBFC pour deux des modèles de contrôle d'accès existants (MAC et ABAC), et ceci pour des raisons de simplification.

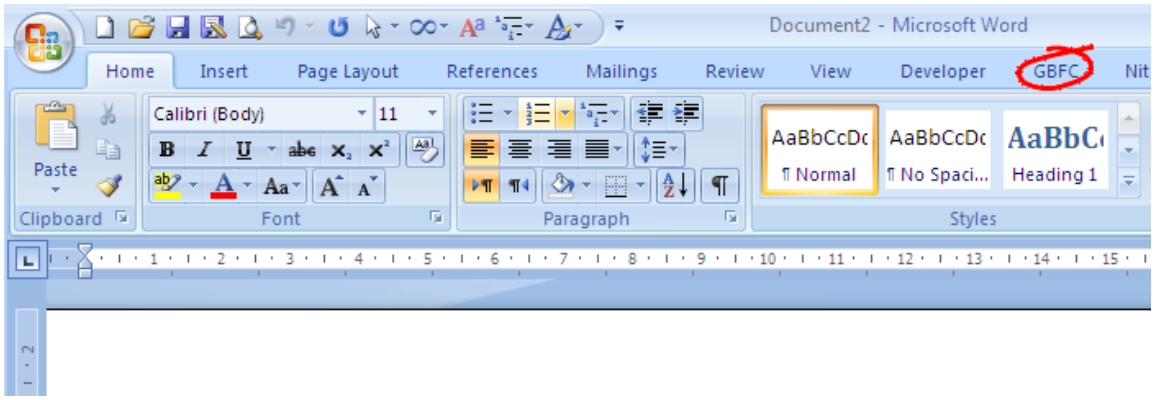


Figure 32. Prise d'écran du prototype GBFC

Comme mentionné dans la Section 5.3.5 du chapitre 5, GBFC dépend du système de contrôle d'accès existant pour réaliser les opérations d'identification et d'authentification avant de procéder à la gestion des autorisations et à la gestion d'accès aux ressources. Dans notre prototype, on a intégré ce mécanisme qui permet de réaliser l'identification et l'authentification de l'utilisateur de façon plus simple et plus flexible. Ceci nous permet une meilleure adaptation du contrôle d'accès aux objectifs de démonstration et d'expérimentation de notre modèle en action. A ce stade, et sur la base du nom et du mot de passe entrés via un mécanisme de login, l'utilisateur est identifié et est attribué ses autorisations relativement aux fonctions du système et au document à accéder (Figure 33).

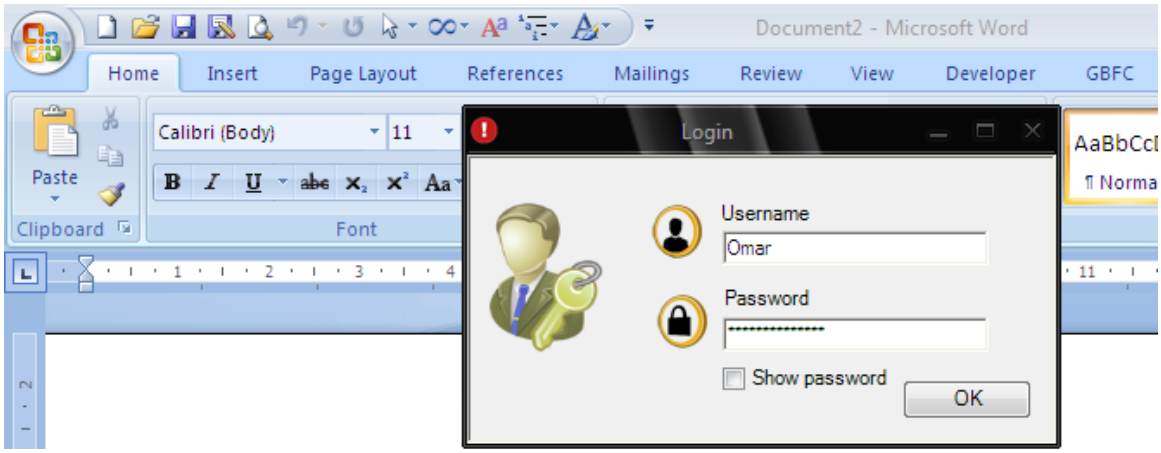


Figure 33. Prise d'écran fenêtre de login

Ainsi, l'usager "Omar", par exemple, est identifié comme administrateur de sécurité, ce qui lui permet de visualiser les contrôles de gestion des diverses fonctionnalités attribuées à sa fonction dans le système tel que représenté dans la Figure 34. Un deuxième usager "User" se verra authentifié comme utilisateur standard qui aura accès aux fonctionnalités du système via son interface client. L'accès par un troisième usager non autorisé engendrera une adaptation de ressources et des fonctionnalités du système pour garantir le niveau souhaité de sécurité et de confidentialité des informations.

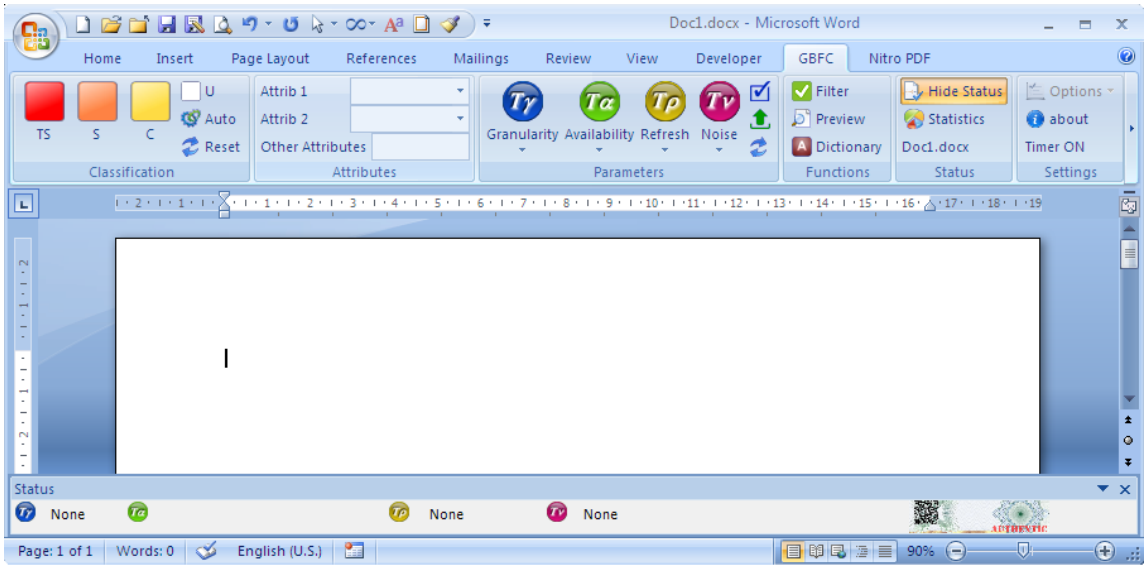


Figure 34. Prise d'écran interface administrateur

7.2.2.1 Interface Administrateur

7.2.2.1.1 Organisation

Le prototype implémente les différentes fonctions de contrôle de flux dans le ruban GBFC intégré à Microsoft Word. Ce ruban renferme plusieurs groupes de contrôles :

Groupe Classification : qui offre la fonction d'étiquetage (tagging) des mots du texte du document sur la base de leur classification ((*U), (C), (S)* et *(TS)*). L'étiquetage est visualisé sous forme de couleurs appliquées au texte classifié (respectivement : Noire, Jaune, Olive et Rouge) conformément aux classifications des modèles multi-niveaux. L'étiquetage peut se faire par mot ou par sélection de plusieurs mots et peut être révoqué (reset) de la même

manière. De plus, le prototype offre la possibilité de révoquer la classification du document tout entier en plus de la possibilité de classification automatique sur la base de choix opérés par l'administrateur de sécurité (bouton Auto) voir Figure 35.

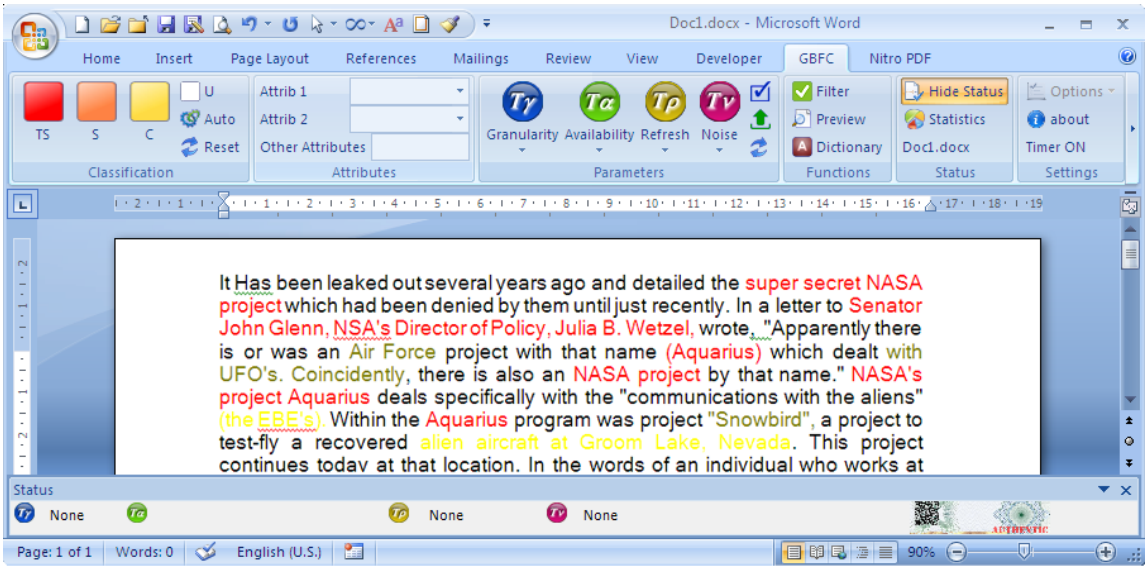


Figure 35. Prise d'écran divers groupes et fonctions du prototype

Groupe Attributs : Représente la classification basée sur les attributs. En effet, ce groupe renferme des outils de sélection d'attributs permettant d'appliquer les paramètres de sécurité sur la base des attributs utilisateur, environnement et autres (Figure 35).

Groupe Paramètres : Ce groupe permet la gestion des paramètres de sécurité GBFC (Niveau de granularité $T\gamma$, Taux de disponibilité $T\alpha$, Taux de rafraîchissement $T\rho$, Niveau de bruit Tv). Ces paramètres peuvent être appliqués au seul document ouvert ou à un ensemble de documents sélectionnés. La figure 36 montre les valeurs de chacun des paramètres de sécurité que l'administrateur de sécurité peut appliquer au document. Un volet "Status" au pied du document affiche les valeurs sélectionnées. Il faudra noter que la classification des composants texte du document, les attributs et les valeurs spécifiés pour les paramètres de sécurité sont enregistrés comme métadonnées du fichier et sont par la suite chargés à chaque ouverture de celui-ci.

Groupe Fonctions : Le groupe fonctions regroupe des contrôles permettant d'appliquer et de visualiser les différents choix de sécurité du document. Il renferme un bouton de validation des différentes options sélectionnées par l'administrateur de sécurité en plus de contrôles d'aperçus, de gestion de dictionnaires, etc.

Groupe Statut : Ce groupe renferme des contrôles d'affichage des statuts des différents paramètres de sécurité, des statistiques du document et autres statuts utiles pour la gestion et le contrôle de flux.

Groupe Configuration (*Settings*): Englobe des options de configuration et les informations du système.

7.2.2.1.2 Fonctionnement

A travers cette interface l'administrateur de sécurité accède au document renfermant les informations confidentielles et utilise les contrôles du groupe C*lassification* et *Attributs* pour attribuer à chaque élément texte une classification qui définit son niveau de confidentialité. Dans notre prototype nous avons opté pour 4 niveaux de classification à savoir : ((*U), (C), (S)* et *(TS)*). L'administrateur sélectionne le composant texte (mot, phrase, paragraphe, etc.) et utilise les boutons du groupe *Classification* pour leur attribuer la classification souhaitée. Cette classification peut aussi être automatisée par la définition des critères à considérer dans ce processus (toutes les phrases qui contiennent des noms propres par exemple). Le système est basé sur une technique d'étiquetage (*tagging*) des composants texte, qui est implémentée dans notre prototype sous forme de couleurs pour raison de simplification et de clarté (se référer à la Figure 35). Plus d'options de classifications peuvent être offertes -à posteriori- sous forme de rôles et d'attributs (pour intégrer RBAC et ABAC) dans le groupe attributs. Généralement cette intégration se fait par l'implémentation des directives du MAC dans ces deux modèles (cf. Section 4.4, Chapitre 4). Après avoir achevé la phase de classification du document, l'administrateur utilise les menus du groupe *Paramètres* pour configurer les paramètres de sécurité appliqués au document (Figure 36). Ces configurations (niveau de granularité $T\gamma$, taux de disponibilité

$T\alpha$, Taux de rafraîchissement $T\rho$, Niveau de bruit $T\nu$) sont intégrés dans le document sous forme de métadonnées. Certains des paramètres de sécurité (taux de disponibilité basé sur le type de données et taux de rafraîchissement par exemple) n'ont pas été développés dans le cadre de notre prototype du fait de la complexité de leur implémentation ou de l'inadaptation de l'environnement de programmation à cette implémentation.

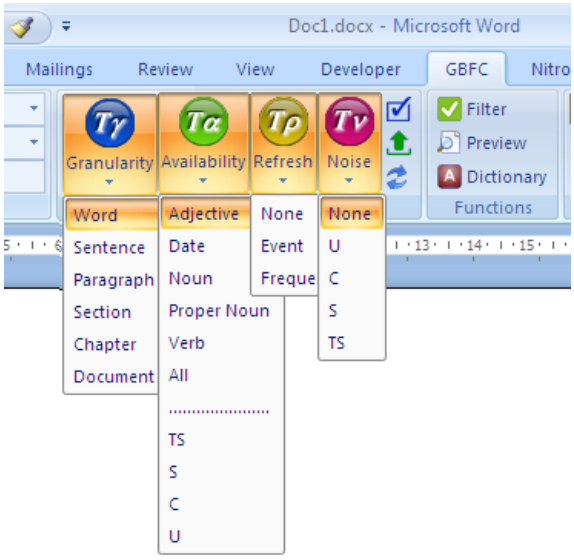
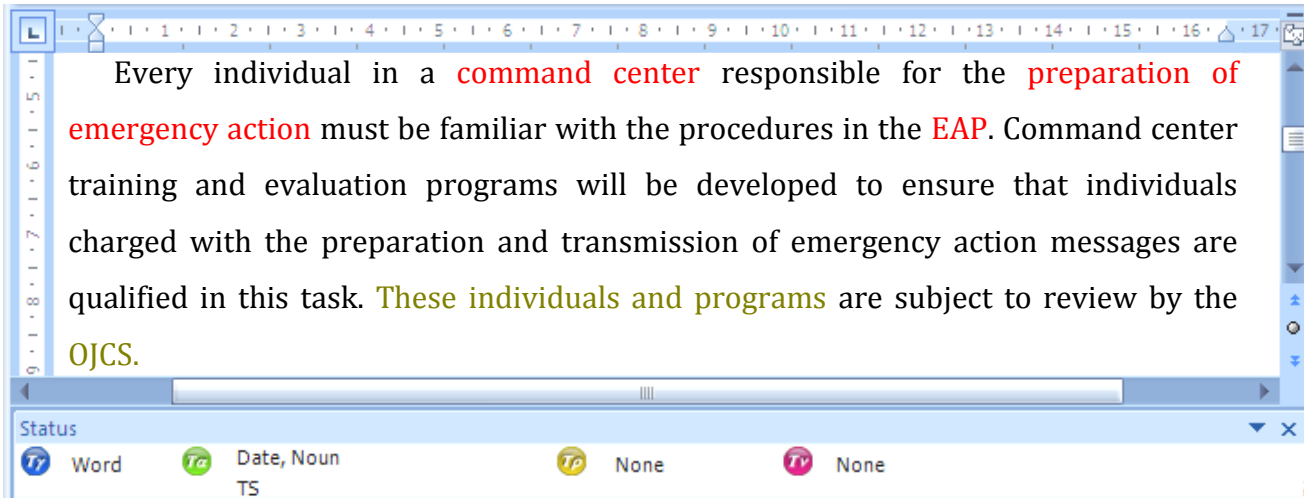


Figure 36. Prise d'écran groupe critères de sécurité

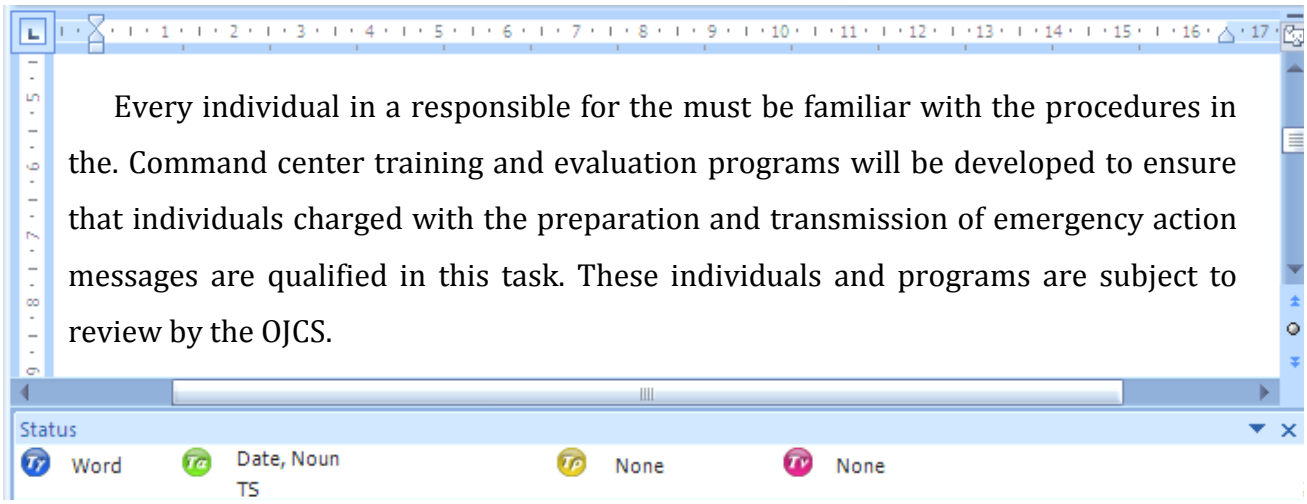
Les critères choisis peuvent être visualisés sur la barre d'état affichée au pied du document :

L'administrateur peut par la suite valider son choix par le bouton apply : qui affecte les critères choisis au document. Il peut aussi tout mettre à zéro avec le bouton reset : . Dans le cas où le document ouvert par l'administrateur renferme déjà des critères de sécurité prédéfinis, celui-ci peut les charger en utilisant le bouton load : . Après avoir défini et validé son choix des critères de sécurité du document, l'administrateur peut visualiser le résultat qui sera affiché en cas d'accès par un utilisateur non autorisé (en

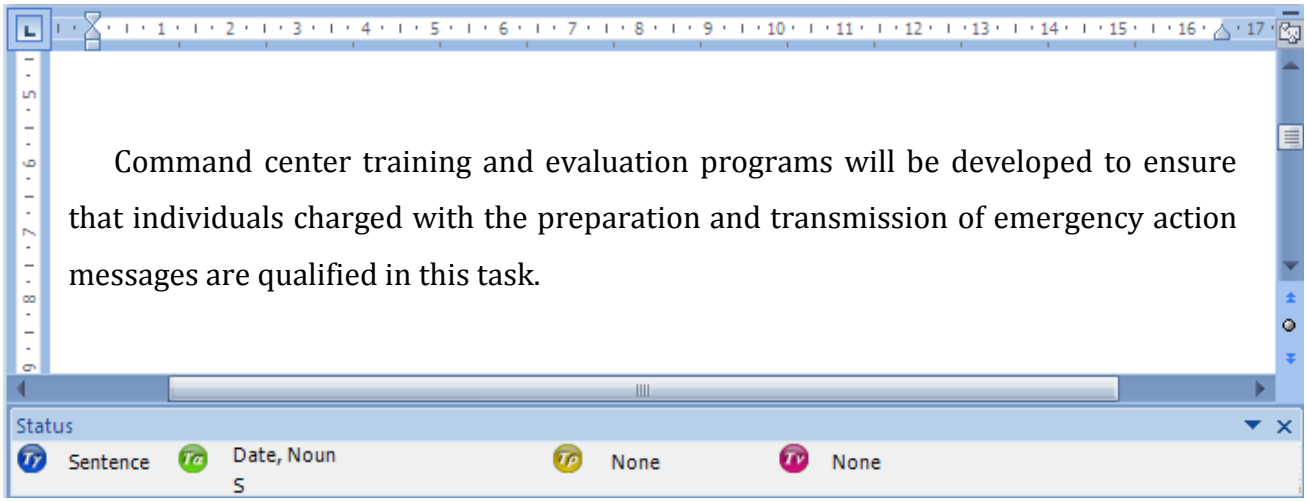
utilisant le bouton Filter). Ainsi, par exemple si le texte de l'encadré ci-dessous est traité par l'administrateur selon cette classification avec fixation des critères de sécurité *Tγ*= MOT; *Tα=TS;* et *Tv*= AUCUN :



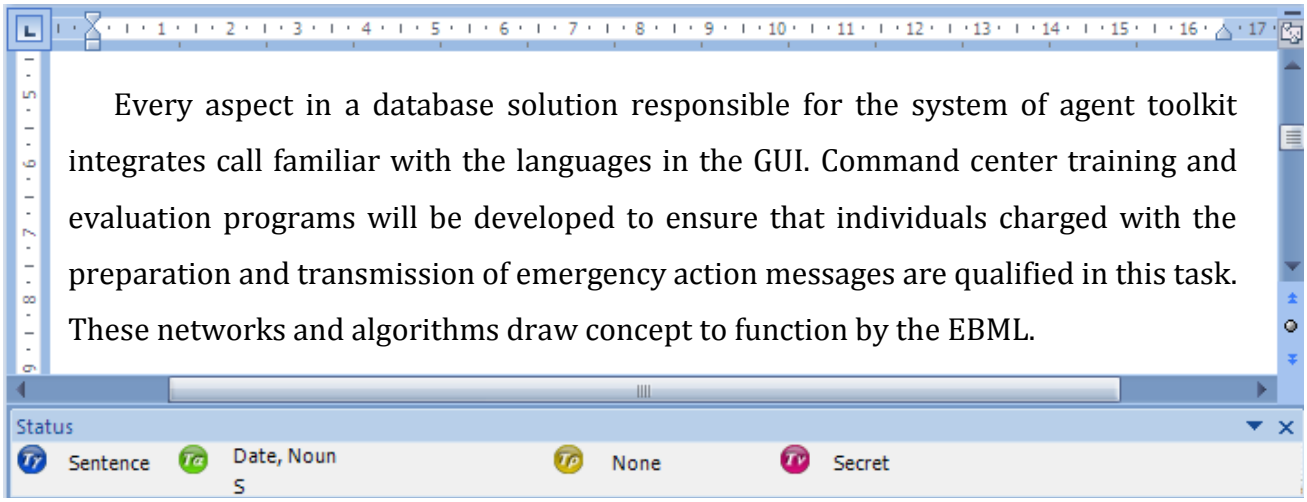
Ceci donnera en cas d'accès illégitime chez le sujet non autorisé :



Si l'administrateur change les critères de sorte que $T\gamma$= PHRASE; $T\alpha$=*S;* et $T\nu$= AUCUN le résultat en cas d'accès illégitime (niveau client) sera :



S'il introduit l'injection de bruit ($T\nu = S$) au cas précédent le résultat sur la station client sera du genre :



On remarque que, dans ce dernier cas de scénario, les phrases qui comportent des éléments classifiés SECRET (*S*) sont automatiquement remplacées par des phrases de bruit.

7.2.2.2 Interface Utilisateur

7.2.2.2.1 Organisation

L'interface utilisateur est développée avec le moindre de détails et de contrôles apparents afin d'épargner à l'utilisateur le souci relié à la gestion de sécurité qui se fait en arrière plan. Ceci rend le système et ses interactions imperceptibles du point de vue de l'utilisateur au niveau des stations clients. Cette interface permettra tout de même au sujet de se connecter au système et de s'identifier afin de valider ses autorisations. De la même sorte il pourra se déconnecter et visualiser certaines informations (sur le document ou autres) que l'administrateur, ou les instances de gestion de l'organisation jugent utiles pour l'accomplissement de sa tâche.

Dans tous les cas, le sujet qui accède aux informations confidentielles au niveau d'une station client n'est aucunement capable de percevoir les mécanismes de sécurité qui sont derrière son accès aux informations confidentielles. En plus, dans le cas d'accès illégitime par un sujet malveillant, et bien que les informations confidentielles soient bien protégées et isolées au niveau du serveur, le document accédé pourra subir encore plus de manipulations (au niveau technique) dans le but de minimiser les risques qui peuvent surgir d'un tel accès.

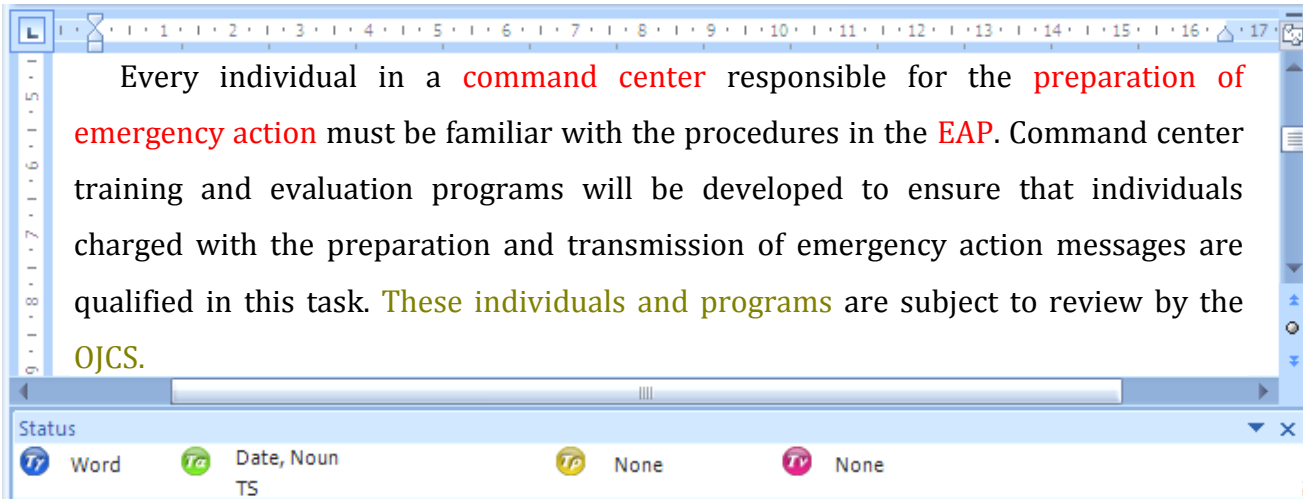
7.2.2.2.2 Fonctionnement

En l'absence d'une architecture client/serveur la simulation des fonctionnalités du GBFC est faite à travers l'utilisation des liens et des signets incorporés dans MS Word. On dispose alors du document confidentiel granulé et référencé, qui intègre les critères de sécurité fixés par l'administrateur et qui sera accédé par un sujet donné au niveau du client. Ce document comporte des paragraphes insérés sous forme de liens (links), représentant les références dans le GBFC, à partir d'un deuxième document (qui comporte les informations confidentielles) simulant ainsi le document d'origine présent sur le serveur (comme préconisé par le GBFC). A l'accès par un sujet, notre programme (simulant l'Engin de Gestion d'Accès du GBFC) modifie la structure du document d'origine pour appliquer les critères de sécurité prédéfinis et adapter le contenu à afficher aux autorisations du sujet qui

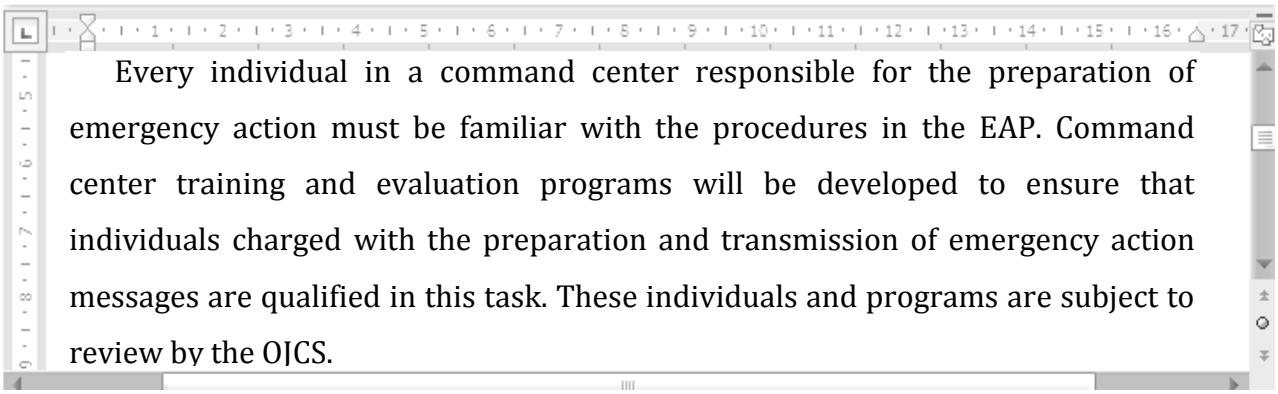
initie l'opération d'accès (simulant l'action de mise à jour des pointeurs au niveau du serveur pour le GBFC). Les paragraphes correspondants aux liens présents dans le document accédé par le sujet (niveau client) seront alors remplacés par les paragraphes correspondants, par du vide ou par du bruit respectivement aux cas d'accès par un sujet autorisé, non-autorisé accrédité ou non-autorisé malveillant.

Relativement à leurs droits d'accès et autorisations, les sujets qui accèdent au document au niveau des stations clients pourront visualiser des résultats similaires à ceux visualisés via le bouton 

par l'administrateur après application des critères de sécurité. Cependant le sujet n'a aucune connaissances ni de la classification du document, ni des critères de sécurité qui y sont appliqués ($T\gamma$, $T\alpha$, $T\rho$, $T\nu$), ni des mécanismes d'application et de gestion des ces différents composants de sécurité. Prenons ainsi le même document de la Section 5.4 du Chapitre 5. Comme déjà vu, l'administrateur de sécurité visualise le document au niveau du serveur sous cette forme :

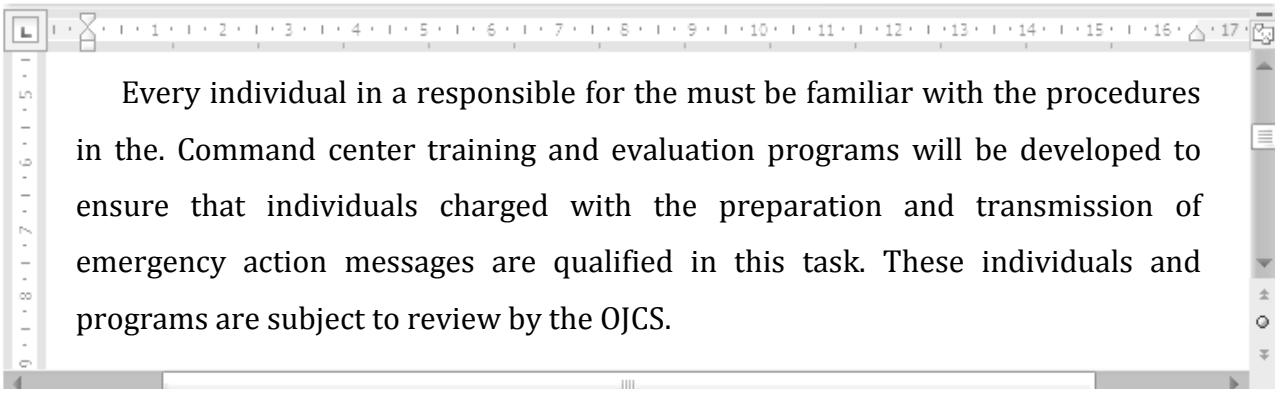


Avec $T\gamma$=*WORD*, $T\alpha$=*TS*, $T\nu$=*None*, le sujet de classification Top Secret aura :



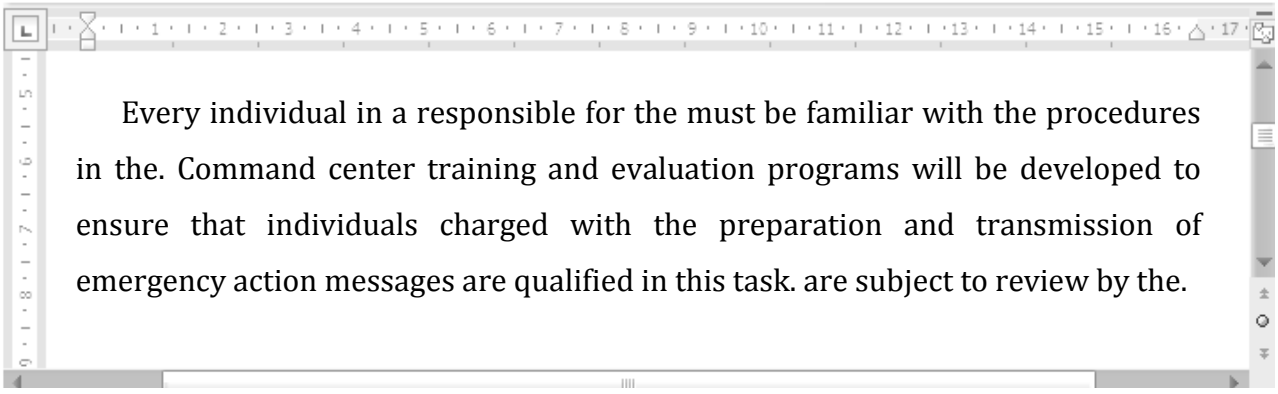
Every individual in a command center responsible for the preparation of emergency action must be familiar with the procedures in the EAP. Command center training and evaluation programs will be developed to ensure that individuals charged with the preparation and transmission of emergency action messages are qualified in this task. These individuals and programs are subject to review by the OJCS.

Le sujet de classification Secret aura :



Every individual in a responsible for the must be familiar with the procedures in the. Command center training and evaluation programs will be developed to ensure that individuals charged with the preparation and transmission of emergency action messages are qualified in this task. These individuals and programs are subject to review by the OJCS.

Un sujet non autorisé aura un résultat comme ceci :

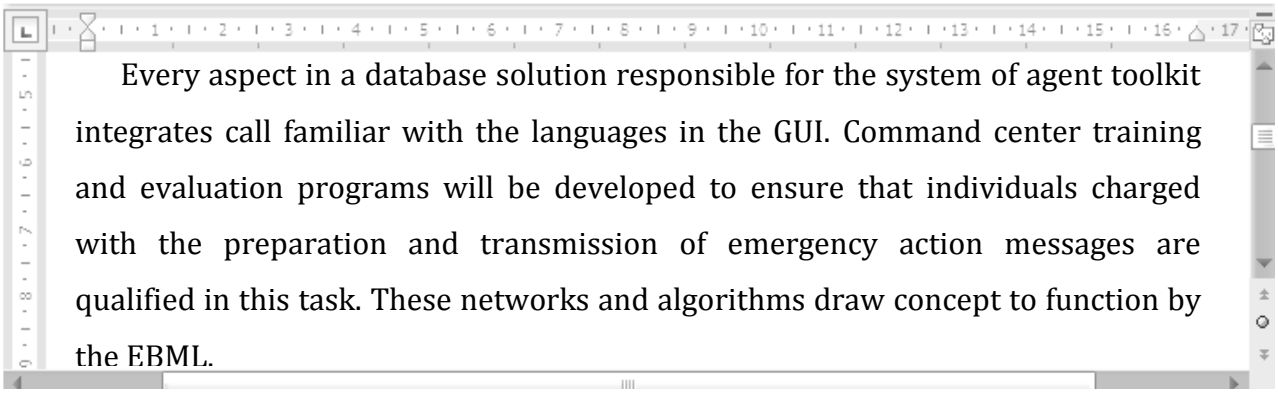


Every individual in a responsible for the must be familiar with the procedures in the. Command center training and evaluation programs will be developed to ensure that individuals charged with the preparation and transmission of emergency action messages are qualified in this task. are subject to review by the.

… et ainsi de suite.

Suite à un changement des critères de sécurité par l'administrateur de sécurité du genre : *Tγ=SENTENCE, Tα=S, Tν=S*

On se retrouve avec un niveau de granularité Phrase, un taux de disponibilité et une injection de bruit de niveaux Secret et par conséquent, un sujet non autorisé aura un résultat du genre:


Every aspect in a database solution responsible for the system of agent toolkit integrates call familiar with the languages in the GUI. Command center training and evaluation programs will be developed to ensure that individuals charged with the preparation and transmission of emergency action messages are qualified in this task. These networks and algorithms draw concept to function by the EBML.

Ceci nous montre le niveau de flexibilité dont dispose l'administrateur de sécurité quant à l'implémentation des critères de sécurité et à l'application des exigences de sécurité en général et de confidentialité de l'information en particulier dans les divers scénarios d'accès.

D'autres scénarios peuvent être couverts durant la démonstration de ce prototype qui sera offerte dans le cadre de la soutenance finale.

7.3 Perspectives d'implémentation

Dans le présent chapitre, on a présenté le prototype logiciel GBFC et on a proposé une implémentation de certains composants et fonctionnalités décrits tout au long de ce projet de recherche. Au delà du niveau prototype développé dans le cadre de cette thèse, et comme perspective à venir, nous prévoyons de compléter ce système en intégrant les principales fonctions de gestion et de contrôle de flux sous une architecture client/serveur

afin de pouvoir implémenter, tester et évaluer de façon plus approfondie notre modèle en application. Il est cependant important de souligner que ce modèle -comme c'est le cas pour d'autres modèles de sécurité- nécessite une implémentation au niveau système d'exploitation. Une pareille implémentation permettrait de profiter à fond des capacités qu'offrent l'aspect granulaire de l'information, les mécanismes d'accès basés sur les références et l'action d'injection de bruit pour atteindre l'objectif final de garantie d'un contrôle de flux d'information robuste et adapté aux besoins des individus et des organisations.

Chapitre 8 : Domaines d'applications et analyse critique du modèle

Dans cet avant-dernier chapitre nous dressons une brève description des domaines d'application possibles du modèle de contrôle de flux basé sur la granularité. Nous essayons aussi de réaliser une analyse de certaines limites apparentes relatives à l'implémentation du modèle en proposant des réponses à ces différentes critiques.

8.1 Domaines d'applications

Dans cette recherche nous avons examiné les capacités du GBFC relativement à l'instauration du contrôle de flux d'informations en tant que modèle logique dédié. Ces capacités offrent à ce modèle d'importantes opportunités d'application dans plusieurs domaines.

En effet, nous avons traité dans cette thèse les applications de ce modèle dans le domaine de protection de la confidentialité d'informations sous forme de texte. Cette protection peut être généralisée à d'autres types de données qui généralement supportent la manipulation sous forme granulaire. Des exemples de ces types de données sont : les bases de données, les images, les vidéos, etc. Une fois qu'on arrive à contrôler l'aspect granulaire de ces types de données (généralement déjà accompli par les travaux de recherche dans ces domaines), il sera aisé de leur appliquer les autres critères de sécurité du GBFC. On aura ainsi la possibilité de charger une image (logée dans un serveur web par exemple) sous forme de granules de pixels dont certains sont confidentiels et par conséquent accédés uniquement via des références volatiles gérées par l'engin de gestion d'accès du GBFC.

Cette possibilité est déterminante du fait que l'implémentation du GBFC pourra prendre en charge ces formes de données et offrir une solution à certains problèmes de protection

des droits d'auteurs, d'informations personnelles et de vie privée. On effet, on pourra envisager, par exemple, le cas d'accès par un sujet non autorisé à certaines zones d'une photo personnelle uniquement alors que d'autres sont inaccessibles ou même remplacées par des pixels de bruit. On sera aussi capable de protéger un document confidentiel d'être reproduit ou copié en y appliquant un accès granulaire à travers les références comme décrit dans la Section 6.2 du Chapitre 6.

Dans le domaine de la protection des droits d'auteur, l'application du mécanisme de rafraîchissement du GBFC pourra permettre, par exemple, de limiter à une seule lecture l'accès d'un utilisateur à une vidéo, en plus de la possibilité de la protection du contenu contre les copies illégitimes (*cf.* Section 6.2.3, Chapitre 6).

On a déjà mentionné que GBFC est destiné à être implémenté sur le système d'exploitation permettant ainsi de transformer tout ordinateur en un serveur offrant les services de sécurité et de contrôle de flux de ce modèle. Un client pourra, par exemple, envoyer un dossier détaillé de demande de crédit à une institution financière sans que le dossier ne quitte son ordinateur, et sans que cette institution ait la possibilité de copier ou de reproduire son contenu, protégeant ainsi -à un certain point- les informations personnelles et de vie privée qui peuvent s'y trouver.

Ces exemples peuvent être généralisés pour couvrir des implémentations d'envergure pour garantir les fonctions de sécurité et de contrôle de flux multi-domaines sur les plateformes des réseaux sociaux et dans les Clouds, du fait que chaque granule peut être protégé de façon individuelle et indépendamment de la plateforme qui le renferme.

Un autre domaine d'application pour le GBFC est celui de la protection contre les fuites d'informations dans les situations de pertes de matériel. Les statistiques montrent qu'un nombre non négligeable de problèmes de flux illégitimes d'informations est causé par ces pertes. Dans notre cas, la perte de matériel contenant des informations confidentielles n'est rien d'autre que la perte de références à ces informations. Ces références n'ont aucune

valeur tant qu'elles n'ont pas été validées par l'EGA au niveau du serveur (Section 5.3.4, Chapitre 5).

Grace à sa propriété centralisée, notre modèle peut garantir une traçabilité continuelle des divers accès aux granules d'informations. En effet, tout accès aux granules confidentiels, que ce soit en lecture en écriture, se fait via des références présentes au niveau du système client et validées par l'EGA. Ceci se fait via le réseau et nécessite une identification préalable du client (identité, domaine, localisation, …) et donne lieu à un contrôle d'usage subséquent (date et heure d'accès, durée d'accès, opérations de copies, de modifications et/ou de transferts, etc.). Toutes ces opérations de traçabilité -entre autres- peuvent être gérées et assurées à travers l'architecture client/serveur du GBFC.

La sécurité appliquée au Cloud Computing est aussi un domaine d'application possible du GBFC. Cet environnement ouvert, large et distribué renferme beaucoup de défis de sécurité qui méritent d'être explorés et relevés par de nouveaux modèles de sécurité qui proposent des solutions adaptées qui supportent le multi-domaine et la gestion dynamiques des critères de sécurité. En effet, dans ces systèmes, le domaine de sécurité du fournisseur de ressources est différent de celui de l'utilisateur et les mécanismes de sécurité classiques, qui manquent souvent de flexibilité, ne sont généralement pas adaptés (excepté pour ABAC). Appliquant les concepts de granularité et d'accès via les références, GBFC pourra s'adapter parfaitement à ce genre d'environnements tout en offrant un bon niveau de flexibilité, particulièrement avec une implémentation dans le système d'exploitation. Les actions de rafraîchissement et d'injection de bruit viennent alors renforcer le contrôle de flux. En plus, l'architecture adoptée dans le Cloud Computing favorise une gestion et un contrôle de sécurité centralisés nécessaires pour une bonne implémentation des mécanismes de notre modèle.

Finalement, il est à souligner qu'on est conscient que l'adaptation du GBFC à ces divers domaines d'applications nécessite davantage d'investigation et d'efforts de recherche.

8.2 Critiques et difficultés possibles : réponses et justificatifs

Dans cette recherche, nous avons essayé d'asseoir les fondements logiques et techniques du GBFC tout en donnant des exemples d'applications relatifs aux différents mécanismes du modèle. Cependant, certaines remarques peuvent être soulevées relativement à des difficultés éventuelles liées à la conception et au mode d'action de ces mécanismes. On essayera ci-après de donner des réponses à ces remarques et d'offrir des clarifications supplémentaires. Ceci en prenant en considération que les détails techniques d'implémentation de notre modèle ne font pas partie explicitement de l'objectif de cette recherche.

1- *Problèmes liés à l'aspect centralisé de l'accès, de la gestion et du stockage de l'information. Cette propriété de système centralisé sur laquelle est basée le modèle GBFC pourrait poser un problème de disponibilité de l'information en cas de failles du système central ou des limites de performance en cas de problèmes de connexions réseaux.*

Certes, l'EGA, les informations confidentielles et la base de données des ressources utilisées par ce système sont tous logés dans le serveur, mais ceci est essentiel pour assurer un contrôle d'accès et de flux d'informations confidentielles.

De plus, l'architecture centralisée est de plus en plus adoptée, spécialement dans les services de messagerie, de bases de données distribuées, de réseaux sociaux et de Cloud Computing où il est très rare de constater des problèmes de dysfonctionnement ou de disponibilité. Ceci est dû à l'implémentation de plateformes multi-serveurs, multiservices et multi-localisation qui permettent à tout moment le passage à des serveurs de bases de données et d'applications secondaires (backup) en cas de failles des systèmes principaux.

On ajoute à ceci, les progrès achevés dans les accès réseaux et les services de communications qui deviennent de plus en plus accessibles, puissants, rapides, et fiables (accès distants, internet mobile, …).

2- *Considérant l'état actuel de la technologie, même avec une implémentation du GBFC, l'usager pourrait accéder aux granules d'information confidentiels sur son système client à travers leur chargement dans la mémoire graphique par exemple.*

En effet, avec GBFC, le sujet arrive à charger les granules classifiés -à travers leurs références- sur son système. Cependant il ne faudra pas oublier que :

- Ce modèle opère selon une architecture client/serveur qui est configurable par l'administrateur ou par les instances de sécurité.
- Les informations sont chargées dans leur forme granulaire, qui est configurable. L'accès aux informations peut être opéré à un niveau de granularité élevé (fine grained access). Cette granularité rend la tâche de copie de l'information difficile.
- GBFC est supposé être implémenté et intégré au système d'exploitation, ce qui permet un contrôle plus strict des accès aux objets localisés sur les stations clients (restrictions aux accès mémoires, restriction des opérations de copies, etc.). Une telle intégration, qui permettra la protection des références sur le client est envisageable, voire indispensable pour des systèmes de haute sécurité.
- Les technologies appliquées au domaine de sécurité avancent dans le sens de proposer des solutions plus restrictives de contrôle d'accès aux mémoires au niveau des systèmes. Le but est de veiller à ce que les objets qui ont servi à l'accès aux informations confidentielles soient libérés ou réaffectés à d'autres sujets de façon à prévenir les fuites et les accès illégitimes (*Object reuse and reallocation*) [39, 122]. La tendance est vers la proposition de restrictions additionnelles avec de nouveaux concepts de mémoires à lecture unique, etc. [127].

3- *GBFC pourrait s'avérer inefficace vis-à-vis des flux illégitimes dus au facteur humain.*

Avec ce modèle, on est loin de prétendre d'avoir complètement résolu le problème de flux illégitimes d'informations. Toutes les méthodologies qui adressent ce problème ne font que proposer des solutions pour repousser ou réduire l'éventualité (ou les occurrences) de ce genre de flux et minimiser ses impactes dans la vie des individus et des organisations.

Le facteur humain est certes décisif et peu contrôlable dans les situations de flux illégitimes (copie écrans, mémorisation, flux manuels, etc.), cependant il est insignifiant comparé aux dégâts causés par des processus et des systèmes automatisés. En effet, en retournant aux statistiques de la Section 1.2.1 du Chapitre 1, on remarque que le nombre moyen d'enregistrements par incident de fuite d'information est de l'ordre de centaines de milliers (plus de 246 mille) ce qui est loin de pouvoir être réalisé de façon manuelle ou uniquement à travers une intervention strictement humaine (sans processus informatique à l'appui). Ceci dit, nous estimons que notre modèle arrive à résoudre les problèmes de fuites d'informations causés par des processus informatiques se basant sur les divers mécanismes décrits dans le chapitre 6.

4- *Plusieurs modèles de sécurité existent déjà, quel serait l'apport d'un modèle additionnel comme le GBFC?*

Notre modèle ajoute une plus-value aux modèles existants du fait qu'il est conçu avec comme objectif principal la prévention de flux illégitimes. Contrairement à la majorité des modèles de contrôle d'accès (excepté les modèles MAC), GBFC est dédié au contrôle de flux. Ce contrôle est assuré à travers plusieurs mécanismes propres au GBFC : granularité, accès via des références, rafraîchissement des références et injection de bruit. La pluparts de ces mécanismes sont nouveaux au domaine de la sécurité des informations et du contrôle de flux en particulier et constituent les points forts de notre modèle. Dans ce sens, nous pouvons dire que notre modèle est orthogonal par rapport aux modèles existants, et peut être combiné avec eux (*cf.* Section 5.3.5, Chapitre 5 et Section 6.3.1, Chapitre 6).

5- *GBFC offre plusieurs paramètres de sécurité à appliquer au document confidentiel ce qui rendrait la tâche de l'administrateur plus complexe quant au choix des valeurs à affecter à ces paramètres.*

La multitude de critères de contrôle de sécurité du GBFC est, selon nous, un atout. Évidement, ceci offre à l'administrateur de sécurité un champ d'action beaucoup plus large et une manœuvrabilité intéressante. Il reste à offrir une carte de route qui permet à l'administrateur de facilement situer les besoins en sécurité de son système et les traduire sous forme de valeurs à affecter aux divers critères de sécurité. On peut aussi observer que le modèle n'exige pas que tous les paramètres soient instanciés. Chaque administrateur de système pourra décider quel niveau de complexité adopter.

Dans le graphique ci-dessous, nous avons tenté d'offrir une vue synthétique de la relation entre les divers critères de sécurité du GBFC avec les 3 aspects suivants : niveau de sécurité, niveau de disponibilité et niveau du risque de fuites d'information se basant sur le Tableau 6 du Chapitre 5 relatif aux valeurs des paramètres de sécurité du GBFC.

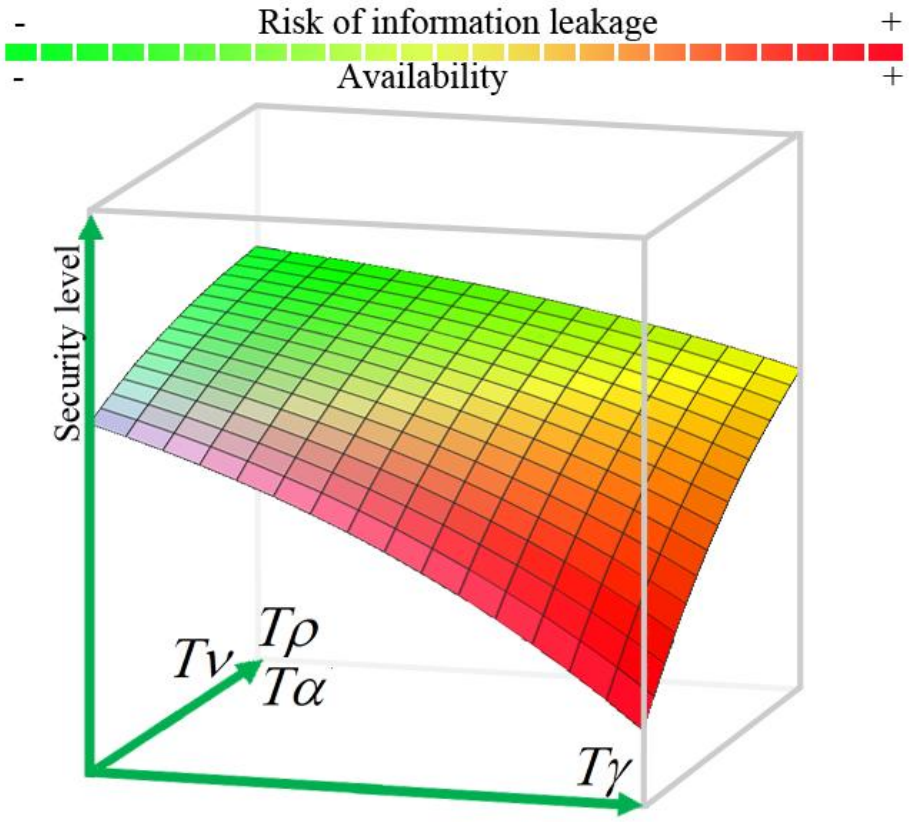


Figure 37. Évaluation du niveau de sécurité sur la base des paramètres du GBFC

Dans la Figure 37, nous retrouvons les différents paramètres de sécurité du modèle GBFC (niveau de granularité $T\gamma$, taux de disponibilité $T\alpha$, Taux de rafraîchissement $T\rho$, Niveau de bruit $T\nu$) qui sont évalués pour déterminer le niveau de sécurité, le niveau de risque de fuite et le niveau de disponibilité des informations confidentielles. Ainsi, à très haut niveau de granularité (mot), il y a plus de risque d'inférence que dans le cas de granularité faible (section ou chapitre par exemple), ceci étant inversement proportionnel au niveau de disponibilité de l'information une fois le contrôle de disponibilité appliqué. A ces granules nous appliquons les autres critères qui offrent un niveau de sécurité proportionnel à leurs valeurs comme décrit dans le Tableau 6 du Chapitre 5.

Il reste à souligner que tout projet de recherche, tel que le nôtre, reste un terrain fertile de développement et d’améliorations dans une quête continuelle d'avancement et d'excellence.

Chapitre 9 : Conclusions et perspectives

On arrive dans ce chapitre à la conclusion de notre projet de recherche portant sur le développement intégral d'un modèle de contrôle de flux basé sur la granularité dont la finalité est la protection de la confidentialité des informations par le biais de la prévention des flux illégitimes. Nous avons, tout au long de ce travail, tenté de cerner les différentes facettes de ce modèle, tout en insistant sur ses innovations et ses apports relativement à la protection contre les fuites d'informations. On traitera, ci-dessous, les principales contributions de cette thèse et on clôturera par une conclusion générale avec une liste non exhaustive des perspectives de recherches dans le cadre de ce thème.

9.1 Contributions de recherche

Dans cette thèse, nous avons adressé le problème du contrôle de flux d'informations dans l'organisation. Nous avons commencé par montrer que les modèles de contrôle d'accès existants sont encore loin de garantir un contrôle de flux d'informations satisfaisant. Plusieurs raisons sont à l'origine de cette limitation, dont l'incapacité de remédier entièrement aux problèmes de confinement et d'inférence. En effet, les modèles de contrôle d'accès conventionnels décrivent des politiques de lutte contre la propagation d'informations classifiées entre différentes classes et sont souvent soit trop restrictifs et rigides pour permettre une disponibilité acceptable de l'information (famille MAC) ou trop souples et ouverts pour garantir un niveau acceptable de contrôle de flux (DAC et similaires). En plus, ces systèmes, y compris les modèles plus récents tels RBAC et ABAC, après une validation d'accès à l'information, ne se préoccupent pas de l'usage que fait l'utilisateur de celle-ci, chose qui généralement est prise en charge par des mécanismes de sécurité additionnels. Il s'agit de renforcer une situation d'isolement ou de confinement de l'utilisateur afin d'empêcher tout flux d'information illicite vers des sujets tiers non autorisés. La Section 4.4 du Chapitre 4 traite ces problèmes -entre autres- en détail.

Pour adresser cette situation, nous avons développé notre modèle de contrôle de flux. Il s'agit d'un modèle dédié qui repose sur la granularité, l'accès via des références contrôlées, la restriction de flux et de disponibilité, et l'injection de bruit. GBFC tire profit de la puissance singulière et innovante qu'offre la combinaison de ces techniques pour proposer une solution robuste aux problèmes de fuites d'informations. La description détaillée de chacune de ces techniques en plus du processus et de l'algorithme du modèle sont fournis dans la Section 5.2 du Chapitre 5.

Notre méthodologie tente de résoudre le problème de fuite d'informations en adressant la cause principale du problème : le flux. Ceci est réalisé par la protection des trois composantes clés de tout flux d'information : Sujets, Objets et Données.

Nous avons montré la capacité du modèle GBFC à manipuler des informations classifiées granulaires sous la forme de références pour renforcer le contrôle de flux, même dans des situations extrêmes de pertes de matériel, d'attaques malveillantes et de fuites délibérées d'informations.

En outre, ce modèle offre des mécanismes de sécurité et de traçabilité des informations confidentielles de bout en bout rarement supportés par les modèles existants. La structure centralisée du modèle offre une grande maniabilité et adaptabilité aux différents environnements de sécurité mono et multi-domaines. Cela rend le GBFC bien adapté au Cloud Computing car la sécurité de chaque granule peut être gérée de façon indépendante dans le Cloud.

De plus, l'architecture centralisée peut être facilement mise en œuvre au niveau du système d'exploitation transformant ainsi chaque poste de travail en plate-forme de contrôle de sécurité totalement indépendante qui assure un contrôle de flux renfoncé et garantit une meilleure protection des informations et de vie privée.

Ceux-ci sont certains avantages du modèle GBFC parmi d'autres (cf. Chapitre 5, Section 5.3). Ces avantages sont confirmés par des exemples d'application et ont été concrétisés par le développement du modèle logique du GBFC (Chapitre 6, Section 6.2) et par une démonstration des capacités du modèle à pallier aux défaillances de contrôle de flux d'informations dont souffrent les modèles de contrôle d'accès existants. En effet, l'analyse des scenarios de fuites d'informations, dans la section 6.4 du chapitre 6, nous a permis de valider la capacité de notre modèle à protéger les informations confidentielles contre les flux illégitimes. Mieux encore, cette analyse montre la possibilité de remédier aux situations de fuites effectives d'informations.

Cela nous a permis de valider notre hypothèse de recherche avancée dans le Chapitre 1 (Section 1.4) et qui préconise qu'un modèle de sécurité tel que le nôtre, basé sur la granularité, l'accès via des références et la restriction de flux, est bien capable de garantir un contrôle de flux vigoureux tout en offrant une solution acceptable aux problèmes de fuites d'informations.

Le prototype logiciel, couvert par le Chapitre 7, a été conçu dans une optique de démonstration et de validation de certains apports du GBFC, pour venir à l'appui au modèle logique et ouvrir de nouvelles voies de perfectionnement et d'extension de ce modèle.

Nous avons aussi exploré certains domaines d'application éventuels de notre modèle et approché ses fonctionnalités de manière critique pour une vision plus large et plus claire (Chapitre 8).

En sommaire, les contributions essentielles de notre thèse sont :

1. Une analyse des principales familles de modèles de contrôle d'accès et de contrôle de flux, ayant pour but de dégager certaines des limites de ces modèles quant au contrôle de flux et à la prévention de fuites d'informations (Section 4.4, Chapitre 4).

2. La proposition de notre modèle de contrôle de flux basé sur la granularité dans son aspect organisationnel, fonctionnel et logique (Chapitre 5 et 6).
3. Des démonstrations formelles du fait que le modèle GBFC aide à pallier certaines faiblesses des autres modèles de contrôle d'accès et s'adapte aux divers scénarios de contrôle d'accès et de flux d'informations (Section 6.4, Chapitre 6).
4. La vérification de notre hypothèse de recherche (Section 6.4.2.4 et 6.4.2.5, Chapitre 6).
5. Une implémentation sous forme de prototype servant de moyen de démonstration des principales ce modèle. (Chapitre 7).
6. L'élaboration d'une liste non exhaustive des domaines d'application du modèle GBFC (Section 8.1, Chapitre 8).

A ces contributions s'ajoutent l'aspect évolutif et la flexibilité inhérents à cette solution et qui lui permettent de s'étendre vers d'autres domaines et couvrir encore plus de futures applications.

9.2 Perspectives de recherche

En addition aux contributions réalisées dans le cadre de cette thèse, un ensemble de perspectives de recherche, de perfectionnement et de travaux liés à ce modèle sont fortement envisageables. Certes, notre vision est d'autant plus large relativement à ce modèle de sécurité qui pourra être généralisé pour supporter d'autres formes d'informations. Ces formes peuvent être des bases de données, des images, de l'audio, de la vidéo ou d'autres structures de données qui ne pourront pas être traités dans cette thèse et établiront des thématiques de recherches futures. D'autres domaines de recherche liés à ce projet concernent l'intégration de méthodes et de techniques de traitement automatique du langage naturel (NLP) afin de dissimuler toute manipulation de l'information aux usagers non autorisés (noyer l'information dans du bruit). Un autre point d'importance majeure sera la possibilité de généralisation et d'adaptation de ce modèle à des environnements d'intérêt

tels les systèmes d’exploitation, le Cloud Computing ou encore les infrastructures distribuées, les médias sociaux et similaires.

Annexe 1 : Du ABAC au ZBAC

ABAC: Attribute Based Access Control
BBAC: Behavior-Based Access Control
CBAC: Claims Based Access Control
DBAC: Decision Based Access Control / Domain-Based Access Control
EBAC: Event-Based Access Control
FBAC: Fingerprint Access Control
GBAC: Governance-Based Access Control / Group Based Access Control/Guarantee-Based Access Control
HBAC: History Based Access Control / Host-Based Access Control
IBAC: Identity Based Access Control / Identification Based Access Control
JBAC: Job-based access control
KBAC: Knowledge Based Access Control / Knowledge-Based Admission Control
LBAC: Label Based Access Control / Lattice-Based Access Control
MBAC: Metadata Based Access Control
NBAC: NetBackup Access Control / autheNtication Based Access Control
OBAC: Object-Based Access Control/Ontology Based Access Control/Organization Based Access Control
PBAC: Policy Based Access Control
QBAC: Qualifications Based Access Control
RBAC: Role Based Access Control
SBAC: Service Based Access Control / Status-Based Access Control / Semantic-Based Access Control
TBAC: Trust-Based Access Control / Task Based Access Control
UBAC: User Based Access Control
VBAC: View-Based Access Control
WBAC: Workflow-Based Access Control
XBAC: XACML- based access control
YBAC: ---
ZBAC: authoriZation Based Access Control

Et plus …
BPAC: Business Process Access Control (WBAC)
MRBAC: Multi-role based access control
NDAC: Non-Discretionary Access Control
R&TBAC: Role-Task Based Access Control
RAdAC : Risk Adaptive Access Control
RSBAC: Rule Set Based Access Control

Bibliographie

[1] OQLF, 2013. [Online]. Available: http://gdt.oqlf.gouv.qc.ca.

[2] Risk Based Security, "First Quarter 2014 Exposes 176 Million Records," 29 05 2014. [Online]. Available: https://www.riskbasedsecurity.com/2014/05/first-quarter-2014-exposes-176-million-records-troubling-trend-of-larger-more-severe-data-breaches-continues/. [Accessed 05 01 2015].

[3] A. Russo and A. Sabelfeld, "Dynamic vs. Static Flow-Sensitive Security Analysis," in *23rd IEEE Computer Security Foundations Symposium*, 2010.

[4] S. Widup, "The Leaking Vault 2011, Six Years of Data Breaches," Digital Forensics Association, 2011.

[5] DataLossDB, "Data Loss Statistics," 2014. [Online]. Available: http://datalossdb.org/statistics. [Accessed 4 01 2015].

[6] Wikileaks, 2013. [Online]. Available: http://wikileaks.org/.

[7] B. Hicks, S. Rueda, L. St. Clair, T. Jaeger and P. McDaniel, "A logical specification and analysis for SELinux MLS policy," in *Transactions on Information and System Security (TISSEC)*, 2010.

[8] W. Masri, "Dynamic Information Flow Analysis, Slicing and Profiling," Case Western Reserve University, Cleveland, Ohio, USA, 2005.

[9] US Department of Defence, "Security requirements for automated Information Systems," DoD, 1988.

[10] INTOSAI EDP Audit Committee, "Information System Security Review Methodology," 1995.

[11] S. Geller, C. Hauser, F. Tronel and V. Viet Triem Tong, "Information Flow Control for Intrusion Detection Derived from MAC Policy," in *Meeting of the ICC*, 2011.

[12] R. Kissel, "Glossary of Key Information Security Terms," *NIST IR 7298 Revision 1*, 2011.

[13] Committee on National Security Systems, "National Information Assurance (IA) Glossary," CNSS, 2010.

[14] Merriam Webster Incorporated , "Confidential - Definition and More from the Free Merriam-Webster Dictionary," Merriam-Webster Inc., [Online]. Available: http://www.merriam-webster.com/dictionary. [Accessed 18 11 2014].

[15] Object Management Group, "OMG Unified Modeling Language (OMG UML) Version 2.5," Object Management Group, 2013.

[16] A. Maamir, A. Fellah and L. A. Salem, "Fine Granularity Access Rights for Information Flow Control in Object Oriented Systems," *International Journal of Security and its Applications*, vol. 2, no. 3, pp. 81-92, 2008.

[17] P. Samarati and S. de Capitani di Vimercati, "Access Control: Policies, Models, and Mechanisms," in *Foundations of Security Analysis and Design*, vol. 2171, London, UK, Springer-Verlag, 2001, pp. 137-196.

[18] US Department of Defence, "DoD Personnel Security Program," 1987.

[19] CGI Group, "Governance-Based Access Control (GBAC): Enabling improved information sharing that meets compliance requirements".

[20] J. R. Vacca, Computer and Information Security Handbook, 2 ed., Morgan Kaufmann Series, 2009.

[21] H. F. Tipton and M. Krause, Information Security Management Handbook, 6 ed., Auerbach Publications, 2007.

[22] H. Shon, CISSP certification all-in-one exam guide, McGraw-Hill, 2013.

[23] G. Stoneburner, "Underlying Technical Models for Information Technology Security," National Institute of Standards and technology, 2001.

[24] ISO, "Information Security Management Definitions," ISO/IEC 27001, [Online]. Available: http://www.iso.org/.

[25] Alberta Government, Information Management Branch, "Information Security Classification," 2005.

[26] M. Bishop, Introduction to Computer Security, 1 ed., Addison-Wesley, 2005.

[27] H. Mantel, "Information Flow Control and Applications - Bridging a Gap," in *International Symposium of Formal Methods Europe*, 2001.

[28] G. Lowe, "Defining Information Flow," in *IEEE Computer Security Foundations Workshop*, 1999.

[29] K. Bolshakov and E. Reshetova, "FreeBSD Mandatory Access Control Usage for Implementing Enterprise Security Policies," in *CoRR, abs/0706.1755*, 2007.

[30] A. Sabelfeld and A. C. Myers, "Language-based information-flow security," *IEEE Journal on selected areas in communications*, vol. 21, no. 1, pp. 5-19, 2003.

[31] D. E. Denning, "A lattice model of secure information flow," *Communications of the ACM (CACM)*, vol. 19, pp. 236-243, 1976.

[32] R. S. Sandhu, "Lattice-based access control models," *IEEE Computer*, vol. 26, no. 11, pp. 9-19, 1993.

[33] G. R. Andrews and R. P. Reitman, "An axiomatic approach to information flow in programs," *ACM Transactions on Programming Languages and Systems*, vol. 2, no. 1, pp. 56-76, 1980.

[34] S. O. Hwang and K. S. Yoon, "Privacy protection in ubiquitous computing based on privacy label and information flow," in *Computational Science and Its Applications - ICCSA 2*, 2004.

[35] M. Benantar, Access Control Systems: Security, Identity Management and Trust Models, 1 ed., Springer, 2006.

[36] C. E. Landwehr, "Formal Models for Computer Security," *ACM Computing Surveys (CSUR)*, vol. 13, no. 3, pp. 247-278, 1981.

[37] S. Zander, G. Armitage and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Communications Surveys & Tutorials*, vol. 9, no. 3, pp. 44-57, 2007.

[38] W. L. Butler, "A note on the confinement problem," *Communications of the ACM*, vol. 16, no. 10, pp. 613-615, 1973.

[39] National Computer Security Center, US DoD, "Trusted computer system evaluation criteria," 1985.

[40] D. E. Denning and P. J. Denning, "Data Security," *Computing Surveys*, vol. II, no. 3, pp. 227-249, 1997.

[41] D. Hedin and A. Sabelfeld, "A Perspective on Information-Flow Control," in *Marktoberdorf Summer School. IOS Press*, 2011.

[42] US Department of Defence, "DoD Directive- Security requirements for automated information systems," 1988.

[43] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology, 2013.

[44] D. F. Ferraiolo, R. Kuhn and R. Chandramouli, Role-Based Access Control, 2 ed., Artech House Publishers, 2007.

[45] D. E. Denning, "Secure information flow in computer systems," Purdue University West Lafayette, 1975.

[46] T. S. Mikko and O. K. Harri, "A review of information security issues and respective research contributions," *SIGMIS Database*, vol. 38, no. 1, pp. 60-80, 2007.

[47] P. Y. A. Ryan and S. A. Schneider, "Process Algebra and Non-interference," in *12th IEEE Computer Security Foundations Workshop*, 1999.

[48] S. Castano, M. Fugini, M. Martell and P. Samarati, Database Security, 1 ed., Boston, MA: Addison-Wesley, 1995.

[49] R. Kemmerer and P. Porras, "Covert Flow Trees: A Visual Approach to Analyzing Covert Storage Channels," in *IEEE Transactions on Software Engineering, Vol. 17, No. 11*, 1991.

[50] I. S. Moskowitz and M. H. Kang, "Covert Channels – Here to Stay?," in *9th Conference on Computer Assurance (COMPASS '94)*, 1994.

[51] J. K. Millen, "20 Years of Covert Channel Modeling and Analysis," in *IEEE*

Symposium on Security and Privacy., 1999.

[52] J. A. Goguen and J. Meseguer, "Security policies and security models," in *Symposium on Security and Privacy*, 1982.

[53] A. W. Roscoe and M. H. Goldsmith, "What is intransitive noninterference?," in *12th IEEE Computer Security Foundations Workshop*, 1999.

[54] D. von Oheimb, "Information Flow Control Revisited: Noninfluence = Noninterference + Nonleakage," in *European Symposium on Research in Computer Security (ESORICS), LNCS 3193*, 2004.

[55] NIST, "A Report on the Privilege (Access) Management Workshop," National Institute of Standards and Technology, 2010.

[56] A. R. Khan, "Access Control in Cloud Computing Environment," *ARPN Journal of Engineering and Applied Sciences,*, vol. 7, no. 5, pp. 613-615, 2012.

[57] M. Bishop, Computer Security: Art and Science, Addison Wesley, 2002.

[58] E. Sahafizadeh and S. Parsa, "Survey on Access Control Models," in *2nd International Conference on Future Computer and Communication (ICFCC)*, 2010.

[59] S. Demurjian, "Implementation of Mandatory Access Control in Role based Security System with Oracle Snapshot Skill," 2001.

[60] A. V. D. M. Kayem, S. G. Akl and P. Martin, "A Presentation of Access Control Methods," in *Adaptive Cryptographic Access Control*, 1 ed., Springer Science+Business, 2010, pp. 11-40.

[61] D. E. Bell and L. J. LaPadula, "Secure computer systems: Mathematical foundations and model," The MITRE Corp., Bedford, MA, 1973.

[62] D. E. Bell and L. J. LaPadula, "Secure computer system: Unified exposition and multics interpretation," The Mitre Corp., Bedford, MA, 1973.

[63] V. C. Hu, D. F. Ferraiolo and D. R. Kuhn, "Assessment of Access Control Systems," National Institute of Standards and Technology (NIST), 2006.

[64] K. J. Biba, "Integrity considerations for secure computer systems," The MITRE Corporation, 1977.

[65] J. D. Bokefode, S. A. Ubale, S. S. Apte and D. G. Modani, "Analysis of DAC MAC RBAC Access Control based Models for Security," *International Journal of Computer Applications* , vol. 104, no. 5, pp. 6-13, 2014.

[66] D. F. C. Brewer and M. J. Nash, "The Chinese Wall Security Policy," in *IEEE Symposium on Security and Privacy*, 1989.

[67] P. Y. A. Ryan, "Mathematical Models of Computer Security," in *Foundations of Security Analysis and Design*, 1 ed., Springer-Verlag, 2001, pp. 1-62.

[68] D. F. Ferraiolo and R. Kuhn, "Role-Based Access Controls," in *15th National Computer Security Conference*, 1992.

[69] R. S. Sandhu, D. Ferraiolo and R. Kuhn, "The NIST Model for Role Based

Access Control: Toward a Unified Standard," in *5th ACM Workshop on Role Based Access Control*, 2000.

[70] S. Osborn, R. S. Sandhu and Q. Munawer, "Configuring Role-Based Access Control to enforce Mandatory and Discretionary access control policies," *ACM Trans. Information and system security*, vol. 3, no. 2, pp. 1-23, 2000.

[71] S. Osborn, "Information Flow Analysis of an RBAC system," in *SACMAT02*, 2002.

[72] N. Tuval and E. Gudes, "Resolving Information Flow Conflicts in RBAC Systems," *Data and Applications Security*, vol. LNCS 4127, pp. 148-162, 2006.

[73] J. Crampton, "On permissions, inheritance and role hierarchies," in *10th ACM Conference on Computer and Communications Security*, 2003.

[74] NIST, "Attribute Based Access Control," National Institute of Standards and Technology, 2014.

[75] NIST-NSA, "A Survey of Access Control Methods," National Institute of Standards and Technology and National Security Agency, 2009.

[76] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller and K. Scarfone, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations," NIST, 2014.

[77] D. Ferraiolo, "Towards an ABAC Family of Models," National Institute of Standards and Technology, 2013.

[78] G. Boudol and M. Kolundzija, "Access Control and Declassification," *CCIS Computer Network Security*, vol. 1, no. Springer-Verlag, pp. 85-98, 2007.

[79] A. C. Myers, "JFlow: practical mostly-static information flow control," in *26th ACM SIGPLAN-SIGACT* , 1999.

[80] A. C. Myers and B. Liskov, "Protecting privacy using the decentralized label model," *ACM Transactions on Software Engingeering Methodology*, vol. 9, pp. 410-442, 2000.

[81] A. C. Myers and B. Liskov, "A decentralized model for information flow control," in *17th ACM Symp. on Operating System Principles (SOSP)*, 1997.

[82] P. Li and S. Zdancewic, "Arrows for Secure Information Flow," *Theoretical Computer Science*, vol. 411, no. 19, pp. 1974-1994, 2010.

[83] D. Kafura and D. Gracanin, "An Information Flow Control Meta-Model," in *Symposium on Access Control Models and Technologies (SACMAT'13)*, 2013.

[84] N. Zeldovich, S. Boyd-Wickizer and D. Mazieres, "Securing distributed systems with information flow control," in *USENIX NSDI*, 2008.

[85] S. Zdancewic, "Challenges for Information-flow Security," in *1st International Workshop on the Programming Language Interference and Dependence (PLID'04)*, 2004.

[86] K. P. Fischer-Hellmann, Information Flow Based Security Control Beyond

RBAC, 1 ed., Springer Vieweg, 2012.

[87] T. L. Hinrichs, W. C. Garrison, A. J. Lee, S. Saunders and J. C. Mitchell, "TBA: A Hybrid of Logic and Extensional Access Control Systems," in *International Workshop on Formal Aspects of Security and Trust (FAST)*, 2011.

[88] S. Etalle, T. L. Hinrichs, A. J. Lee, D. Trivellato and N. Zannone, "Policy administration in tag-based authorization," in *5th International Symposium on Foundations and Practice of Security (FPS)*, 2013.

[89] P. Samarati, E. Bertino, A. Ciampichetti and S. Jajodia, "Information Flow Control inObject-Oriented Systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 9, no. 4, pp. 524-538, 1997.

[90] F. Cuppens and G. Trouessin, "Information flow controls vs inference controls: An integrated approach," in *Third European Symposium on Research in Computer Security*, 1994.

[91] K. Izaki, K. Tanaka and M. Takizawa, "Information Flow Control in Role-Based Model for Distributed Objects," in *IEEE International Conf. on Parallel and Distributed Systems*, 2001.

[92] Verizon, "2013 Data Breach Investigations report," 2013.

[93] C. R. Smith, C. Buckley and E. Younker, "Information Security - Establish a Strong Defense in Cyberspace," in *Securing the Enterprise: The Latest Strategies and Technologies for Building a Safe Architecture*, Gartner Inc., 2003, pp. 27-39.

[94] W. Jie, Computer Network Security Theory and Practice, Higher Education Press, Higher Education Press, Beijing and Springer-Verlag GmbH, 2009.

[95] S. Bosworth and M. E. Kabay, Computer Security Handbook, 4 ed., John Wiley & sons, 2002.

[96] D. Salomon, Foundations of Computer Security, London: Springer-Verlag , 2006.

[97] R. Focardi and R. Gorrieri, Foundations of Security Analysis and Design, Springer-Verlag Berlin Heidelberg, 2001.

[98] J. Migga Kizza, Guide to Computer Network Security, 2 ed., London: Springer-Verlag, 2013.

[99] J. R. Vacca, Guide to Wireless Network Security, Springer Science+Business Media, 2006.

[100] D. W. Frye, Network Security Policies and Procedures, Springer Science+Business Media, 2007.

[101] T. R. Peltier, Information security policies and procedures. A practitioner's reference, CRC Press LLC, 1999.

[102] E. Tomoya, B. Valbona and T. Makoto, "Role-Based Scheduling and Synchronization Algorithms to Prevent Illegal Information Flow," in *First*

International Conference on Network-based Information System, 2007.

[103] R. Chon, T. Enokido and M. Takizawa, "Inter-Role Information Flow in Object-based Systems," in *IEEE 18th International Conf. on Advanced Information Networking and Applications*, 2004.

[104] Z. Mao, N. Li and H. Chen, "Trojan Horse Resistant Discretionary Access Control," in *ACM Symposium on Access Control Models and Technologies (SACMAT'09)*, 2009.

[105] A. Spalka, A. B. Cremers and H. Lehmler, "Protecting confidentiality against Trojan Horse Programs in Discretionary Access Control Systems," *Lecture Notes in Computer Science*, vol. 1841, pp. 1-17, 2000.

[106] A. Maamir, A. Fellah and L. A. Salem, "Controlling Information Flow in Object Oriented Systems," *Journal of Information Assurance and Security*, vol. 07/2008, no. 2, pp. 140-146, 2008.

[107] Oracle Corporation, "Oracle8i Concepts," 1999.

[108] ICAM Subcommittee, "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance," ICAMSC, 2011.

[109] J. Park and R. S. Sandhu, "Towards usage control models: beyond traditional access control," in *Symposium on Access control Models and Technologies (SACMAT)*, 2002.

[110] McAfee, "Data Loss by the Numbers," 2012.

[111] InfoWatch Analytical Labs, "Global Data Leakages & Insider Threats," 2012.

[112] J. T. Yao, "A Ten-year Review of Granular Computing," in *IEEE International Conference on Granular Computing*, 2007.

[113] L. A. Zadeh, "Towards a theory of fuzzy information granulation and its centrality in human reasoning and fuzzy logic," *Fuzzy Sets and Systems*, vol. 90, no. 2, pp. 111-127, 1997.

[114] K. Ghazinour, M. Majedi and K. Barker, "A Lattice-based Privacy Aware Access Control Model," in *IEEE International Conference on Computational Science and Engineering*, 2009.

[115] D. Thorleuchter and D. Van den Poel, "High Granular Multi-Level-Security Model for Improved Usability," in *International Conference on System Science, Engineering Design and Manufacturing Informatization*, 2011.

[116] M. Ebbers, W. O'Brien and B. Ogden, "Introduction to the new mainframe zOS Basics," 2006.

[117] Information Security Oversight Office, "Marking Classified National Security Information," 2007.

[118] Excellence Center for Development of Security, "Marking Classified Information," 2012.

[119] Joint Chiefs Of Staff, "Emergency action procedures of the Joint Chiefs of

Staff : Nuclear Control Orders," 1985.

[120] L. Logrippo, "Logical Method for Reasoning about Access Control and Data Flow Control Models," in *7th International Symposium on Foundations and Practice of Security (FSP 2014)*, 2014.

[121] M. M. Kocaturk and T. I. Gundem, "A Fine-Grained Access Control System Combining MAC and RBACK Models for XML," *INFORMATICA*, vol. 19, no. 4, pp. 517-534, 2008.

[122] A. Silberschatz, P. Baer Galvin and G. Gagne, Operating System Concepts, 9 ed., John Wiley & Sons, Inc, 2013.

[123] V. Thangaswamy, VSTO 3.0 for Office 2007 Programming, Packt Publishing Limited, 2009.

[124] G. Booch, J. Rumbaugh and I. Jacobson, The Unified Modeling Language User Guide, Addison Wesley, 1998.

[125] J. Rumbaugh, I. Jacobson and G. Booch, The Unified Modeling Language Reference Manual, Addison Wesley, 1999.

[126] M. Fowler and K. Scott, UML Distilled Second Edition A Brief Guide to the Standard Object, Addison Wesley, 1999.

[127] Y.-K. Liu, "Building one-time memories from isolated qubits," in *5th conference on Innovations in theoretical computer science (ITCS) conference*, 2014.

Index

A

B

C

D

E

F

G

I

M

N

O

P

R

S

T

U

V

X